
Giorgio Sbaraglia
CYBER SECURITY
kit di sopravvivenza
Il web è un luogo pericoloso.
Dobbiamo difenderci!
Prefazione di
Alessio L.R. Pennasilico
goWare

Giorgio Sbaraglia

CYBER SECURITY

kit di sopravvivenza

Il web è un luogo pericoloso.
Dobbiamo difenderci!

Prefazione di
Alessio L.R. Pennasilico

goWare

Grazie per aver acquistato l'ebook di Giorgio Sbaraglia
Cybersecurity kit di sopravvivenza.
Il web è un luogo pericoloso.
Dobbiamo difenderci!

Per ricevere offerte speciali, informazioni sulle promozioni e le nuove uscite iscriviti alla nostra newsletter

ISCRIVITI

Oppure vieni sul nostro sito
www.goware-apps.com

Se vuoi contattare l'autore
scrivi qui

Con il patrocinio di

Giorgio Sbaraglia è membro del Clusit

https://clusit.it/mese-europeo-della-sicurezza-informatica-ottobre-2018/

ISBN: 978-88-3363-107-3

Testi della rubrica “L’angolo del nerd”: Uberto Vittorio Favero

Editor: Cristina Vernizzi
Copertina: Francesco Mancini
Sviluppo ePub: Elisa Baglioni

goWare è una start-up fiorentina specializzata in nuova editoria

Fateci avere i vostri commenti a: info@goware-apps.it
Blogger e giornalisti possono richiedere una copia saggio
a Maria Ranieri: mari@goware-apps.com

Seguici su

facebook twitter newsletter

flipboard: goware <ebook> extra blog

Indice dei contenuti

Presentazione

Perché dovrebbero attaccare proprio me? Oggi nessuno può considerarsi al sicuro, perché gli attacchi sono sempre più frequenti e talora automatizzati.

Gli strumenti informatici sono importanti, ma il punto debole della sicurezza è sempre il fattore umano. È noto che oltre il 90% dei cyber attacchi sono causati da un errore umano: può bastare un click per perdere tutti i dati personali di un utente o per mettere in crisi un'intera azienda.

Questo libro racconta come il *cybercrime* si è evoluto, con esempi e storie vere. Vengono illustrate le tecniche d'attacco, dal *phishing* ai *ransomware*, dai *malware* sugli smartphone all'uso sbagliato delle password.

E soprattutto spiega come fare per difenderci, con consigli utili per gli utenti e con approfondimenti tecnici per i più esperti.

Tutto questo raccolto in un unico testo che ci mostra – a 360 gradi – che cosa è la *cybersecurity*, una disciplina affascinante e mai noiosa, che si evolve ogni giorno con nuovi attori e attacchi sempre diversi.

***

GIORGIO SBARAGLIA, ingegnere, per molti anni dirigente in una grande società di costruzioni, appassionato da sempre ai temi della sicurezza informatica, ha trasformato la sua passione in una professione. Membro del CLUSIT, svolge oggi attività di consulenza e formazione per la sicurezza informatica e per il GDPR.

Tiene corsi su questi temi per molte importanti società italiane, tra le quali la prestigiosa Business School de "Il Sole 24 Ore". Ha pubblicato per goWare il libro *GDPR kit di sopravvivenza*.

A Paola ed Elena

Prefazione

di Alessio L.R. Pennasilico

Information & Cyber Security Advisor
Presidente Associazione Informatici Professionisti
Comitato Tecnico Scientifico Clusit

La Cybersecurity non è più, e non può più essere, un argomento per esperti. Se mai lo è stata.

Per questa ragione è indispensabile raccontare a tutti, anche a chi tecnico non è, e non deve esserlo, quali rischi si corrono e come ci si può difendere, facendolo con il linguaggio adatto e portando contenuti realmente interessanti e casi reali. Per comprendere che non ci dobbiamo preparare al futuro, ma cercare di recuperare un enorme ritardo sulla consapevolezza, che dovremmo aver avuto costruito negli anni passati, e non abbiamo fatto.

Per queste ragioni, è fondamentale un libro come *Cybersecurity: kit di sopravvivenza*, scritto da un professionista esperto, come Giorgio Sbaraglia, che dopo tante, mai troppe, ore di aula come docente, sa spiegare al grande pubblico lo scenario di riferimento, le minacce che rischiano di inficiare le opportunità, i comportamenti più adatti da tenere.

Internet, infatti, è un luogo meraviglioso, ha trasformato le nostre vite, su molti aspetti in meglio, e continuerà a farlo. Per questa ragione dobbiamo essere attenti a non volgere questa opportunità in un incubo.

Conoscere e comprendere questi temi è indispensabile per garantire la nostra "incolumità digitale": la nostra, ma soprattutto quella dei nostri figli, ragazzi con una vita digitale più ricca, ma con meno "paranoia".

#iosonopreoccupato perché stiamo ancora ignorando o sottovalutando troppi rischi. Ma spero in un futuro migliore, che dobbiamo costruire con un pezzetto di consapevolezza per volta, con attenzione e costanza, per comprendere e attuare il comportamento adatto a tutelarci.

E questo libro può essere uno dei primi e più importanti elementi di conoscenza e comprensione dello scenario per chi utilizza quotidianamente gli strumenti digitali e vuole garantire la corretta gestione di tutte le informazioni che riguardano sé, i suoi cari, il suo lavoro.

Introduzione

Perché un libro sulla Cybersecurity

La rete dà e la rete prende: per capire quanto è diventato pericoloso il web... basta andare nel web, fare qualche domanda a Google, che in una frazione di secondo ci scoverà mille risposte.

Nella rete possiamo trovare qualunque spiegazione e forse incappare anche in qualche brutta sorpresa.

Se nel web c'è già tutto (ma anche il contrario di tutto!), a cosa potrebbe servire un libro che parla proprio del web e dei suoi pericoli?

Ho voluto scrivere questo libro per dare un quadro complessivo del tema, raccogliendo in un'unica trattazione i tanti aspetti del web e dei rischi informatici che nel web si annidano. E anche per rendere disponibile al lettore italiano alcune informazioni reperibili soltanto in inglese.

Non si tratta però di un compendio rivolto agli specialisti, a chi lavora nel settore IT (Information Technology) delle aziende, ma di un testo indirizzato a tutte le persone che usano un computer, uno smartphone, un tablet. Tutti noi oggi lo facciamo, ma spesso in modo superficiale, con una conoscenza soltanto confusa o approssimativa di questi strumenti e dei rischi che corriamo quando navighiamo in rete.

Ancor oggi alcune persone mi dicono che non utilizzano la carta di credito per acquisti in internet perché hanno paura, o mi chiedono come fare a riconoscere una mail che nasconde una truffa, e poi magari scopro che queste persone usano password totalmente insicure come "password" o "12345678".

Ho voluto raccogliere in queste pagine l'esperienza che ho acquisito come formatore in aula sul tema della cybersecurity, dove racconto che "**il web è diventato un luogo pericoloso, certo, ma possiamo difenderci!**". Questa è la frase che dà il titolo ai miei corsi, soprattutto quelli più basici, quelli – appunto –

di consapevolezza. E il messaggio che vorrei trasmettere è in fondo molto semplice: dobbiamo essere consapevoli di quanto la rete sia diventata pericolosa, acquisendo un poco di quella "sana paranoia" che nella sicurezza informatica rappresenta una virtù. Non è poi così difficile difendersi, serve soprattutto acquisire la consapevolezza ("awareness") dei rischi e sapere come affrontarli.

Vedremo infatti che, nella maggior parte dei cyber attacchi, la tecnica è relativamente semplice, talvolta quasi rudimentale, ma l'attacco ha successo per la debolezza del fattore umano: cadiamo nella trappola per superficialità e mancanza di conoscenza, perché nell'utilizzo quotidiano dei dispositivi informatici ci è mancata la fase – indispensabile – della formazione.

La mia attività di formatore è un'esperienza coinvolgente che mi porta a contatto con tante persone (sono stati circa tremila i partecipanti in aula negli ultimi due anni). Molti sono spaventati dalle mille minacce della rete, dall'ansia di non saperle riconoscere. E sopportano senza convinzione, e spesso senza comprenderne pienamente il senso, le limitazioni e le prescrizioni d'utilizzo che l'azienda impone loro, proprio allo scopo di evitare gli incidenti informatici.

Quando in aula racconto perché certi rischi si verificano e spiego poi come riconoscerli ed evitarli, mi accorgo che la conoscenza e la consapevolezza trasformano un mondo ostile in qualcosa che diventa interessante. E per rendere più comprensibile e accattivante una materia apparentemente ostica mi piace raccontare storie.

Anche in questo libro il lettore troverà molte storie, funzionali a introdurre un tema e a illustrarlo con esempi pratici tratti da accadimenti reali che fanno capire quali sono i rischi del web e quali sono i comportamenti corretti da mettere in pratica.

Non è stato difficile scrivere questo libro, la cosa più complicata è stata decidere quando e dove fermarsi, quando concludere ogni argomento. Perché ogni giorno ci porta un evento nuovo, un altro attacco diverso da quelli precedenti. La cybersecurity è una disciplina affascinante e mai noiosa.

Mi auguro perciò di riuscire a trasmettere al lettore questa continua evoluzione: ben sapendo che quello che scriviamo oggi potrebbe essere superato già domani,

rimarranno comunque validi i metodi per conoscere e capire il mondo della cybersecurity.

Cybercrime e cybersecurity: una panoramica

Un graffito di Abstrk, un artista americano di origine cubane, nel quartiere di Magic City a Miami.

1

Che cos'è la Cybersecurity e perché è così importante

1.1 Dalla Cibernetica alla Cybersecurity

Il termine "**cibernetica**" deriva dalla parola in greco antico *kybernetes* (κυβερνήτης) che indica il pilota di una nave, con la radice *kyber* che significa "timone". Il termine, per estensione, sta ad indicare colui che guida, o governa, una città o uno stato: l'espressione *kybernetikès techne*, l'arte del pilotare, assume il significato più ampio di "arte del governo".

Il termine "cibernetica" è stato coniato dal matematico statunitense Norbert Wiener, nel libro *Cybernetics, or control and communication in the animal and the machine* (1948).

Wiener è riconosciuto come il padre della cibernetica moderna, che nella sua opera la definì come la scienza "del controllo e della comunicazione nell'animale e nella macchina".

La cibernetica rappresenta un'attività interdisciplinare, che si propone di studiare e di realizzare macchine ad alto grado di automatismo, atte a sostituire l'uomo nella sua funzione di controllore e di pilota (*kybernetes*) di macchine e di impianti.

Si sono così sviluppati gli elaboratori elettronici in grado di eseguire in modo automatico processi di elaborazione delle informazioni: macchine capaci di evolversi e di modificarsi, mediante fenomeni di apprendimento, fino ad arrivare all'intelligenza artificiale ed alle reti neurali, che creano una corrispondenza fra le strutture nervose naturali e quelle artificiali.

L'**informatica** (in inglese *computer science*) si occupa del trattamento dell'informazione mediante sistemi elettronici automatizzati: i calcolatori (in inglese *computer*).

Oggi i computer si presentano sotto diverse forme: non più solo il classico desktop posto sulle scrivanie degli uffici, ma una moltitudine di dispositivi con caratteristiche diverse tutti però dotati di un processore, un sistema operativo e un collegamento di rete.

E tutti questi oggetti devono essere messi in sicurezza, protetti, perché contengono le informazioni, l'asset più importante per un'azienda. Ogni organizzazione, pubblica o privata, grande o piccola, deve essere in grado di garantire la sicurezza dei propri dati, in un mondo dove i rischi informatici sono in continuo aumento.

Nasce quindi la **cybersecurity**, una scienza ancora giovane e della quale anche ora si fatica a comprendere l'importanza strategica, ma che diventerà sempre più necessaria, per non mettere a rischio la sopravvivenza stessa di un'organizzazione.

> Gli attacchi informatici sono una minaccia crescente per un'economia che sempre più si basa su tecnologie digitali. Il rischio cibernetico interessa molteplici attività produttive e di consumo; per sua natura oltrepassa i confini tra paesi e settori[1].

1.2 Che cosa è e quanto ci costa il cybercrime oggi

Siamo completamenti immersi nel web, che coinvolge ogni momento della nostra vita sia personale che professionale. Internet è diventato il motore della "quarta rivoluzione industriale", generando opportunità di crescita e sviluppo impensabili fino a pochi decenni fa.

Inevitabilmente il business creato dalla rete non poteva non avere – come in tutte le attività umane – qualche "effetto collaterale" negativo. Stiamo parlando evidentemente del cybercrime che in questi ultimi anni ha assunto dimensioni impressionanti.

FAQ ▶ CHE COSA È IL CYBERCRIME?

Il **reato informatico** (o **cybercrime**) consiste in una attività criminosa, analoga a quella tradizionale ma caratterizzata dall'abuso della tecnologia informatica (sia hardware che software). Con lo sviluppo dell'"industria informatica", questa attività ha acquistato un peso sempre più importante e oggi sta diventando una delle attività maggiormente

lucrose anche per la criminalità organizzata tradizionale.
Si è creato un **nuovo modello di business** che ha sempre l'obiettivo di realizzare guadagni, ma lo fa sfruttando (in modo sempre più sofisticato e professionale) le debolezze informatiche delle aziende e delle persone.
In altre parole: la criminalità organizzata ha ormai capito che con "quelli che usano i computer" (in genere abbastanza male...) è possibile realizzare attacchi estremamente redditizi e con bassi rischi.
Le forme del cybercrime sono molte e variegate:

- la frode informatica finalizzata a realizzare un guadagno
- il falso in documenti informatici
- il danneggiamento ed il sabotaggio informatico
- l'accesso abusivo, associato alla violazione delle misure di sicurezza del sistema
- lo spionaggio (a scopo politico o industriale)
- l'estorsione (il caso tipico del ransomware).

In altre situazioni il cybercrime è finalizzato ad attaccare e mettere in crisi i sistemi informativi di sicurezza nazionale di uno Stato. In questo caso si parla più precisamente di "*cyberwarfare*" (guerra cibernetica tra stati).
Ne parleremo in dettaglio nel capitolo 9 "Gli attacchi ai sistemi industriali (ICS)".

Pochi ma significativi dati possono illustrare questa affermazione.

Nel solo 2015 sono andati persi nel mondo 445 miliardi di dollari per salvaguardare la proprietà intellettuale, per i lavori bruciati e per il tempo speso a rimediare i danni del crimine informatico.

Il 97% delle 500 aziende più ricche del mondo secondo Fortune ha subito almeno un attacco informatico (cit. Peter Warren Singer[2], direttore del Center for 21st Century Security and Intelligence presso il Brookings Institution).

Negli ultimi anni la dimensione del fenomeno è andata sempre crescendo, senza soluzione di continuità.

Nel 2016, il peso del cybercrime nell'economia mondiale è stato stimato in 650 miliardi di dollari. Gli analisti di IDC[3] (International Data Corporation, la prima società mondiale specializzata in ricerche di mercato, consulenza nei settori

ICT e dell'innovazione digitale) prevedono che tale valore arriverà a 1.000 miliardi di dollari nel 2020. [Vedi Figura 1]

Secondo Juniper Research[4] entro il 2019 toccheranno i duemila miliardi di dollari (un numero simile al PIL di una nazione come l'Italia!). Per Virginia "Ginni" Rometty, CEO di IBM, siamo davanti alla più grande minaccia per le aziende di tutto il mondo.

Negli USA, il paese ritenuto più avanzato e leader nell'informatica, il costo per l'economia derivante da "*malicious cyber activity*" è stimabile tra 57 e 109 miliardi di dollari, che corrispondono indicativamente allo 0,3-0,6% del PIL nazionale.

Il "fatturato" del cybercrime sta superando a livello mondiale quello del traffico di droga. Tutto questo ci porta ad una conclusione: il mondo sta cambiando, non ci sono più gli hacker di una volta...

1.3 Lo scenario in Italia

In Italia la situazione non è migliore. Al contrario, lo scenario è preoccupante, dato che siamo ancora oggi un paese con una cultura informatica piuttosto bassa, soprattutto per quanto riguarda la formazione del "fattore umano".

Ripercorriamo la storia con alcuni dati riportati dal CLUSIT[5], la più autorevole associazione italiana nel campo della sicurezza informatica (nata nel 2000 e che oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese), che ogni anno, dal 2011, redige un rapporto annuale sulla sicurezza informatica in Italia.

Il **Rapporto CLUSIT 2016** evidenzia una crescita del 30% nel 2015 rispetto all'anno 2014 del crimine informatico in Italia.

Il **Rapporto CLUSIT 2017** ci dice che "gli attacchi compiuti con tecniche di Phishing e Social Engineering sono cresciuti nel 2016 del **+1.166%,** rispetto al 2015" (spiegheremo poi in dettaglio cosa sono Phishing e Social Engineering, che rappresentano le tecniche d'attacco più diffuse in tutti i settori).

L'ultimo **Rapporto CLUSIT** [Vedi Figura 2], pubblicato a marzo **2018**, riporta dati ancora più preoccupanti: il 45% delle aziende italiane sono state colpite da cyber attacchi. Ed i danni stimati per questi attacchi sono stati pari a **10 miliardi**

di euro (un numero paragonabile ad una manovra finanziaria e corrispondente a circa lo 0,5% del nostro PIL).

Ma quali sono i rischi più temuti dalle aziende a causa del cybercrime?
Troviamo dati interessanti nel Rapporto Italia 2017 di Eurispes [Vedi Figura 3], che ci elenca quello che preoccupa maggiormente le aziende.

Quindi il problema non è solo perdere soldi o perdere dati, che poi è la stessa cosa perché "i dati sono il petrolio del terzo millennio", come ha sostenuto Tim Berners-Lee[6], colui che è considerato l'inventore del World Wide Web. Spaventano anche il furto d'identità e soprattutto il danno reputazionale.

FAQ ▶ CHE COSA È IL FURTO D'IDENTITÀ?

Il furto d'identità è una condotta criminale in cui ci si spaccia per un'altra persona per ottenere indebitamente denaro o vantaggi o per screditare e mettere in cattiva luce la persona fisica che si finge di essere. In questo caso può rappresentare anche una forma di cyberbullismo (esercitato soprattutto attraverso i social media).
Vittima del furto d'identità può risultare anche un'azienda con ricadute economiche, ma soprattutto reputazionali e legali.

Davanti a questo scenario, cosa fanno le aziende italiane?
Gabriele Faggioli, presidente del CLUSIT, afferma che:

> Le aziende italiane oggi hanno più consapevolezza dell'importanza della gestione della sicurezza, ma secondo le nostre statistiche sono ancora in ritardo. La spesa delle aziende per la sicurezza, pur aumentata, è ancora troppo bassa: gli investimenti in IT sono stati di 76 miliardi di euro nel 2017. Di questi, solo 1,09 miliardi sono andati nella sicurezza informatica, una cifra che corrisponde ad appena l'1,5%, ben inferiore a quella degli altri paesi europei.

Questo dato è comunque in crescita del 12% rispetto al 2016. Un passo in avanti importante, rispetto agli anni scorsi, quando il mercato nazionale cresceva a ritmi decisamente inferiori (4-6%).
Il 78% di questa spesa è concentrata nelle grandi aziende, trainato anche dal progetto di adeguamento al GDPR (il nuovo regolamento europeo sulla privacy).

Alle PMI rimane solo il 22% dell'investimento, che si riduce al diminuire della dimensione aziendale.

Secondo uno studio della Banca d'Italia, nel 2016 le aziende italiane hanno investito in media 4.530 euro ciascuna, una cifra sicuramente bassa. Secondo lo stesso studio, l'atteggiamento più diffuso è quello di "chiudere la stalla dopo che i buoi sono scappati". L'investimento in sicurezza informatica è visto come non remunerativo... fino a che non succede l'incidente.

In questo senso, la risonanza mediatica che hanno avuto gli attacchi più importanti su scala mondiale (WannaCry e NotPetya sopra tutti) è stata utile per far crescere nelle persone e nelle aziende la consapevolezza dell'esistenza del rischio informatico.

CLUSIT promuove in Italia l'**European Cyber Security Month** (ECSM) [Vedi Figura 4], una campagna dell'Unione Europea che si tiene ogni anno durante tutto il mese di ottobre per promuovere tra i cittadini la conoscenza delle minacce informatiche e dei metodi per contrastarle, per cambiare la loro percezione di cyber minacce e fornire informazioni aggiornate in materia di protezione cibernetica e sicurezza informatica. L'ECSM è organizzato dall'agenzia europea ENISA (European Network and Information Security Agency), con svariate attività in tutti i Paesi membri dell'UE. L'autore è partner italiano accreditato dell'**ECSM 2018**[7].

1.4 Non ci sono più gli hacker di una volta

Una volta c'erano gli hacker e il loro spirito goliardico. Lo stesso verbo *to hack*, che significa "tagliare", "sfrondare", "sminuzzare", "ridurre", "aprirsi un varco" tra le righe di codice di un programma, era nato al Massachusetts Institute of Technology (MIT) di Boston per indicare semplicemente un'infrazione del regolamento interno: sfidare i divieti per accedere ai tunnel sotterranei come scorciatoie tra i padiglioni del campus (si parlava infatti di "*tunnel hacking*"). L'hacking rappresentava uno spirito goliardico per mostrare il proprio valore, penetrando in sistemi considerati inviolabili.

Ancora oggi, nell'immaginario collettivo e in tutti i film di genere, l'hacker è visto come un giovane, con la felpa scura e il cappuccio, chino sulla tastiera: il classico "nerd" [Vedi Figura 5].

Dimentichiamoci questa figura, perché non esiste più!

Gli hacker "lupi solitari" che abbiamo conosciuto agli albori dell'informatica di massa, gli "smanettoni" che hackeravano per divertimento o per ribellione, che ci inviavano virus più naïf che dannosi, oggi sono stati sostituiti da una struttura organizzata come un'azienda, con ruoli e funzioni precise.

E con il preciso obiettivo di fare soldi e rubare dati. Laddove un business si dimostra remunerativo, chi lo pratica cercherà di ampliarlo, per accrescere i propri guadagni. Questo succede in un'azienda, ma lo stesso sta accadendo nelle "cybercrime S.p.A.".

1.5 Cybercrime S.p.A.

Quella che Alessio L.R. Pennasilico ha definito, con un'immagine estremamente efficace, la **Cybercrime S.p.A.** [Vedi Figura 6] è una vera e propria organizzazione aziendale con finalità cybercriminali. Il "modello organizzativo" rappresentato nello schema che segue risulta particolarmente usato (ed efficace!) per il cybercrime nel settore finanziario.

Affinché una frode produca un ritorno economico servono una serie di elementi. Anzitutto la capacità tecnologica di costruire e mantenere un malware di alto livello; quindi, l'hacker con la felpa ed il cappuccio esiste ancora, ma è solo il componente di una filiera di produzione più complessa. Servono poi le competenze tecniche per aggiornare il malware ogni qualvolta viene identificato dai prodotti di protezione esistenti (antimalware, ecc.). Gli attacchi richiedono poi la conoscenza accurata dell'interfaccia o dell'applicazione da attaccare e una localizzazione perfetta nelle lingue del soggetto attaccato. Servirà poi confezionare attacchi (in genere con e-mail o messaggi) che risultino credibili ed accattivanti: ecco allora che nella cybercrime S.p.A. compare anche la figura dello psicologo. Per questo gli attacchi che riceviamo attraverso e-mail di phishing sono sempre meno rudimentali, anzi spesso queste e-mail risultano difficilmente

distinguibili da quelle vere! La leggenda del "cattivo italiano" ormai non è più credibile.

Infine, per ogni attacco che ha avuto successo, occorre una rete che sia in grado di riciclare e ripulire le somme frodate, fino a farne perdere le tracce. E quindi entrano in campo gli esperti di finanza.

1.6 La Cybersecurity riguarda tutti

Per quanto abbiamo raccontato e davanti ai numeri presentati ci rendiamo conto che le minacce cyber non possono certamente essere affrontate rinunciando alle potenzialità offerte dai sistemi informatici e dalla loro interconnessione in rete, perdendo quindi l'aumento della produttività ed efficienza che l'informatizzazione porta con sé, così come nessuno penserebbe di rinunciare all'uso dell'automobile solo perché ci sono gli incidenti.

Dobbiamo semplicemente:

- acquisire la consapevolezza dei rischi
- adottare le dovute precauzioni e misure preventive
- e, soprattutto, "usare la testa".

Da questo contesto, che negli ultimi anni si è assai ampliato, nasce quindi e diventa sempre più importante la sicurezza informatica o – come si dice oggi – la cybersecurity.

FAQ ▶ CHE COSA È LA CYBERSECURITY?

È costituita da attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale".

Lo scopo complessivo di questo insieme di discipline è proteggere tutti quegli asset materiali e immateriali che possono essere aggrediti tramite il "cyberspazio", ovvero che dipendono da esso, garantendo allo stesso

tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale a supporto.
Un aspetto molto importante della cybersecurity è il **concetto della trasversalità aziendale**: non deve essere considerata una competenza settoriale in carico all'ICT. È invece qualcosa che attraversa trasversalmente l'intera azienda e deve, come detto sopra, "superare i silos organizzativi". La cybersecurity riguarda tutta l'azienda, nessuno escluso, perché tutti hanno un computer, uno smartphone, una connessione internet.
E tutti sono un potenziale bersaglio per il cybercrime...

---

[1] Salvatore Rossi in "Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass", a cura del Gruppo di coordinamento sulla sicurezza cibernetica (GCSC), Banca d'Italia e Ivass, 2018.

[2] http://www.pwsinger.com/biography.html

[3] https://www.idc.com

[4] https://www.juniperresearch.com/home

[5] https://clusit.it

[6] Riccardo Luna "Così ho regalato il web al mondo", Intervista a Tim Berners-Lee, "la Repubblica", 14 novembre 2011
http://www.repubblica.it/tecnologia/2011/11/14/news/intervista_berners_lee-24969134/

[7] https://clusit.it/mese-europeo-della-sicurezza-informatica-ottobre-2018/

2

Deep web e Dark web

2.1 Che cosa sono il Deep web e il Dark web

Non si può trattare di cybercrime senza menzionare il Dark web, perché esso rappresenta l'ecosistema all'interno del quale si annida questa criminalità.

Si sente sempre più spesso parlare di Dark web, talvolta confondendolo con il Deep web. Ma si tratta di due mondi diversi. Cerchiamo quindi di capire cosa sono.

Con il termine **Deep web** si indica l'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (ad es. Google, Bing). Non si tratta di pagine clandestine o illegali, ma semplicemente di applicazioni web o pagine private aziendali, archivi legali o scientifici, pagine web dinamiche (il cui contenuto viene generato sul momento dal server), pagine non collegate a nessun'altra pagina web, pagine private ad accesso ristretto (a cui per accedere è necessario autenticarsi o fare il login). Non troveremo mai questi contenuti tramite Google, ma conoscendone l'indirizzo vi si può accedere con un normale browser.

L'opposto del **Deep web** si chiama **Surface web** (o Visible web o Indexed web): è quello che noi tutti navighiamo con i normali browser.

Quanto è grande il Deep web?

Difficile saperlo, ma si ritiene che il Surface web rappresenti meno del 5% di tutto il web. Tenuto conto che le pagine indicizzate da Google nel 2014 erano 30.000 miliardi, per un totale di dati indicizzati di oltre 100.000.000 GB (dati ricavato da www.statisticbrain.com), per avere la dimensione del Deep web dobbiamo probabilmente moltiplicare questi numeri per 50-100 volte.

Il **Dark web** [Vedi Figura 7] è solo un sottoinsieme, una piccola frazione del Deep web: rappresenta l'insieme di contenuti ospitati in siti web il cui indirizzo IP è nascosto, ma ai quali si può accedere qualora se ne conosca l'indirizzo.

Secondo ricerche fatte (non semplici, trattandosi di un mondo sommerso e clandestino) si ritiene che il Dark web possa contenere solo qualche decina di migliaia di indirizzi Url (tra 50 e 100.000, non oltre).

Appartengono al Dark web anche i contenuti privati scambiati tra utenti all'interno di un network chiuso di computer, ossia le strutture definite **darknet**. Qui si trova la parte più "oscura" della rete, quella che ospita anche i blackmarket, dove si trova di tutto: dalle droghe alle armi, dai killer ai documenti falsi.
Tra le darknet abbiamo:

- TOR (The Onion Router),
- The Invisible Internet Project[8] (I2P),
- Freenet[9]
- anoNet.

TOR è la più diffusa tra le darknet. È stata creata negli anni '90 nei laboratori della Marina Militare USA, nel 2006 è stata resa di pubblico dominio ed è oggi gestita da Tor Project[10], un'associazione non-profit con sede negli Stati Uniti.

Esistono altre **reti segrete governative e militari**, quali: SIPRNet (Secure Internet Protocol Router Network), NIPRNet (Nonclassified Sensitive Internet Protocol Router Network), JWICS (Joint Worldwide Intelligence Communications System), CRONOS (Crisis Response Operations In NATO Operating Systems) della NATO. Sono reti introvabili e inaccessibili, ma in realtà anche questi network segretissimi hanno subito attacchi e violazioni, a riprova che nel web tutto può essere attaccato.

2.2 Come funziona TOR

L'infrastruttura TOR è costituita da circa 6.000 server (volontari) in tutto il mondo e si compone di pagine con un dominio .onion alle quali si può accedere solo con il browser TOR, scaricabile da https://www.torproject.org. Non è possibile utilizzare i browser abituali: digitando un qualunque dominio .onion nella barra degli indirizzi di un normale browser (Google Chrome, Safari o Firefox), il sito corrispondente non risulterà raggiungibile.

La rete TOR è considerata il miglior standard esistente per navigare o comunicare in modo anonimo ed è utile anche per superare le censure internet in molti paesi non democratici.

Infatti sul sito di Tor Project è scritto che Tor difende la privacy e la sicurezza. Ed è vero, ma siccome "non è ancora stata inventata una pistola che spara solo ai cattivi", questa rete viene utilizzata anche da organizzazioni dedite al crimine informatico, proprio perché garantisce una navigazione in totale anonimato.

Usare TOR non è difficile. È necessario innanzitutto installare il browser TOR (che è una versione derivata da Firefox) dal sito https://www.torproject.org/download/download-easy.html.en.

Poi basta digitare l'url al quale si vuole accedere (e può essere anche un normale sito del Surface web, come fa la maggior parte degli utenti TOR).

I dati di navigazione non transitano direttamente dal client al server, ma passano attraverso i server Tor che agiscono da router, costruendo un circuito virtuale crittografato a strati (come una "cipolla", da cui il nome Onion) [Vedi Figura 8].

Quando si avvia la navigazione aprendo il browser TOR, questo sceglie dall'elenco "directory server" una lista di nodi e da queste individua 3 nodi (3 è la configurazione standard) in modo casuale, che costituiscono una catena di navigazione. In ciascun passaggio la comunicazione viene crittografata e questo si ripete per ciascun nodo (a strati come la cipolla). Ogni nodo della rete conosce solo il precedente e il successivo, nessun altro. Questo rende pressoché impossibile – o comunque molto complicato – risalire al client di partenza. Per contro, la navigazione risulta molto più lenta, proprio per il percorso che viene fatto.

Esistono anche dei motori di ricerca ad hoc per trovare contenuti, come Onion.City, Onion.to, Not Evil, Onion Web Search e Torch.

2.3 I black market del Dark web

Attraverso TOR si arriva ai black market della rete oscura, dove si possono acquistare droga, armi, documenti falsi e altri oggetti illegali. Sotto la superficie del web si può trovare realmente di tutto: dai siti pedopornografici, a quelli dove si ingaggiano sicari per commissionare omicidi.

Secondo le indagini del Nucleo Speciale di Frodi Tecnologiche della Guardia di Finanza, nel Dark web italiano è possibile reperire per il 60% sostanze stupefacenti, per il resto armi di ogni tipo, documenti falsi o rubati e servizi illegali di virus informatici per effettuare cyber attacchi.

E il volume d'affari è impressionante: 35 dei principali black market riescono a gestire transazioni per un ammontare che oscilla dai 300.000 $ ai 500.000 $ al giorno.

Circa il 70% di tutti i venditori si limita alla vendita di prodotti per un ammontare complessivo inferiore ai 1.000 $, un altro 18% dei venditori realizza vendite tra i 1.000 $ e i 10.000 $, solo il 2% dei produttori è riuscito a vendere più di 100.000 $.

Ci troviamo dinanzi a una economia in espansione, considerando che il popolare – e famigerato – black market **Silk Road** nel 2012 aveva un giro di affari annuo di circa 22 milioni di dollari (Studio Carnegie Mellon University 2012). Oggi Silk Road è chiuso ed il suo creatore Ross Ulbricht (pseudonimo Dread Pirate Roberts) è stato condannato nel 2015 al carcere a vita.

Scomparso Silk Road, sono comparsi al suo posto altri black market:

- **AlphaBay**, nato a fine 2014 e divenuto in poco tempo il principale sito dove avveniva la compravendita di droghe, ma anche di software malevoli, carte di credito e, in misura minore, armi; nel 2017 è stato chiuso da FBI, che ha fatto arrestare in Thailandia il fondatore Alexandre Cazes (canadese di 26 anni) che poco dopo si è suicidato in carcere
- **Hansa Market**, smantellato nel 2017 con una delle più brillanti operazioni di polizia nel mondo delle darknet, coordinata da FBI, Politie (la polizia olandese) ed Europol.

Questo dimostra che in questa continua guerra tra "guardie e ladri" qualche volta vincono anche le guardie... Ma nuovi blackmarket continuano a spuntare come funghi, come Wall Street Market e Traderoute.

2.4 Le criptovalute e il Bitcoin

Come la rete TOR viene utilizzata dal cybercrime perché può garantire l'anonimato, per lo stesso motivo il crimine informatico fa uso delle criptovalute, che sono comparse da meno di dieci anni.

Tutto è cominciato il 31 ottobre 2008, quando fu pubblicato il white paper "**Bitcoin: A Peer-to-Peer Electronic Cash System**"[11], scritto da un certo Satoshi Nakamoto[12], che enunciava un sistema "peer-to-peer di denaro elettronico per spedire direttamente pagamenti online da un'entità ad un'altra senza passare tramite un'istituzione finanziaria". Il sistema sfruttava la blockchain (catena di blocchi protetta da crittografia), che già esisteva[13]. Nessuno sa chi sia Satoshi Nakamoto e chi si celi dietro questo nome, ma quel giorno era nato il Bitcoin.

Oggi, nel 2018, le criptovalute si sono moltiplicate: al 26 agosto 2018 ce ne sono 2.194, per una capitalizzazione complessiva di oltre 215 miliardi di dollari, di cui 115 miliardi di dollari sono Bitcoin (fonte: Investing.com[14]). Elenchiamo le più importanti, cioè quelle aventi il maggior market cap (il valore circolante) con indicato l'anno di nascita:

- Bitcoin (BTC) (2009)
- Ethereum (Ξ) (2015)
- Ripple XRP (2012)
- Litecoin (Ł) (2013)
- Monero (XRM) (2014)
- Feathercoin (FTC) (2015)

Vediamo ora, in sintesi, come funzionano le criptovalute:

- Sono **valute digitali**, non fisiche, che utilizzano **sistemi di tipo peer-to-peer** (P2P), ossia sistemi paritari, senza un server centrale, in cui le transazioni sono validate dai nodi "paritari" (peer). Questi sistemi rendono le transazioni molto sicure, ma anche assai "macchinose", perché ciascuna richiede l'intervento di tutti i nodi che partecipano alla blockchain. Proprio per questo motivo, la blockchain permette il processamento di un massimo teorico di 7 transazioni al secondo. Se si considera che il solo circuito Visa viaggia sulle migliaia di

transazioni al secondo, ci si rende conto di come il Bitcoin fatichi a essere considerato un mezzo di pagamento pratico (se non cambierà qualcosa). Alla fine del 2017, quando il Bitcoin ha avuto una crescita clamorosa, arrivando fino a quasi 20.000 dollari, la maggior parte delle nuove transazioni richiedeva più di una settimana per essere confermata, il che rappresenta un tempo insostenibile per un sistema di pagamento. Quindi, per il momento, il Bitcoin si è ridotto a essere solo un investimento.

- Il sistema è totalmente orizzontale: non c'è un unico controllore centralizzato, le criptovalute non sono né generate né controllate da un'autorità o banca centrale. Non essendoci un'"autorità" nel Bitcoin, nessuno può cancellare una transazione già confermata.
- Le criptovalute non sono quotate nei listini delle Borse, ma hanno loro quotazioni "semiufficiali" indicate dalle società (Exchange) che le trattano.
- Vengono generate con complessi algoritmi crittografici regolati dal meccanismo della blockchain. Quelli che li generano sono definiti "miner" (minatori). Per le regole stabilite dalla blockchain dei Bitcoin, il mining diventa sempre più difficile e oneroso, perché richiede computer molto potenti ed elevati costi di energia elettrica. Si stima che il consumo di elettricità per il mining abbia ormai superato la quantità annua di energia consumata da una nazione come l'Irlanda: 49 TWh.
- Si conservano in un "wallet" (borsellino elettronico), che ciascuno può avere nel proprio computer.
- Sono legali. Eventualmente potrebbe essere illegale l'uso che se ne fa (ma questo vale anche per le valute tradizionali).
- Si possono acquistare Bitcoin e li si può usare per fare pagamenti: sono accettati già in diversi siti di e-commerce. Anche in Italia si cominciano a trovare esercizi commerciali che li accettano, così come è possibile acquistare carte prepagate in Bitcoin. Per individuare gli esercizi che accettano Bitcoin, si può consultare il sito coinmap.org. La diffusione è ancora bassa, soprattutto a causa dei tempi delle transazioni, che – come spiegato – rendono la criptomoneta poco adatta agli acquisti.
- Le transazioni sono sempre tracciate, ma anonime. Non è pertanto possibile risalire al proprietario della criptovaluta (a meno che non sia lui a rendersi

noto), ma chiunque può vedere, per ogni singola transazione, quale indirizzo Bitcoin stia inviando i Bitcoin e quale indirizzo Bitcoin li stia ricevendo.

Elenchiamo infine alcune delle società che fanno Exchange, compravendita di criptovalute. Sono siti assolutamente legali che svolgono questa attività in modo lecito:

- https://www.bitfinex.com
- https://cex.io (Londra)
- https://www.bitboat.net/it (Italia)
- https://localbitcoins.com (Finlandia)
- https://www.coinbase.com

e molte altre migliaia...

2.4.1 Come vedere un conto Bitcoin

Abbiamo detto che tutte le transazioni in Bitcoin sono tracciate e pubbliche.

Vediamo come si può consultare un qualsiasi conto Bitcoin, prendendo a esempio uno dei wallet utilizzati per pagare i riscatti del ransomware WannaCry.

Il wallet è identificato da: *"12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"* [Vedi Figura 9].

Accedendo al sito: https://www.blockchain.com/ e andando al link: https://www.blockchain.com/btc/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw chiunque può vedere tutti i movimenti del conto. Ovviamente non potremo sapere chi è l'intestatario del conto, che rimane anonimo...

---

[8] https://geti2p.net/en/

[9] https://freenetproject.org

[10] https://www.torproject.org

[11] https://bitcoin.org/bitcoin.pdf

[12] https://it.wikipedia.org/wiki/Satoshi_Nakamoto

[13] Ne avevano scritto nel 1991 Stuart Haber e W. Scott Stornetta, *How to time-stamp a digital document*, in "Journal of Cryptology", 3/2, 1991, pp. 99-111.

[14] https://it.investing.com/crypto/currencies

3

Perché ci attaccano

Oggi tutti le informazioni (aziendali e non solo) sono digitalizzate. In molti casi non esiste neppure più l'archiviazione in forma cartacea. E visto che "i dati sono il petrolio del terzo millennio" (nella famosa e già citata definizione di Tim Berners-Lee) diventano essi stessi un asset strategico, da difendere (per l'organizzazione che viene attaccata) o da rubare (per l'attaccante). Chiunque riesca ad accedere illecitamente a un sistema informatico – che sia un semplice personal computer, piuttosto che una rete complessa – può vedere e controllare molti dati e ottenere vantaggi, economici e non solo.

FAQ ▶ COSA È UN CYBER ATTACCO?

Con il termine generico di **cyber attacco** (**o attacco informatico**) si intende un qualunque tipo di attacco che colpisce sistemi informativi, infrastrutture, reti di calcolatori e/o dispositivi elettronici personali tramite armi informatiche (malware) che in genere utilizzano la vulnerabilità dei sistemi informatici attaccati.
Il cyber attacco è generalmente finalizzato al furto, all'alterazione o alla distruzione di dati presenti nell'obiettivo violato. In altri casi mira allo spionaggio, attraverso l'installazione di programmi cosiddetti spyware.
L'attacco può essere volto addirittura al blocco delle infrastrutture di intere nazioni. In questo caso si parla di "cyberwarfare" (guerre cibernetiche) o cyberterrorismo, a seconda del contesto.

Le tecniche degli attacchi informatici sono molto diverse, a seconda dell'obiettivo e dello scopo. Le vedremo nei capitoli 6-12. I motivi possono essere svariati e le finalità differenti. Vediamoli in dettaglio.

1 Prendere il controllo di un sistema informatico, anche a scopo di sabotaggio

Come spiegheremo nel capitolo 9 "Gli attacchi ai sistemi industriali (ICS)", ci sono molti casi noti di attacchi a infrastrutture critiche, alcuni addirittura

condotti da uno stato contro un altro.

Più in generale, riuscire a penetrare un sistema e prenderne il controllo permette all'attaccante di sfruttare il sistema per compiere azioni fraudolente, in danno dell'attaccato.

2 Rubare informazioni, ad esempio segreti industriali o proprietà intellettuali, a scopo di spionaggio

Lo spionaggio industriale è sempre esistito, ma oggi viene praticato soprattutto nella modalità informatica. In alcuni casi viene realizzato introducendo all'interno del sistema attaccato programmi spia (i cosiddetti "spyware") che rimangono nascosti per il più lungo tempo possibile e inviano all'attaccante informazioni su quello che accade nei computer della vittima.

Gli spyware sono usati anche sui device mobili. Si parla in questo caso di "captatori informatici", impiegati anche dalle polizie per fare intercettazioni telefoniche. Ne parleremo nel capitolo 10 "Malware su dispositivi mobili".

▶ UN CASO REALE – E MOLTO SERIO – DI SPIONAGGIO

Alcuni anni fa gli hacker cinesi, al servizio dell'Esercito popolare di Pechino, avrebbero violato la società britannica BAE, impegnata nel progetto del jet F-35, l'innovativo caccia sviluppato dagli USA assieme ad alcuni paesi europei (Italia compresa). In precedenza, sembra che gli hacker cinesi (probabilmente gli stessi) avessero sottratto anche progetti relativi ad altri aerei quali il B-2 ed il supercaccia F-22 Raptor. Le prove di questo spionaggio? Poco tempo dopo la Cina ha presentato il suo cacciabombardiere J-20, che aveva molte e sospette somiglianze con il Raptor.

3 Disturbare il buon funzionamento di un servizio

Limitare o bloccare il sistema informatico (o il sito web) di un'azienda potrebbe portare vantaggi all'attaccante che ne ha preso il controllo per danneggiare il concorrente o avversario, oppure più semplicemente per estorcergli denaro.

Gli attacchi DoS e DDoS ne sono un tipico esempio: un DoS (**Denial of Service**) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio; il DDoS (**Distributed Denial of Service**) è lo stesso tipo di attacco ma

distribuito su molti computer attaccanti per amplificarne l'effetto. Ne parleremo più in dettaglio nel capitolo 8 "Le tecniche di attacco più sofisticate".

4 Procurarsi informazioni personali su un utente: il furto di credenziali

Accedere all'account personale o aziendale di un utente significa entrare in possesso dei suoi dati (le sue credenziali) al fine di utilizzarli per azioni illecite. Questo può arrivare sino al "furto (o usurpazione) di identità".

5 Furto di dati bancari

Si tratta sempre di furto di credenziali e di dati personali, ma in questo caso lo scopo è quello di sottrarre denaro.

Il cybercrime mira soprattutto a "fare soldi" e proprio per questo le banche sono sempre state tra gli obiettivi più colpiti, essendo il settore potenzialmente più remunerativo. Di solito l'attaccante mira a convincere la vittima – con tecniche di phishing attraverso e-mail (v. cap. 6 "Il social engineering, il phishing e gli attacchi attraverso la posta elettronica") – a dargli le sue credenziali bancarie (username + password) così da accedere al conto e compiere operazioni per rubargli denaro.

Secondo le statistiche di Kaspersky, nel 2017 le banche sono state oggetto del 27% degli attacchi di phishing, i sistemi di pagamento online del 15,87%, mentre i negozi online del 10,95%.

6 Utilizzare le risorse del sistema dell'utente

Una volta che l'attaccante è riuscito a entrare nel sistema della vittima, può prenderne il controllo per usarlo in molti modi.

Ad esempio lo può trasformare in un suo "servitore" (tecnicamente si parla di computer "zombie") e utilizzarlo per indirizzare traffico dati verso un altro bersaglio allo scopo di bloccarlo: è l'attacco DoS o DDoS.

Oppure può utilizzare una parte della potenza di calcolo del computer attaccato per generare criptovalute come il Bitcoin (il cosiddetto "mining"). Questo tipo di attacco viene realizzato attraverso un malware scaricato inconsapevolmente dall'utente attaccato (magari assieme a programmi gratuiti, dei quali dobbiamo

sempre diffidare!). In genere l'utente non se ne rende neppure conto, salvo notare un rallentamento del proprio dispositivo. Questo attacco è definito "Cryptojacking" (v. Glossario) ed è in crescita esponenziale, di pari passo con la crescita delle criptovalute. Si stima che nei primi tre mesi del 2018 sia aumentato del 600% rispetto all'anno precedente.

7 Alterare o prendere il controllo del sito web di un'azienda o di un'organizzazione

Questa tecnica d'attacco può essere usata per diverse finalità:

- **Per trasmettere messaggi attraverso il "defacement" del sito**: il "defacciamento" consiste nella sostituzione di una pagina – in genere l'home page – con un'altra, mediante la quale l'attaccante trasmette un messaggio (politico o altro).
- **Per metterlo offline**: questo obiettivo si realizza per esempio attraverso l'attacco DDoS (Distributed Denial of Service) che "spara" contro il sito un volume di traffico maggiore della banda disponibile in modo da saturarne le risorse e farlo "andare giù" (si usa questo termine per indicare un sito che non risulta accessibile).
- **Per inviare spam, per distribuire malware, per inserirvi pagine di phishing o per reindirizzare a siti malevoli**: il sito viene usato per lanciare attacchi ad altri obiettivi sfruttando la buona reputazione del sito stesso, ritenuto attendibile dai principali motori online che gestiscono le blacklist. Gli attacchi veicolati da un sito "in whitelist" non saranno bloccati fino a che lo stesso sito non sarà "bollato" come sito di spam e inserito nelle blacklist. A quel punto, neppure il legittimo proprietario riuscirà più a utilizzarlo!
- **Per rubare i dati:** questa è – ovviamente – una delle finalità principali, come già spiegato in precedenza.

FAQ ▶ COSA SONO LE BLACKLIST DEI DOMINI?

Le **blacklist o** anche "**block list**" sono liste di indirizzi IP mantenute aggiornate e rese disponibili da una serie di server consultabili da chiunque (tra questi anche Google), in cui vengono elencati gli indirizzi IP ritenuti fonte di spam. Le blacklist sono un sistema per combattere lo

spam e sono utilizzate da molti software antispam. Le e-mail inviate dal sito verranno rifiutate dai principali servizi di posta dotati di sistemi antispam correttamente configurati e al mittente verrà restituito un messaggio simile a questo:
"*The following addresses had permanent fatal errors reason: mail not accepted from blacklisted* IP *address" (I seguenti indirizzi hanno avuto errori irreversibili permanenti: mail non accettate dall'indirizzo* IP *nella blacklist)*
Si finisce in blacklist anche qualora si venga identificati da Google come "siti compromessi" con la conseguente segnalazione nei risultati del motore di ricerca.
Un sito in blacklist avrà la sua operatività estremamente ridotta (se non completamente bloccata) e a quel punto si dovranno attivare azioni di "recupero" attraverso il provider che fornisce il servizio web.

FAQ ▶ COME VERIFICARE SE SIAMO FINITI IN BLACKLIST

Esistono alcuni siti che gestiscono le blacklist e che possiamo interrogare inserendo l'indirizzo IP da verificare:

- The Spamhaus Project: https://www.spamhaus.org/lookup/
- Barracuda Central: http://www.barracudacentral.org/lookups
- Blacklistalert.org: http://www.blacklistalert.org/ che verifica l'IP su circa quaranta blacklist

4

I rischi per le aziende

4.1 Quali sono i rischi più diffusi?

La cybersecurity riguarda qualsiasi organizzazione e qualsiasi persona, anche il privato cittadino, perché, a prescindere dal settore di attività, tutti utilizziamo computer, server, sistemi di posta elettronica, dispositivi mobili (notebook, tablet e smartphone): ognuno di questi rappresenta una porta attraverso cui le minacce possono introdursi e causare danni.
Le **minacce** che possono danneggiare o bloccare il sistema informativo di un'azienda o di un'organizzazione sono principalmente le seguenti:

- l'**errore umano** che apre la strada a virus e malware
- l'**evento accidentale** che compromette il sistema informativo (es. sbalzo di tensione, incendio, ecc.)
- l'**azione dolosa di terzi** (es. furto di informazioni e dati da parte di interni o esterni, attacco hacker, furto dei computer, ecc.).

4.2 Quali sono i principali danni che un cyber attacco può causare a un'azienda?

I danni che possono compromettere l'operatività aziendale (la business continuity) o addirittura mettere a rischio l'esistenza stessa dell'azienda (ma anche di un'organizzazione non profit) possono essere di diversi tipi, ma tutti ugualmente temibili:

- **Danni diretti e materiali ai sistemi elettronici e informatici**: ad esempio, in caso di danneggiamento del server potrebbe rendersi necessario un intervento tecnico per la sua riparazione o sostituzione. Il costo dell'intervento, delle licenze software, del ripristino dei dati, della pulizia dai malware, del nuovo server, sono tutte voci di spesa che incidono sul bilancio aziendale.

- **Interruzione delle attività**: in caso di cyber attacco al sistema informatico, potrebbero essere rallentate o bloccate le funzioni e le attività dell'azienda (magazzino, produzione, gestione dei clienti e fornitori, ecc.). L'interruzione o il rallentamento delle attività rappresenta una perdita economica per l'azienda (mancato fatturato).
- **Furto o manomissione di dati, informazioni o progetti strategici per l'azienda**: in questo caso si parla di furto di proprietà intellettuale, che può avere un impatto molto serio per aziende tecnologicamente avanzate, non solo in ambito IT.
- **Furto di denaro:** esecuzione di pagamenti o distrazione di denaro per via informatica. È il caso della Business Email Compromise (BEC), di cui parleremo in seguito (v. cap. 6 "Il social engineering, il phishing e gli attacchi attraverso la posta elettronica").
- **Danni legali e/o richieste di risarcimento danni da parte di terzi**: ad esempio, nel caso di perdita o sottrazione di dati sensibili o riservati, i titolari dei dati potrebbero richiedere un risarcimento sulla base di un danno da loro subito (è il caso previsto nel GDPR).
- **Danno reputazionale e perdita di clienti e fornitori**: nel caso di disservizi o di perdita di dati importanti si potrebbe verificare un deterioramento delle relazioni con i clienti, fornitori, finanziatori, ecc., con un impatto negativo di difficile quantificazione.

4.3 Il danno reputazionale

Nelle aziende di grandi dimensioni e che hanno un'immagine pubblica molto esposta, il danno più temuto è quello reputazionale. Pensiamo alle società delle comunicazioni, del mass market e soprattutto alle banche: sono in genere aziende con un'organizzazione che è in grado di porre rimedio ad un cyber attacco, essendosi dotate (si spera!) di un Disaster Recovery Plan (DRP) per garantire la "business continuity".

Ma può essere ben più complicato rimediare al danno della reputazione aziendale.

Per una banca, per esempio, potrebbe non bastare il recupero dei file persi per un cyber attacco (e sicuramente reperibili in un backup). Il vero problema sarà di

convincere i propri clienti che l'azienda non corre rischi, che il sito è sicuro, che chi deposita denaro in quella banca non rischia di farselo rubare...
Il web di oggi ha alcune caratteristiche, per altri versi utili, che lo rendono uno strumento con una potenza devastante e difficilmente controllabile:

- è **scalabile**: si può diffondere all'infinito
- è **persistente**: nulla viene perso
- è **replicabile**: di ogni cosa di può fare copia e condivisione
- è **ricercabile**: tutto può essere indicizzato e trovato.

Quindi sarà di vitale importanza arginare sul nascere qualsiasi rischio reputazionale, nella consapevolezza che chi attacca una banca o una grande società potrebbe mirare proprio a quello, anche per scopi di ricatto ed estorsione.
Vediamo ora alcuni casi famosi di grandi società, che a causa di un attacco informatico hanno subito un danno d'immagine che le ha pesantemente danneggiate.

4.3.1 Il data breach di Yahoo!

Una delle aziende storiche del web si è dimostrata poco attenta alla sicurezza e ancor meno alla gestione della crisi conseguente all'attacco, addirittura cercando di tenere nascosta la violazione per lungo tempo, fino a quando i dati non sono stati messi in vendita nel Dark web.
Nel 2013 Yahoo! [Vedi Figura 10] subì un data breach (violazione dei dati personali) importante. Quanto importante? Si parlò in un primo tempo di circa 500 milioni di account rubati. Nel 2016 però il Chief Information Security Officer (CISO) del gruppo, Bob Lord, ha comunicato che in quell'attacco risalente al 2013 sarebbero stati rubati i dati di un miliardo di utenti: il data breach più grande della storia. Tra le informazioni trafugate nomi, indirizzi e-mail, numeri di telefono, date di nascita, password crittografate con hashing e, in certi casi, domande di sicurezza con le relative risposte.
La notizia è venuta fuori durante la trattativa di acquisizione di Yahoo! da parte di Verizon ed ha messo a serio rischio la conclusione dell'accordo. La telco statunitense, che aveva offerto 4,8 miliardi di dollari per rilevare Yahoo!, ha

preteso un consistente sconto, proprio a causa dell'incidente e del danno reputazionale subito da Yahoo!

La transazione si è poi conclusa con un abbassamento del prezzo pagato da Verizon (si parla di uno "sconto" di almeno 500 milioni di dollari!), ma gli effetti del data breach non erano ancora finiti, tutt'altro.

Nel 2017, durante il processo di fusione con AOL, per creare la nuova compagnia Oath, nella quale Verizon ha fatto confluire Yahoo!, quest'ultima ha dovuto ammettere che la cifra ufficiale comunicata precedentemente (1 miliardo di account violati) non era veritiera: pare che siano almeno 3 miliardi le persone realmente coinvolte nel data breach del 2013. In pratica, tutti gli utenti iscritti alla piattaforma!

La società ha invitato – ma lo ha fatto con anni di ritardo – tutti gli utenti a modificare le password e ha invalidato le domande di sicurezza non crittografate. Ovviamente la CEO Marissa Meyer è stata rimossa.

Per quello che era stato il primo portale di rilievo della storia del web (nato nel 1994, ben prima di Google) non si poteva di certo immaginare una fine così ingloriosa...

4.3.2 Un danno reputazionale devastante: il caso Equifax

Tra i tanti casi accaduti di recente, quello di Equifax rappresenta uno dei più famosi e devastanti per l'impatto reputazionale che ha comportato.

Equifax[15] è una azienda con sede ad Atlanta (Georgia), quotata al NYSE (New York Stock Exchange) e con un fatturato di oltre 3 miliardi di dollari nel 2017.

È una delle tre società che in USA gestisce il "credit rating", assegnando ad ogni cliente un "credit score" per accedere al credito. In pratica è una delle più grandi agenzie di valutazione del credito al mondo insieme a Experian e TransUnion.

Il caso Equifax scoppia il 7 settembre 2017, quando la società ufficializza il fatto di aver subito un attacco informatico fra maggio e luglio. In questo clamoroso data breach sono stati rubati dati che includono principalmente nomi, date di nascita, indirizzi, numeri delle patenti di guida e social security number di ben 143 milioni di persone, quasi la metà della popolazione degli Stati Uniti. Soprattutto il "social security number" è un dato molto delicato, perché è un

codice assegnato a vita a ogni cittadino USA, utilizzato come strumento di identificazione univoca delle persone fisiche, tramite il quale si può accedere a molteplici servizi governativi o offerti da privati (ad esempio, chiedere un mutuo). È perciò molto più riservato del nostro codice fiscale, per esempio, e deve assolutamente rimanere segreto.

Non solo, si scopre che ciò è accaduto a causa della vulnerabilità di un programma software usato dall'azienda. Più tardi si sarebbe palesato anche un altro aspetto incredibile in questa vicenda già sconcertante: il portale argentino di Equifax usava l'imbarazzante "admin/admin" come username e password!

Ma l'azienda, che ne era venuta al corrente il 29 luglio, ha dato la notizia solo il 7 settembre. Perché? Forse perché nel frattempo alcuni dirigenti Equifax hanno venduto le proprie quote azionarie della società, per un valore complessivo di 1,8 milioni di dollari (pari a circa 1,5 milioni di euro), evitando così le conseguenze del prevedibile crollo in borsa.

Il danno reputazionale e finanziario per Equifax è stato devastante: l'azienda ha perso in una sola settimana il 35% del valore in borsa, passando da 141,59 a 92,98 USD.

Il 15 settembre 2017 si dimettono il Chief Information Officer e il Chief Security Officer. Il 26 settembre 2017 è costretto a lasciare anche il Chief Executive Officer, non solo per il pauroso data breach, ma anche per la pessima gestione dell'incidente.

Tutto questo in una società ritenuta all'avanguardia e che gestiva dati personali molto delicati dei cittadini americani.

Proviamo a immaginare un incidente del genere oggi, in vigenza del GDPR (Regolamento Europeo sulla Privacy), che prevede sanzioni fino al 4% del fatturato aziendale!

4.4 Il pericolo arriva soprattutto dall'interno

Esaminiamo ora un altro aspetto critico e in genere assai sottovalutato, perché frutto di un "cambio di scenario" che tanti non hanno ancora compreso.

Un tempo si considerava il concetto di rete aziendale isolata, cioè connessa solo in pochi punti al web.
Nelle aziende di oggi, invece, non esiste più il "perimetro da difendere" con i dipendenti "dentro" e gli attaccanti "fuori" (dentro=buoni, fuori=cattivi), come eravamo abituati a considerare fino a qualche anno fa. Ora tutto è cambiato perché:

- i social network sono esterni al perimetro aziendale
- si lavora in mobilità e i devices mobili sono esterni al perimetro aziendale
- i dati sono salvati sul cloud e su server esterni.

Oggi dunque non è più individuabile un "perimetro aziendale" e questo ci obbliga a ripensare alle nostre tecniche di cyber difesa.

Il "teorema del Fortino", come lo ha definito Corrado Giustozzi[16] (membro ENISA e CLUSIT), quello che dice "costruisco degli alti muri intorno a me e questo basta per proteggermi", ormai non è più valido. Si parla per questo di "**deperimetralizzazione**".
E questo soprattutto ci deve far considerare il rischio generato dall'utente interno [Vedi Figura 11] (mentre prima ci si preoccupava solo dell'attacco dall'esterno), che addirittura è superiore a quello che arriva dall'esterno. Possiamo suddividere l'attaccante interno in tre categorie [Vedi Figura 12]:

1) Gli inconsapevoli o compromessi ("inadvertent actor"), che commettono errori o sono vittime di attacchi per la loro scarsa consapevolezza.
2) Gli accidentali, quelli che non rispettano le procedure di sicurezza e hanno un approccio "disinvolto" e poco attento quando utilizzano gli strumenti aziendali. Spesso sono gli utenti che si considerano evoluti, quindi "autorizzati" a eludere le policy di sicurezza stabilite dall'azienda e a installare in autonomia software e applicativi ritenuti migliori o più utili di quelli ufficiali messi a disposizione dall'azienda. Questo fenomeno si definisce "Shadow IT" ed è diffuso nelle aziende dove il controllo IT non è adeguato.
3) I fraudolenti o intenzionali ("malicious insiders"), che lo fanno per risentimento verso l'azienda o per rubare e vendere i dati aziendali.

Dobbiamo inoltre tener presente, a maggior ragione ora che l'Europa ha adottato il nuovo Regolamento sulla Privacy (GDPR), che i dati sono un patrimonio aziendale da proteggere.

Non dimentichiamo mai che **"nel momento in cui una persona ha la possibilità di accedere al dato, diventa un punto critico"**: qualcuno potrebbe indurre in tentazione la persona in possesso del dato, oppure potrebbe sferrare attacchi sempre più mirati a ingannarla sfruttando tecniche di social engineering e attuando ricatti e tentativi di corruzione.

Ritorneremo su questo argomento, quando tratteremo il principio del minimo privilegio nella gestione degli accessi ai dati aziendali.

4.5 La mitigazione del rischio

Nella cybersecurity non è possibile arrivare al rischio zero. E se mai fosse possibile azzerare il rischio, questo comporterebbe un costo insostenibile (e incompatibile con un corretto rapporto costi/benefici).

Estremizzando, si può affermare che un attaccante che abbia a disposizione tempo infinito e risorse illimitate, prima o poi riuscirà ad avere successo. Starà a noi attivare le misure difensive per rendere l'attacco troppo oneroso e quindi non conveniente.

Si parla perciò di **mitigazione del rischio**, un processo che deve sempre partire dall'analisi dei rischi potenziali, a cui dovrà seguire la definizione delle misure più idonee per ridurli a un livello sostenibile.

4.5.1 L'analisi del rischio informatico

Per fare questo, un'azienda deve preliminarmente valutare i seguenti aspetti:

- Quali sono i processi e i dati critici (quelli dei quali non può fare a meno)?
- Qual è il "rischio residuo", cioè quali e quanti dati si può permettere di perdere?
- In quanto tempo deve essere in grado di ripristinare i processi critici, per garantire la cosiddetta "business continuity"?

Analizzando i suoi dati l'azienda dovrà valutare i seguenti tre aspetti che devono essere salvaguardati dai cyber rischi [Vedi Figura 13]:

- **Integrità**: i dati non devono essere modificati o cancellati.
- **Confidenzialità (riservatezza)**: i dati devono essere accessibili solo da chi è stato autorizzato.
- **Disponibilità**: i dati devono sempre essere accessibili quando richiesto.

Vediamo in estrema sintesi come si applica l'analisi del rischio nell'ambito della sicurezza informatica, utilizzando i metodi stabiliti dalla normativa ISO/IEC 27001 "Sistemi di Gestione della Sicurezza delle Informazioni"[17].
Si adotta la metodologia tipica del "Risk Management", considerando le due principali dimensioni connesse al cybersecurity risk:

1. la probabilità di accadimento
2. l'intensità dell'impatto (o gravità).

Potranno esserci quindi rischi molto probabili, ma il cui impatto per l'azienda è basso o, viceversa, rischi molto improbabili, ma che potrebbero risultare molto gravi in caso di accadimento.
Si evince quindi che l'analisi del rischio è un modello di tipo probabilistico: il "**fattore di rischio**" è il risultato (quantificato) del prodotto di due fattori:

Fattore di Rischio = (Impatto) × (Probabilità) [Vedi Figura 14]

4.5.2 Il Risk Management

Individuati i principali fattori di rischio, si dovrà stabilire per ciascun rischio la corretta strategia di trattamento e, per ciascun rischio valutato come "non accettabile", le misure di sicurezza necessarie per limitarne gli effetti.
Le opzioni disponibili per ogni rischio analizzato sono:

- **Accettazione del rischio**: la decisione di conservazione del rischio senza intraprendere ulteriori azioni di mitigazione deve essere presa in base alla valutazione del rischio stesso e ai costi da sostenere per una sua riduzione.
- **Riduzione del rischio**: il livello di rischio deve essere ridotto attraverso interventi prestabiliti, in modo che il rischio residuo possa essere rivalutato come accettabile.
- **Prevenzione del rischio**: l'attività o la condizione che dà luogo al rischio deve

essere evitata e/o mitigata.

- **Trasferimento del rischio**: il rischio deve essere trasferito a terzi in grado di gestirlo più efficacemente, a seconda della valutazione del rischio stesso (p.es.: conservazioni dati in Cloud).

FAQ ▶ CHE COS'È IL "BLACK SWAN"?[18]

Nel trattare dell'analisi del rischio, non possiamo non citare il "Black Swan", il "**Cigno nero**", un concetto che la cybersecurity ha mutuato dall'economia.
Si definisce "Cigno nero" un evento isolato e inaspettato, che ha un impatto enorme, e che solo a posteriori può essere spiegato e reso prevedibile. In altre parole, un evento "a bassissima probabilità e ad altissimo potenziale di danno".
È impossibile che accada... ma se dovesse accadere sarebbe un disastro...
Black Swan è un attacco informatico che costringe un'azienda a chiudere.

Il Risk Management è una metodologia valida per qualsiasi azienda e per qualsiasi tipologia di rischio, ma risulta particolarmente importante laddove si debba considerare la sicurezza dei dati.

Oggi i dati hanno un valore economico reale, addirittura sono da considerare un asset strategico aziendale che andrebbe inserito in bilancio nello stato patrimoniale.

Il Risk Management è una disciplina sempre più di attualità, sulla quale esiste un'ampia letteratura. Cito in proposito l'importante testo di Ioannis Tsiouras, *Risk Management. La norma ISO 31000:2018 – La metodologia per applicare efficacemente il risk management in tutti i contesti.*

4.6 I falsi miti sul cyber risk

In conclusione dell'analisi del cyber rischio, è utile qui cercare di sfatare alcuni "miti" che, purtroppo, ancora oggi esistono e che portano molte aziende a sottovalutare pericolosamente il problema. Vediamoli in sintesi:

- **In Italia siamo al sicuro**: al contrario, l'Italia è uno dei Paesi più a rischio e le

perdite economiche dovute al verificarsi di attacchi cyber sono in continua crescita.

- **È un rischio che riguarda solo le grandi aziende:** le aziende più piccole (le PMI) sono le più vulnerabili, in quanto in genere gestiscono il rischio in maniera approssimativa e con budget limitati.
- **Perché dovrebbero attaccare proprio la mia azienda? Non abbiamo dati importanti:** per ogni azienda i propri dati sono importanti; ma soprattutto, nessuna azienda è completamente al sicuro, perché la maggior parte degli attacchi sono di tipo massivo e indifferenziato, perpetrati con la logica della "pesca a strascico": si lanciano attacchi di massa, con strumenti automatici, senza mirare a un obiettivo preciso, sapendo che comunque qualcuno – non importa chi – finirà nella rete. Pensare quindi di non essere un bersaglio appetibile significa non curare la sicurezza dei propri sistemi informatici e quindi diventare di fatto un bersaglio facile.
- **Non mi è mai successo, perché dovrebbe accadere proprio ora?**: non dobbiamo pensare "se accadrà", ma solo "quando accadrà". Quindi è vitale essere preparati e sapere cosa fare quando – prima o poi – accadrà. Nella cybersecurity la prevenzione può salvare l'azienda. E frasi del tipo "*Non mi è mai successo...*" oppure *"Abbiamo sempre fatto così..."* sono un modo suicida per affrontare rischi che si stanno evolvendo con una rapidità impressionante.

4.7 La Cybersecurity è un problema culturale

Tutto questo ci fa capire che la **cybersecurity è un problema più culturale che tecnico**.

Serve una formazione adeguata di base, per creare il concetto – culturale, non informatico – di "cyber hygiene", per imparare le best practices e fare in modo che queste entrino nelle nostre abitudini, per la sicurezza del nostro sistema informatico, aziendale o personale che sia.

Un programma di awareness (consapevolezza) sulla sicurezza informatica non è quindi solo "formazione", ma deve generare un circolo virtuoso che parta dalla "comprensione" dei rischi connessi all'utilizzo del sistema informativo e conduca i

suoi fruitori ad adottare comportamenti adeguati durante le attività lavorative quotidiane.
Prendiamo ad esempio le automobili, che noi tutti conosciamo ed usiamo: le auto di oggi hanno airbag, Abs, cinture e molti altri dispositivi di sicurezza. Tutto bene? Certo, ma se guido l'auto ubriaco, a fari spenti nel cuore della notte, mi farò molto male, comunque.
Chiedere ai tecnici informatici che non succeda "qualcosa", è come chiedere al meccanico che non ci succeda un incidente: al volante ci siamo noi...

"Se il problema della sicurezza fosse solo tecnologico, la tecnologia lo avrebbe già risolto".

Sarà lo scopo di questo libro insegnarci a riconoscere i rischi, capirli ed evitare di cadere nelle trappole – sempre più astute – che ci vengono tese.

---

[15] https://www.equifax.com/personal/

[16] https://www.enisa.europa.eu

[17] UNI CEI ISO/IEC 27001 "Sistemi di Gestione della Sicurezza delle Informazioni", marzo 2014

[18] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Penguin, London 2007; trad. it. *Il cigno nero. Come l'improbabile governa la nostra vita*, Il Saggiatore, Milano 2013

5

Cosa stanno facendo l'Europa e l'Italia

In un'intervista alla CNBC americana di febbraio 2018[19], il ministro della Difesa della Germania Ursula von der Leyen ha dichiarato che "gli attacchi informatici rappresentano la più grande sfida che minaccia la stabilità globale".
Quindi la consapevolezza del rischio informatico sta crescendo anche a livello istituzionale e i governi stanno iniziando ad agire.

L'**Agenzia ENISA (European Network and Information Security Agency)**[20] è stata creata già nel 2004 dall'UE, con sede in Grecia, e ha lo scopo di occuparsi della sicurezza delle informazioni e delle reti. Tra i suoi compiti principali vi è il supporto alla Commissione Europea, agli Stati Membri, alle istituzioni europee a alle aziende in materia di "sicurezza cibernetica europea". L'Italia è rappresentata da Rita Forsi (MISE), mentre nel Permanent Stakeholders Group di ENISA sono presenti Corrado Giustozzi (membro CLUSIT dal 2010) e Alessandro Menna.

Vediamo quali sono i provvedimenti che sono stati adottati di recente per la protezione di dati, reti e informazioni.

[Torna al capitolo] 5.1 La Direttiva NIS e i decreti che la recepiscono

Il 6 luglio 2016 il Parlamento UE ha emanato la **Direttiva (UE) 2016/1148**[21], nota come **Direttiva NIS (Network and Information System)** "recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (come recita il titolo), che delinea un primo sistema integrato e organico di norme in tema di cybersicurezza, secondo un principio di armonizzazione tra gli stati europei.

Il DPCM **del 17 febbraio 2017 (Decreto Gentiloni)**[22] e poi il **D. Lgs. n.65 del 18 maggio 2018**[23] recepiscono per l'Italia la Direttiva NIS [Vedi Figura 15].

Vengono stabilite le funzioni dei diversi attori preposti a gestire la cybersecurity in Italia e in coordinamento con l'Europa:

- **DIS (Dipartimento Informazioni per la Sicurezza):** è l'organismo centrale della sicurezza cibernetica con il compito di coordinare, sia a livello nazionale, sia in ambito UE, NATO, ONU e OCSE (Organizzazione per la sicurezza e la cooperazione in Europa), le questioni relative alla sicurezza delle reti e dei sistemi informativi. L'elemento di novità introdotto dal nuovo Decreto è nel ruolo sempre più centrale e preponderante che il Dipartimento delle Informazioni per la Sicurezza (DIS) acquisisce nel settore della sicurezza cibernetica: da oggi in poi vero e proprio braccio operativo sul piano strategico del Presidente del Consiglio, nonché collante tra il CISR, l'intera pubblica amministrazione e il settore privato.
- **CISR (Comitato Interministeriale per la Sicurezza della Repubblica):** è un organo istituzionale di raccordo politico-strategico sul tema della sicurezza nazionale, con compiti di consulenza, proposta e deliberazione.
- **CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche):** è l'unità specializzata, interna al Servizio della Polizia Postale e delle Comunicazioni, dedicata alla prevenzione e repressione dei crimini informatici diretti ai danni delle infrastrutture critiche nazionali.
- **Cert-N (Computer Emergency Response Team Nazionale):** struttura istituita presso il Ministero dello Sviluppo Economico e deputata a coordinare la risposta a incidenti informatici.
- **Cert-PA (Computer Emergency Response Team della Pubblica Amministrazione)**: opera all'interno dell'Agenzia per l'Italia Digitale (**AgID**), alla quale il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico ha affidato il compito di curare la sicurezza cibernetica delle pubbliche amministrazioni Italiane.
- **CSIRT (Computer Security Incident Response Team):** istituita presso il Consiglio dei Ministri, è la struttura incaricata di coordinare la risposta a incidenti informatici, a mitigarne gli effetti e a prevenire il verificarsi di ulteriori eventi.
- **NSC (Nucleo per la Sicurezza Cibernetica):** è un organo costituito presso il

DIS, per gli aspetti relativi alla prevenzione e preparazione a eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

5.2 Il Framework nazionale della Cybersicurezza

La sicurezza informatica di un'azienda può essere garantita se e solo se anche le altre aziende collegate e le infrastrutture sono a loro volta sicure. È un intero ecosistema da proteggere, perché interconnesso: l'errore di un singolo può creare ripercussioni sugli altri.

In questa logica è nato nel 2016 il Framework Nazionale per la Cyber Security[24], realizzato dal Research Center of Cyber Intelligence and Information Security (CIS) dell'Università La Sapienza di Roma (diretto dal Prof. Roberto Baldoni) assieme al Laboratorio Nazionale CINI (Consorzio Interuniversitario Nazionale per l'Informatica) di cybersecurity.

Il Quadro prende spunto dal *Framework for Improving Critical Infrastructure Cybersecurity*[25] del NIST (National Institute of Standards and Technology), ma si cala nella realtà italiana, fatta di piccole e medie imprese (ne tratta al Capitolo 6), nelle quali non esiste personale IT specifico, per questioni strutturali e di fatturato.

In molte di queste realtà i computer vengono usati in modo promiscuo (lavoro e tempo libero), i server risiedono in luoghi non protetti e neppure si sa quanti e quali computer possano connettersi alla rete e dove siano archiviati i dati aziendali.

L'innalzamento dei livelli di sicurezza delle PMI è un passaggio fondamentale per la messa in sicurezza anche delle aziende più grandi e di tutto il sistema-paese. In questo momento le PMI rappresentano, per il loro modo di operare, un rischio importante per le grandi aziende capi-filiera. Un numero sempre maggiore di attacchi a grandi società viene infatti realizzato grazie a vulnerabilità presenti nelle imprese che fanno parte della loro filiera. Ce lo insegnano casi recenti, come gli attacchi a Target, Sony e Unicredit, dove i cyber-criminali sono penetrati attraverso vulnerabilità delle aziende fornitrici.

Il Framework italiano introduce una cultura della gestione del rischio all'interno

dell'azienda per combattere la minaccia cyber *("cybersecurity risk management")*. Ne citiamo alcuni passaggi significativi:

> Gli attacchi informatici, cresciuti negli ultimi anni in modo esponenziale per complessità e risorse utilizzate, non possono essere fermati dalle singole organizzazioni, ma hanno bisogno di una risposta dal sistema paese, poiché tendono a diminuirne la prosperità economica e l'indipendenza. Il rischio cyber non può essere annullato ma è importante che una nazione sviluppata si doti di una serie di strumenti e metodologie per migliorare la consapevolezza, affrontare in modo strutturato la risposta e supportare le organizzazioni, gli enti e le organizzazioni pubbliche e private, residenti sul proprio territorio, per la riduzione del rischio e la mitigazione degli effetti di eventuali, possibili incidenti di sicurezza.
>
> Questo significa che il periodo in cui la sicurezza veniva gestita unicamente in outsourcing è definitivamente finito: ogni azienda deve necessariamente impiegare risorse umane interne a difesa dei propri asset aziendali.
>
> In questo documento viene proposto un Framework nazionale di cybersecurity con l'intento, innanzitutto, di costruire un linguaggio comune per confrontare le pratiche aziendali di prevenzione e contrasto dei rischi cyber. Il Framework può aiutare una impresa a organizzare un percorso di gestione del rischio cyber, sviluppato nel tempo, in funzione del suo business, della sua dimensione e di altri elementi caratterizzanti e specifici dell'impresa. L'adozione del Framework è pertanto su base volontaria.

Nel documento *2016 Italian Cybersecurity Report*[26] il Framework propone **15 controlli essenziali di cybersecurity,** dandone una guida di implementazione e una stima indicativa dei costi considerando due tipologie di imprese. Per "controllo essenziale" si intende una pratica relativa alla cybersecurity che, qualora ignorata oppure implementata in modo non appropriato, causa un **aumento considerevole del rischio informatico.**

Tale aumento del rischio implica che l'operatività, la riservatezza dei dati dell'organizzazione e la loro integrità potrebbero essere lese da attaccanti con una probabilità troppo alta per essere considerata accettabile. Di contro, la corretta implementazione di tutti i controlli di cybersecurity ritenuti essenziali ha, come immediata conseguenza, una riduzione importante, seppur non totale, del rischio.

5.2.1 I 15 controlli essenziali di Cybersecurity

Vediamo ora i 15 controlli, secondo la suddivisione per tipologie che propone il Framework:

Inventario dispositivi e software (3.1)

1. Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
2. I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
3. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
4. È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.

Governance (3.2)

5. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.

Protezione da malware (3.3)

6. Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, anti-malware, ecc.) regolarmente aggiornato.

Gestione password e account (3.4)

7. Le password sono diverse per ogni account, di complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
8. Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
9. Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza

Formazione e consapevolezza (3.5)

10. Il personale è adeguatamente sensibilizzato e formato sui rischi di

cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere gli allegati e-mail, utilizzare solo software autorizzato, ecc.). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.

Protezione dei dati (3.6)

11. La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
12. Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.

Protezione delle reti (3.7)

13. Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es. Firewall e altri dispositivi/software anti-intrusione).

Prevenzione e mitigazione (3.8)

14. In caso di incidente (es. sia rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
15. Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

Questi 15 controlli essenziali altro non sono che le regole di "cyber hygiene" di cui abbiamo parlato in precedenza: concetti ovvi, non difficili da mettere in pratica, ma troppo spesso sottovalutati, soprattutto da chi in azienda occupa i ruoli apicali e sembra ignorare questo aspetto o relegarlo a mero problema tecnico. L'approccio alla cybersecurity deve quindi permeare le strategie aziendali dall'alto verso il basso e la consapevolezza deve partire dai vertici aziendali.
Il rapporto dice anche, con riferimento al Processo di sicurezza interno da mettere in pratica:

> Esso dovrà coinvolgere tutti i livelli del personale, entrando di fatto nel DNA aziendale, in modo che tutti siano preparati ad affrontare la minaccia". E ancora: "investire in formazione del personale, diventa un elemento caratterizzante e primario... la sicurezza ha un costo, e uno dei costi maggiori è quello dovuto alla formazione.
>
> Il delicato equilibrio tra rischio e opportunità passa per un nuovo tipo di formazione, necessario per chiunque in azienda possa accedere a dispositivi che direttamente o indirettamente possono raggiungere gli asset dati aziendali. Quindi, investire in formazione del personale, diventa un elemento caratterizzante e primario per raggiungere questo equilibrio. Temporeggiare oggi nel fornire a sé stessi e ai propri dipendenti competenze e consapevolezza di base potrebbe avere ripercussioni negative importanti sul proprio business.

5.2.2 I costi (sostenibili) della Cybersecurity

Il rapporto, oltre a raccomandare questi controlli, fornisce anche una stima dei costi per implementarli.
Vengono fatte due simulazioni:

- **Azienda tipo 1**: micro-impresa manifatturiera con 9 dipendenti. I costi stimati sono circa 10.000 euro, suddivisi in 2.700 euro di costi iniziali e 7.800 euro di costi annui ricorrenti.
- **Azienda tipo 2**: media impresa di trasporti con circa 50 dipendenti. I costi stimati sono 22.450 euro, suddivisi in 4.650 euro di costi iniziali e 19.800 euro di costi annui ricorrenti.

Ipotizzando una riduzione del rischio cyber di circa l'80% rispetto a non implementare i controlli, risulta che i costi sostenuti in un periodo di 5 anni (41.450 euro per Azienda tipo 1, 103.650 euro per Azienda tipo 2) sono di gran lunga inferiori ai costi che le aziende dovrebbero subire come danno economico-finanziario in caso di incidente informatico (costi di ripristino, perdita di volume di affari, tempi di inattività, danno d'immagine).

5.3 GDPR (Regolamento UE 2016/679 sulla Privacy)

Un'altra norma importante è recentemente comparsa nell'ambito della cybersecurity: si tratta del GDPR (General Data Protection Regulation). È

conosciuto anche come Regolamento europeo sulla Privacy, ma non riguarda solo la privacy, come vedremo.

È diventato obbligatorio dal 25 maggio 2018 e, per la prima volta, introduce il concetto di "data breach".

FAQ ▶ CHE COSA È IL DATA BREACH?

Il GDPR, all'Art. 4 comma 12) lo definisce come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Il concetto di data breach era completamente assente nel precedente Codice Privacy (il D. Lgs. 196/2003), nato in anni in cui il web era agli albori e il cybercrime praticamente non esisteva. Con il GDPR il legislatore europeo vuole indurre le aziende – attraverso il "pretesto" della privacy – a riprogettare e migliorare la sicurezza dei propri dati per proteggere meglio il loro asset "immateriale" più importante, che sono proprio i dati. Quindi la privacy è trattata anche e soprattutto come messa in sicurezza dei dati.

L'indicazione di proteggere i dati comincia sin dalla fase di progettazione, la cosiddetta "privacy by design", con l'Art. 32 che recita: "il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio della sicurezza aziendale". Viene rafforzata e resa più stringente dall'Art. 33 ("Notifica di una violazione dei dati personali all'autorità di controllo") che impone di notificare il data breach all'Autorità di controllo – che in Italia è il Garante Privacy – "senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza".

Il successivo Art. 34 è ancora più forte, perché obbliga (in presenza di alcune condizioni) di dare comunicazione di una violazione dei dati personali anche all'interessato i cui dati siano stati oggetto di data breach. Sono evidentissimi i rischi reputazionali che questo potrebbe significare, soprattutto per banche e aziende finanziarie, per le quali la credibilità ha un valore strategico e commerciale molto elevato.

Per questo tema, si veda il nostro libro: Giorgio Sbaraglia e Francesco Amato, GDPR *kit di sopravvivenza. Capirlo, applicarlo ed evitare sanzioni sulla privacy e il trattamento dei dati personali*, goWare[27].

---

[19] http://securityaffairs.co/wordpress/69221/security/germanys-defense-minister.html

[20] https://www.enisa.europa.eu

[21] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148

[22] https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

[23] http://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg

[24] http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

[25] https://www.nist.gov/cyberframework

[26] http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf

[27] http://www.goware-apps.com/gdpr-kit-di-sopravvivenza-capirlo-applicarlo-ed-evitare-sanzioni-sulla-privacy-e-il-trattamento-dei-dati-personali-prefazione-stefano-aterno-stefano-quintarelli-giorgio-sbaraglia-francesco-amato/

LE TECNICHE DI CYBER ATTACCO

Un graffito, opera dell'artista di strada Willie (Wie) Soto, a Orlando in Florida.

6

Il social engineering, il phishing e gli attacchi attraverso la posta elettronica

6.1 Il social engineering: che cosa è e perché è così diffuso

Veniamo ora a parlare della tecnica di attacco più diffusa e soprattutto più efficace, quella che viene utilizzata nella stragrande maggioranza degli attacchi informatici (talvolta abbinata ad altre tecniche) perché sfrutta il punto di debolezza maggiormente aggredibile: il fattore umano.

Parliamo quindi del social engineering (in italiano "ingegneria sociale").

La definizione più semplice ed efficace è a mio parere quella che ne dà Paolo Attivissimo (divulgatore scientifico svizzero): "FREGARE IL PROSSIMO CON LA PSICOLOGIA".

Questa tecnica non è nata con l'informatica, tutt'altro, possiamo dire che esiste da sempre.

È social engineering anche il finto addetto della società elettrica che suona il campanello della persona anziana chiedendole di entrare "per controllare il contatore" e poi le ruba tutto.

È social engineering anche Totò che cerca di vendere la Fontana di Trevi agli americani (scena memorabile di un grandissimo attore!).

È social engineering anche quello che fa Frank Abagnale (personaggio realmente esistito), interpretato da Leonardo Di Caprio nel film di Steven Spielberg del 2002, *Catch me if you can* (in italiano *Prova a prendermi*), dove si finge pilota d'aereo, chirurgo e molto altro... riuscendo a ingannare le sue vittime (salvo poi finire arrestato da Tom Hanks).

Questa tecnica, da sempre efficace, ha trovato la sua migliore applicazione nell'informatica, dove troppo spesso l'utente non è adeguatamente consapevole di quello che fa e degli strumenti informatici che utilizza.

Nel social engineering, lo scopo degli attaccanti è indurre l'utente a fidarsi per esempio del contenuto di un messaggio che gli viene inviato e quindi convincere la vittima a eseguire le indicazioni.

Prendendo a paragone la nostra casa: per un ladro, invece che scassinare la porta blindata per entrare, sarà molto più semplice suonare il campanello... e convincerci ad aprire la porta!

Il social engineering è fatto apposta per aggirare gli antivirus, Firewall, ecc.: quando il sistema non ha vulnerabilità informatiche da sfruttare, si punta sulle debolezze e sulla curiosità delle persone.

6.2 Le vulnerabilità del "fattore umano"

Il social engineering fa leva proprio sulle "vulnerabilità" umane:

- colpa
- panico
- ignoranza
- curiosità
- desiderio
- avidità
- compassione e buoni sentimenti.

Alcuni semplici esempi:

- Le e-mail che riceviamo e che ci promettono sconti fantastici su prodotti costosi (desiderio e avidità).
- Il messaggio proveniente da uno "studio legale" che afferma di citarci in giudizio per conto di un suo cliente, invitandoci a cliccare su un link "per scaricare la pratica legale" (panico).
- Il messaggio di una fantomatica "polizia postale" che compare all'improvviso (in genere con una finestra di popup) proprio mentre stiamo navigando in un sito per scaricare illegalmente musica o software (colpa).
- L'email dello spedizioniere che ci segnala un pacco in arrivo e ci invita a cliccare sul link per vedere di cosa si tratta (curiosità).

6.3 Il phishing e lo spear phishing: cosa sono e come riconoscerli

Le tecniche attraverso cui il social engineering viene messo in pratica sono sempre le stesse e vanno sotto il nome di phishing e spear phishing.

FAQ ▶ COSA È IL PHISHING?

È un neologismo dato dall'omofonia con *fishing*, letteralmente "pescare", ed è infatti questa la filosofia principale dell'attacco: si cerca di indurre la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale, ad esempio il sito di una banca, al fine di rivelare informazioni personali come username e password, numeri di carta di credito, dati bancari, ecc.
È stato coniato anche il termine "**whaling**" dall'inglese *whale* ("balena"), per indicare un phishing nel quale si punta a far abboccare un pesce grande. Nel whaling rientra anche la "**CEO fraud**" (frode del CEO, di cui parleremo nel par. 6.6 dedicato alla Business Email Compromise), che consiste nel cercare di ingannare un alto dirigente o comunque una figura di elevato profilo aziendale, oppure un suo collaboratore, per indurlo a fornire informazioni riservate o addirittura a spostare somme in favore dell'attaccante.

Il phishing è paragonabile a una "pesca a strascico": gli hacker inviano, con sistemi automatici, migliaia di e-mail tutte uguali, sapendo che alcune raggiungeranno lo scopo e verranno aperte. È una "pesca" che cerca di farci abboccare con e-mail che sono costruite, più o meno accuratamente, per sembrare reali, come quelle che ci potrebbe inviare uno spedizioniere per comunicarci l'invio di un pacco, o come quelle che ci inviano i fornitori di servizi telefonici o di energia con le fatture allegate.

FAQ ▶ COME FANNO GLI SPAMMER A TROVARE GLI INDIRIZZI E-MAIL?

Ci provano... o perlomeno questo è un metodo molto diffuso, ma non l'unico.
Infatti la tecnica più usata è quella del **Dictionary attack**, che si basa semplicemente sull'indovinare gli indirizzi. In pratica, lo spammer cerca di comporre indirizzi che potrebbero effettivamente esistere. Per la parte a destra della chiocciola (@) usa nomi di dominio validi e per la parte a sinistra genera stringhe in base a qualche logica, per lo più nomi di

persone.
Per questo motivo l'indirizzo *nome.cognome@dominio.it* è uno dei più soggetti a questo tipo di attacco.
In alternativa, vengono usate le **Address list**: si tratta di acquisire liste di indirizzi da soggetti che li raccolgono per poi rivenderli.
Infine, può essere usato uno **Spambot,** che è un particolare tipo di web-crawler in grado di raccogliere gli indirizzi e-mail dai siti web, dai newsgroup, dai post dei gruppi di discussione e dalle conversazioni delle chat-room. Gli Spambot si basano sullo stesso principio del funzionamento dei crawler (detti anche web crawler, spider o robot), ovvero software che analizzano i contenuti di una rete o di un database in modo automatizzato, in genere per conto di un motore di ricerca.
A differenza di questi ultimi, cercano nelle pagine web tutti gli indirizzi e-mail presenti.

La tecnica in sé rimane sempre la stessa, ma sono diventate più sofisticate le strategie per superare i filtri antispam e antivirus e, soprattutto, sono molto più curate le e-mail, che spesso risultano perfettamente identiche a messaggi leciti che l'utente si aspetta di ricevere.
L'obiettivo è veicolare malware attraverso allegati di posta o link, finalizzati a:

- entrare nei sistemi informatici della vittima e prendere il controllo del computer dell'utente vittima attraverso l'uso di un malware
- rubarne le credenziali di accesso per poi "svuotare" il conto.

La compromissione dell'utente inizia con l'arrivo di un'e-mail in cui a seconda delle situazioni:

- si richiede all'utente di cliccare su un link
- si allega un file che l'utente non rileva come sospetto e viene pertanto scaricato ed eseguito.

Vale qui la pena di fare chiarezza su un aspetto sul quale c'è ancora molta confusione: **il computer viene infettato solo se si aprono gli allegati o si clicca sui link**. Limitarsi alla lettura del testo dell'e-mail non crea danni.

Quello che sta cambiando, come ci spiega il Rapporto CLUSIT 2018, è che gli attacchi sono sempre più industrializzati, realizzati su scala planetaria contro bersagli multipli. L'hacker "naif" individuale è stato sostituito da organizzazioni criminali strutturate, ove si ricorre anche a psicologi per confezionare messaggi sempre più credibili ed ingannevoli.

Il livello di verosimiglianza dei messaggi che vengono inviati è così elevato che sta diventando sempre più difficile per l'utente medio notare la differenza tra le mail mandate in una campagna di phishing e le e-mail inviate legittimamente dai comuni servizi on-line.

Sono passati più di 20 anni da quella che è considerata la prima campagna di phishing della storia e che coinvolse nel 1996 America on Line, il primo Internet Service Provider degli Stati Uniti, ma ancora oggi questa tecnica fraudolenta continua a mietere vittime.

Il successo del phishing è legato essenzialmente alla mancanza di consapevolezza informatica dell'utilizzatore che fa sì che, ancora oggi, più del 90% degli attacchi informatici inizi con un attacco phishing.

Alcuni numeri per illustrarne il fenomeno [Vedi Figura 16]:

- Le e-mail di phishing rappresentano oltre il 75% dei vettori di attacco, come si può vedere nel grafico sopra. Per il 39,9% usano allegati malevoli, mentre per il 37,4% ci spingono a cliccare su link "infetti".
- Nella maggioranza dei casi le e-mail di phishing sono create per veicolare un ransomware (la minaccia oggi più diffusa: ne parleremo nel cap. 7). La maggioranza di queste e-mail viene bloccata dai sistemi antispam dei nostri computer, ma inevitabilmente qualcuna, perché confezionata con più cura, riesce a scavalcare i nostri sistemi di sicurezza. A questo punto tutto è nelle mani (e nella testa) degli utenti.
- Il 41% delle aziende subisce attacchi di phishing ogni giorno, e più di tre quarti (il 77%) subiscono un attacco almeno una volta al mese [Vedi Figura 17].
- Le statistiche ci dicono che nel 30% dei casi l'utente apre l'e-mail.
- Non solo: il 13% degli utenti clicca anche sull'allegato (o sul link), permettendo al malware di entrare nel computer. A questo punto il disastro è fatto!

Quindi il phishing funziona e molto bene! Tanti "pesci" cadono nella rete e questo rende molto remunerativo il "lavoro" dei cybercriminali.

Perché tanti utenti fanno l'errore di abboccare? Perché ci lasciamo prendere dalla fretta e non ci fermiamo un attimo a chiederci se ha senso ricevere quella e-mail.

Basta veramente poco per capire che quell'email ha qualcosa di strano: consiglio di **posizionare il mouse** (ma, mi raccomando, **senza fare clic!**) **sull'indirizzo del mittente** per vedere se l'indirizzo e-mail è diverso da quello che appare e poi di farlo passare **sul link** per leggerne il testo: se quello che leggiamo ha qualcosa di strano, meglio evitare di cliccare!

I link malevoli vengono in genere ben camuffati (è facilissimo farlo!): il link che appare sull'email non ci fa vedere qual è il **vero link**. Ma se è facile nascondere un link dietro un testo falso, è altrettanto facile smascherare il trucco: posizionando il mouse sul link, il vero link ci apparirà, in genere nella barra di stato che è nella parte bassa dello schermo, oppure vicino al link stesso.

Se il link che compare è lungo, spesso con diverse serie di numeri e lettere, e ben diverso da quello che ci aspetteremmo, dobbiamo assolutamente **evitare di cliccarci sopra**.

Questa semplice accortezza, unita a un **controllo dell'ortografia dell'e-mail**, è una delle modalità più facili – ma efficaci – per smascherare un phishing.

Fermiamoci dunque sempre qualche secondo a ragionare prima di cliccare.

In fondo, quando accendiamo il computer, non è necessario che spegniamo il cervello...

> Poiché la qualità delle e-mail di phishing è notevolmente migliorata, bisogna tenere conto che per alcuni utenti sarà più facile cadere in trappola. Le persone sono la prima linea di difesa contro un attacco di phishing e la **formazione** è sicuramente un aspetto fondamentale per il mantenimento dei livelli di sicurezza. È necessario fornire agli utenti gli strumenti e le informazioni necessari non solo a evitare le trappole ma anche a segnalare eventuali attacchi in modo tempestivo qualora cadano nell'inganno.
>
> (John Shier, Senior Security Expert di Sophos)

Lo **spear phishing** è invece un attacco mirato: **spear** significa "fiocina", quindi il pescatore vuole prendere proprio "quel" pesce. L'oggetto dell'attacco viene accuratamente selezionato e studiato (oggi è molto facile raccogliere informazioni

su una persona, attraverso i social e il web). In questo caso le e-mail inviate sono preparate ad hoc per risultare credibili e indurre le vittime in errore, citando particolari o nomi veri. Talvolta l'indirizzo e-mail del mittente potrebbe essere stato falsificato con una tecnica nota come "**spoofing**" (di cui parleremo più approfonditamente nel par. 6.5): l'e-mail sembrerà arrivare da una persona conosciuta e della quale ci fidiamo (un collega, un superiore, un familiare o un amico) e perciò risulterà molto più subdola. E, molto probabilmente, non sarà neppure stata bloccata dall'antispam, proprio perché costruita con più cura.

6.3.1 Un esempio di spear phishing: il caso "Eye Pyramid"

Un famoso esempio di spear phishing è il caso "Eye Pyramid": un caso di cyberspionaggio per il quale sono stati arrestati a inizio 2017 i due fratelli Occhionero, Giulio, ingegnere nucleare di 45 anni, e Francesca Maria, 49 anni, laureata in chimica.

L'accusa è di aver sottratto informazioni, violando – o tentando di violare – i computer di molti personaggi istituzionali, tra cui Matteo Renzi e Mario Draghi.

I due fratelli hacker avrebbero violato migliaia di dispositivi (si parla di 18.327), riuscendo così a spiare personaggi politici, banchieri, massoni e rappresentanti delle istituzioni a diversi livelli. L'operazione di cyberspionaggio andava avanti da oltre 6 anni.

Venivano inviate e-mail con la tecnica dello spear phishing attraverso mittenti falsificati (spoofing) per risultare credibili ed affidabili al destinatario. Queste e-mail contenevano un allegato all'interno del quale si trovava il software malevolo utilizzato dagli Occhionero che si chiamava Eye Pyramid e che permetteva di controllare a distanza i computer sui quali veniva installato.

Questo software era un trojan (cavallo di Troia) del tipo RAT (remote administration tool). Anche qui entra in gioco il fattore umano: dopo 6 anni di cyberspionaggio, una delle potenziali vittime riceve un'e-mail, ma, essendo persona attenta e consapevole di questi rischi, sospetta che l'e-mail sia pericolosa e la invia a una società specializzata in cybersecurity. E i fratelli Occhionero sono stati scoperti ed arrestati dalla Polizia Postale[28].

6.3.2 Clonato il sito di Fineco

Oggi il cybercrime mira soprattutto a "fare soldi": con l'estorsione, con il furto di credenziali e di dati. Proprio per questo il mondo bancario è sempre stato tra i più colpiti e nell'anno 2017 si è confermato un trend in aumento per le attività legate al cybercrime in ambito finanziario, con un quarto del totale delle mail di phishing inviate.

Secondo le statistiche di Kaspersky, nel corso del 2017 le banche sono state oggetto del 27% degli attacchi di phishing, i sistemi di pagamento online del 15,87%, mentre i negozi online del 10,95%.

Secondo un'altra ricerca condotta da Ponenon per conto di Accenture, nel giro di 5 anni il numero totale degli attacchi agli istituti finanziari è triplicato e i tempi per risolvere i problemi causati da quelli andati a buon fine si stanno allungando a causa dell'aumentato livello di complessità.

La tecnica più usata è in genere quella del phishing: indurre la vittima a fornire le sue credenziali bancarie (username + password) per poter accedere al conto, compiere operazioni e rubargli il denaro.

Un caso clamoroso di truffa informatica che ha riguardato il mondo bancario è stata la clonazione del sito di Fineco.

Il sito ufficiale di Fineco è https://finecobank.com/it/. Alcuni anni fa ne è stata creata una copia identica falsa ("fake") da alcuni malviventi usando un dominio ovviamente differente: www.finecobanca.net nella speranza di indurre gli utenti a credere che quest'ultimo fosse il nuovo sito di Fineco.

Con un'e-mail di phishing si invitavano poi i clienti a reinserire i propri dati nel "sito rinnovato" e, per essere più credibili, si menzionava il phishing, sostenendo che tutto ciò era necessario proprio per evitare questo genere di truffe. Nella figura 18 [Vedi Figura 18] il messaggio truffaldino (con alcune note a evidenziare i punti che ci dovrebbero insospettire) .

Il risultato è stato che in molti ci sono cascati, hanno dato le loro credenziali al sito sbagliato e per questa leggerezza si sono visti sottrarre denaro dal vero conto.

6.3.3 Le PEC falsificate

In un altro caso molto recente (maggio 2018) un'organizzazione criminale italiana è riuscita a registrare e-mail PEC (vere PEC!) con indirizzi quasi identici a

quelli di alcune note banche on line. Questo è stato possibile sfruttando una debolezza del sistema di emissione delle PEC: basta una procedura svolta interamente on-line, ossia senza effettuare il riconoscimento de visu del soggetto richiedente.

In particolare sono state prese di mira ING Direct e Fineco, del tutto estranee alla truffa. La PEC ufficiale di ING è ing.bank@legalmail.it; I criminali hanno registrato un indirizzo PEC che era appena differente, ingbank@legalmail.it (mancava solo un punto), e l'hanno usato per richiedere ai veri clienti ING le loro credenziali di accesso ai conti on-line (username + password).

Le PEC con cui i correntisti pensavano di comunicare con le banche venivano ricevute e lette dai truffatori, che hanno potuto eseguire movimenti di denaro dai conti delle vittime su conti di comodo intestati a soggetti fittizi da cui poi venivano fatti definitivamente sparire. Una truffa astuta, ma tutto sommato semplice, e che non si può neanche considerare un vero attacco informatico. La novità è che le mail utilizzate erano PEC, considerate – a ragione – sicure ed inviolabili.

Ancora una volta è il fattore umano il vero punto di debolezza: qualcuno ha permesso di registrare indirizzi PEC senza verificare l'identità del richiedente e poi qualche cliente – con scarsa attenzione – ha comunicato le sue credenziali bancarie via e-mail (anche se erano state richieste via PEC).

6.3.4 La "SIM Swap Fraud"

In genere i siti di Internet banking prevedono la doppia autenticazione (nota anche come autenticazione a due fattori, v. par. 13.9 "L'Autenticazione a due fattori") per l'accesso (non sempre), ma soprattutto per eseguire operazioni dispositive (sempre).

Per questo ai cybercriminali non basta conoscere username e password, ottenibili attraverso il phishing, ma occorre avere anche il PIN. E di regola questo PIN è un codice a tempo (la cosiddetta OTP, "one time password", di cui parleremo più in dettaglio nel capitolo 13, dedicato all'uso delle password), che l'utente riceve attraverso un SMS.

Come fare dunque a intercettare l'SMS contenente il PIN? I cybercriminali si sono inventati la tecnica della "SIM Swap Fraud". La truffa è stata scoperta dalla Polizia

postale di Catania, dopo una denuncia di un istituto di credito che aveva subito un attacco informatico e ai cui clienti, residenti in varie parti d'Italia, erano stati sottratti 300 mila euro.

I malviventi andavano presso un dealer di telefonia mobile, dichiarando il furto del telefono e richiedendo perciò la sostituzione della SIM. Esibendo un falso documento di identità intestato alla vittima, oppure con la complicità di un addetto del negozio, ottenevano che la scheda SIM del titolare venisse disabilitata e sostituita da quella attivata fraudolentemente.

La vittima rilevava il mancato funzionamento del suo telefono, che era diventato muto, ma non associava immediatamente l'evento a una frode in corso.

Ottenuta la SIM con il numero della vittima, il gioco era fatto: l'SMS di autenticazione arrivava ai malviventi che potevano procedere allo "svuotamento" del conto, eseguendo bonifici in uscita.

Un altro caso, ancora più clamoroso: negli Stati Uniti, nel 2018, tale Michael Terpin[29] ha intentato una causa da 240 milioni di dollari nei confronti di AT&T, una delle più grandi compagnie telefoniche statunitensi, accusandola di essere responsabile del furto di 24 milioni di dollari in Bitcoin, causato da una SIM swap. Il cambio di SIM sarebbe stato fatto con la complicità di un impiegato di AT&T che il cyber-criminale avrebbe corrotto con una classica "mazzetta". Terpin si è accorto che il suo cellulare non funzionava più ma, prima che potesse bloccare la SIM, l'ignoto pirata informatico sarebbe riuscito a trasferire dal suo conto la bellezza di 24 milioni di dollari in Bitcoin.

Di qui l'accusa ad AT&T di non aver tutelato in maniera adeguata la sicurezza dell'account e la richiesta di risarcimento che comprende, oltre i Bitcoin rubati, altri 216 milioni come "punizione" ai danni della compagnia telefonica.

Per scongiurare questa tecnica, che sta diventando frequente, è importante che chiunque usi l'autenticazione a due fattori (e in particolare le banche, che sono quelle più a rischio), lo faccia non utilizzando gli SMS per inviare il codice PIN. Esistono metodi molto più sicuri: i token, che le banche stanno dismettendo per ragioni di costi, oppure l'autenticazione a due fattori attraverso l'app della banca

(è il sistema più affidabile). Ne parliamo al per. 13.9.1 “Come ottenere il secondo fattore di autenticazione”.

[Torna al capitolo] 6.4 Come funziona la posta elettronica

Abbiamo visto sopra che cosa è il social engineering e perché è così diffuso. Abbiamo poi spiegato che il social engineering viene messo in pratica per attaccare tanto le grandi organizzazioni quanto i computer di utenti singoli attraverso le tecniche del phishing e dello spear phishing utilizzando soprattutto lo strumento dell’e-mail.

Vediamo ora perché questo succede, ripercorrendo brevemente l’affascinante storia della nascita ed evoluzione della rete Internet e facendo anche un poco di chiarezza, perché su questi temi c’è ancora una certa confusione.

Internet è come una grande autostrada. È nata alla fine degli anni ’60, si chiamava inizialmente ARPAnet perché fu creata dall’agenzia americana ARPA (Advanced Research Projects Agency), poi rinominata DARPA (Defense Advanced Research Projects Agency), un’agenzia governativa del Dipartimento della Difesa degli Stati Uniti incaricata dello sviluppo di nuove tecnologie per uso militare. Eravamo in epoca di guerra fredda USA-URSS e ARPAnet fu pensata inizialmente per scopi militari, ma da questo progetto nacque quella che è stata probabilmente la più grande rivoluzione del XX secolo: una rete globale che collega tutta la Terra.

I primi quattro nodi di ARPAnet, nel 1969, furono quattro università americane: l’UCLA (University of California, Los Angeles), lo SRI (Stanford Research Institute), l’Università dello Utah, e UCSB (University of California, Santa Barbara).

Nel 1974 venne definito lo standard di trasmissione TCP/IP(Transmission Control Protocol/Internet Protocol): creatori di tali protocolli, resi di pubblico dominio fin dall’inizio e ancora oggi utilizzati, sono stati Robert Kahn e Vinton Cerf, che possiamo considerare tra i padri fondatori di Internet.

Negli anni ’80 ARPA terminò il progetto e ARPAnet divenne la rete pubblica che fu denominata “Internet”.

L’autostrada Internet viene utilizzata da diversi tipi di “veicoli”, cioè tante

modalità di comunicazione:

- il World Wide Web (WWW, inventato da Tim Berners-Lee nel 1989), serve per la navigazione sui siti usando i browser
- la posta elettronica
- l'Internet delle Cose (IoT: Internet of Things)
- il File Transfer Protocol (FTP), che è utilizzato per trasmettere file
- il VoIP (Voice over IP), che consente di parlare al telefono sfruttando Internet invece della rete telefonica tradizionale
- lo Streaming (con cui possiamo vedere i film)
- il File Sharing
- il Cloud computing
- le Chat e altro ancora.

L'email dunque non è che una delle molte modalità di utilizzo di internet. È stata una delle prime nate e proprio in questo risiede la sua intrinseca debolezza. La sua invenzione risale al 1971, quando Ray Tomlinson installò su ARPAnet un sistema in grado di scambiare messaggi fra le varie università americane. Chi realmente ne definì poi il funzionamento fu John Postel.

Tutte le e-mail spedite su Internet vengono trasferite usando un unico protocollo in uscita: **Simple Mail Transfer Protocol** (SMTP). Si tratta di uno standard tecnologico: ogni server internet che utilizza SMTP è in grado di inviare e ricevere posta da qualsiasi altro server SMTP su Internet [Vedi Figura 19].

SMTP rappresenta l'esempio più evidente di come uno strumento creato senza particolare attenzione alla sicurezza oggi gestisce e controlla tutte le attività della nostra società. Tra le tecnologie di Internet, la posta elettronica è infatti quella che probabilmente più ha cambiato il modo di vivere e di lavorare di centinaia di milioni di persone in tutto il mondo. Tutti noi usiamo l'e-mail, non pensando che si tratta di uno degli strumenti più antiquati e vulnerabili della rete.

Il protocollo SMTP è quindi uno dei più vecchi di Internet ed è volutamente mantenuto semplice, visto che un server SMTP deve poter gestire decine di connessioni al secondo. Questa semplicità si traduce in vulnerabilità, perché le

due informazioni identificative che il server mittente passa al destinatario (l'indirizzo e-mail del mittente e quello del destinatario) non vengono verificate e possono essere quindi facilmente falsificate.

L'e-mail può essere intercettata e letta da un malintenzionato, il cosiddetto "Man in the Middle" (MITM), che si frappone tra mittente e destinatario. Infatti, nella maggior parte dei casi, le e-mail vengono trasmesse non criptate, come se fossero state scritte su una cartolina (che tutti possono leggere!). È possibile cifrare le e-mail che si inviano e si ricevono, ma solo se ambedue i provider del servizio e-mail – mittente e destinatario – supportano la **crittografia TLS (con il protocollo HTTPS)**. In altre parole, la crittografia del 100% delle e-mail trasmesse su Internet richiederebbe la collaborazione di tutti i fornitori di servizi e-mail online. In realtà solo alcuni provider rispondono ai suddetti requisiti: uno dei più noti è Gmail di Google.

Abbiamo detto che tra le molte limitazioni c'è quella che il protocollo SMTP non è in grado di gestire l'autenticazione del mittente. Questa è probabilmente la vulnerabilità più grave, perché viene sfruttata da chi usa l'e-mail come strumento di attacco per fare phishing.

È infatti possibile – e anche abbastanza facile! – inviare e-mail falsificando il mittente. In altre parole, si può spedire un'e-mail facendo apparire come mittente l'indirizzo corrispondente a un altro account. Questo anche senza avere accesso all'account falsificato, cioè senza conoscere le credenziali della casella di posta che si usa.

Questa tecnica si chiama **spoofing** ed è estremamente pericolosa, accessibile senza grandi competenze informatiche e – ahimè – estremamente efficace.

6.5 Lo spoofing

È una tecnica di attacco per falsificare informazioni, come l'identità di un host (computer o server) o il mittente di un messaggio. Quando un attaccante riesce a impersonare qualcun altro in una rete, gli è possibile intercettare informazioni riservate, diffondere informazioni false e tendenziose o effettuare attacchi. Lo spoofing risulta molto efficace combinato a tecniche di social engineering per

avere accesso a informazioni "riservate" e credenziali degli utenti. Social media scammers (truffatori) o phishers possono usare questa tecnica ad esempio per convincere un utente a connettersi ad un server malevolo intercettando così le sue credenziali o ad eseguire azioni dannose.

Nonostante lo spam e lo spoofing siano ancor oggi una grave vulnerabilità della posta elettronica, non si ritiene praticabile una revisione radicale del protocollo SMTP, per via del gran numero di implementazioni di questo protocollo e soprattutto per la complessità e il costo di una tale modifica.

La tecnica dello spoofing è molto efficace per realizzare attacchi di phishing e soprattutto di spear phishing, che – come abbiamo già spiegato – sono diventati gli strumenti di attacco più diffusi per veicolare malware, sia a livello privato che aziendale.

Proviamo a pensare cosa potrebbe succedere se riceviamo un'e-mail proveniente (in apparenza!) da un collega, da un superiore o da un amico. Se questa e-mail è ben confezionata, non sarà neppure stata bloccata dall'antispam; e se è resa credibile con riferimenti personali o aziendali, sarà abbastanza probabile che il destinatario (la "vittima" dell'attacco) caschi nel tranello e apra l'allegato o clicchi sul link o esegua l'indicazione riportata nel messaggio.

PRECISAZIONE: nel caso in cui l'attaccante sia riuscito a ottenere la password della casella di posta, le e-mail di phishing sono inviate dalla casella originale che è stata violata e non da un indirizzo fittizio. Si tratta di **violazione della casella** e non di e-mail spoofing.

Questo caso è ancora più grave, perché significa che qualcuno sta usando la nostra casella a nostro nome e che, addirittura, potrebbe cambiare la password e impedirci di accedere alla nostra e-mail. Siamo già nel caso ancor più grave del "furto di identità".

6.6 La Business E-mail Compromise (BEC): che cosa è e quanti danni sta causando nelle aziende

6.6.1 CEO Fraud

Veniamo alla Business E-mail Compromise (BEC) raccontando un caso vero, accaduto a settembre 2017 e finito su tutti i giornali[30] [Vedi Figura 20].
Il direttore della delegazione della Confindustria all'Unione Europea a Bruxelles riceve un'e-mail dalla sua diretta superiore:

> Caro G., dovresti eseguire un bonifico di mezzo milione di euro su questo conto corrente.
> Non mi chiamare perché sono in giro con il presidente e non posso parlare.
> M.P.

Il funzionario della Confindustria a Bruxelles esegue il bonifico che non avrebbe dovuto fare e circa cinquecentomila euro (in realtà la cifra pare un po' inferiore) sono passati da un conto della Confindustria a un conto estero di cui non si conosce l'intestatario. Soldi evaporati, scomparsi per sempre.

Come è stato possibile? Tutto è cominciato da una mail falsa, ma alla quale il funzionario ha purtroppo dato credito. E per questo è stato licenziato.
Il lettore potrebbe pensare: "è stato uno sprovveduto, come si può cascare in una truffa del genere?"
E invece, anche se sembra incredibile, in tantissimi ci cascano...
È successo in Confindustria ma sono centinaia le aziende colpite ogni giorno da frodi finanziarie e milioni le mail contraffatte (mail spoofing, appunto) da cui partono ordini per spostare denaro in ogni parte del mondo.
Ce lo dimostra un importante rapporto redatto dal Federal Bureau of Investigation[31] [Vedi Figura 21] (la ben nota FBI) del 4 maggio 2017 dove vengono esposti i danni generati dalla BEC nel mondo.

Sono numeri impressionanti: tra ottobre 2013 e dicembre 2016 gli incidenti rilevati in USA e nel resto del mondo sono stati 40.203 e il danno subito è pari a 5.302.890.448 di dollari (oltre 5 miliardi).
Secondo l'FBI, le truffe BEC sono state segnalate in oltre cento Paesi e hanno fatto registrare un notevole aumento, pari al 2.370%, delle perdite rilevate tra gennaio 2015 e dicembre 2016.

L'ultimo aggiornamento del Rapporto FBI sulla BEC [Vedi Figura 22] è uscito il 12 luglio 2018[32]: il totale delle perdite è salito all'astronomica cifra di 12.536.948.299 USD (nel periodo tra ottobre 2013 e maggio 2018). Confrontando i due rapporti scopriamo che in meno di un anno e mezzo (da dicembre 2016 a maggio 2018) sono stati persi per la BEC altri 7,2 miliardi di dollari, con un aumento del 2.200% tra il 2015 ed il 2017 e un picco massimo nel settembre 2017 con oltre 18 milioni di dollari persi in un solo mese.

Quindi, riassumendo, l'e-mail spoofing può servire per veicolare malware (tra i cui i famigerati ransomware di cui parleremo in seguito), ma anche per la truffa nota come Business E-mail Compromise (BEC), di cui il caso raccontato rappresenta solo una delle possibili varianti, quella definita come "CEO Fraud" (la frode del CEO).

Ogni giorno, circa 400 aziende sono vittime di attacchi tramite BEC e nella maggior parte dei casi vengono presi di mira addetti all'interno dello staff finanziario: un enorme fattore di rischio per le aziende!

La BEC ha le caratteristiche di una truffa classica: la tecnologia è soltanto un mezzo nuovo per portare a termine raggiri vecchi.

In genere, i cyber attacchi che sfruttano le e-mail come vettore di minacce cibernetiche al loro interno contengono allegati con malware. Con le CEO Fraud e le BEC, invece, non ci sono allegati, ma solo il corpo normale di un messaggio, nel quale l'attaccante cerca solo di rendersi credibile, "clonando" al meglio il mittente.

Nel testo della mail l'aggressore chiede al suo bersaglio di compiere un gesto specifico, che sia un trasferimento di denaro o l'accesso a informazioni riservate. Il destinatario probabilmente non si insospettisce, perché il messaggio non contiene allegati (considerati pericolosi) e proviene da una fonte certificata e autorevole. Quindi probabilmente eseguirà la richiesta, soprattutto se operazioni simili (bonifici, ecc.) avvengono già in azienda e con le stesse modalità.

Paradossalmente, in questi casi, le aziende con processi meno informatizzati e più "tradizionali" risultano meno vulnerabili.

6.6.2 La truffa "The Man in the Mail"

Un'altra delle varianti della BEC è la truffa "The Man in the Mail".

I delinquenti intercettano la posta elettronica di un'azienda e fanno in modo che i pagamenti finiscano sui loro conti correnti. Colpisce soprattutto aziende che fanno import/export, in quanto il conto su cui viene dirottato il pagamento si trova all'estero (generalmente in paesi molto lontani, soprattutto extra-europei).

Le motivazioni sono chiare: in certi paesi le regole bancarie sono meno rigorose, oppure il criminale potrebbe avere qualche "appoggio" all'interno della banca. E soprattutto la vittima della truffa troverà complicato avventurarsi in cause legali in un paese estero e lontano, con costi alti ed esito incerto. Infatti nella maggior parte dei casi (ne abbiamo incontrati tanti...), si tende a lasciar perdere e a rinunciare a qualsiasi azione risarcitoria, salvo nei casi in cui l'importo perso sia veramente considerevole.

Come funziona quindi la truffa "The Man in the Mail"?

Il malvivente viola la casella di posta, quella del mittente oppure quella del destinatario, mediante tecniche diverse, ma ugualmente efficaci: phishing, social engineering, furto delle credenziali o attacco "brute force" (v. par. [13.3 Come ci vengono rubate le password?]), keylogger (v. par. [8.4 I keylogger]). Studia quindi le comunicazioni dell'azienda, la carta intestata, le firme dei responsabili, lo stile della corrispondenza. Scopre i ruoli aziendali, individuando – per esempio – chi è preposto ad eseguire i pagamenti ai fornitori.

Poi si inserisce in conversazioni già in corso comunicando, alla persona giusta dell'azienda, coordinate bancarie diverse (le sue!) su cui eseguire i pagamenti. Per fare questo usa appunto lo "spoofing", falsificando il mittente, oppure usando un indirizzo e-mail appena diverso, o – ancora – accedendo direttamente all'email violata.

In alcuni casi, avendo avuto accesso alla corrispondenza tra cliente e fornitore, riesce anche a richiamare numeri d'ordine o importi relativi a forniture realmente eseguite.

Il risultato è che l'azienda cliente (quella che deve pagare) si vede arrivare un messaggio con una fattura confezionata con la grafica uguale a quella vera

(copiata dall'hacker), che indica di eseguire il pagamento su un conto diverso (non quello solito). E probabilmente lo eseguirà senza farsi troppe domande...

I numeri riportati nel citato Rapporto FBI ci fanno capire che questa truffa – se ben organizzata – ha ottime probabilità di successo.

Facebook e Google nel 2017 sono state vittime della BEC portata dallo stesso truffatore (Evaldas Rimasauskas) che è riuscito a sottrarre circa 100 milioni di dollari a entrambe[33], spacciandosi per un fornitore taiwanese della ditta Quanta Computer e richiedendo pagamenti per forniture. La truffa è stata scoperta, il delinquente arrestato e Facebook e Google hanno dichiarato di essere riuscite a recuperare il denaro. A un'azienda famosa come Mattel (che produce la bambola Barbie) è andata peggio, con perdite per circa 3 milioni di dollari.

Io stesso, nella mia attività di formazione nel campo della cybersecurity, mi trovo quotidianamente a parlare di questo argomento nelle aziende. E posso dire che praticamente tutte le aziende che ho incontrato hanno subito attacchi di tipo BEC: qualcuna è riuscita a non caderci, ma molte altre hanno invece pagato sul conto sbagliato...

Le cifre sono state da poche migliaia di euro fino a decine di migliaia. In alcuni casi, per fortuna rari, si è arrivati ad alcune centinaia di migliaia di euro.

6.6.3 Come difendersi dalla Business E-mail Compromise

Riassumiamo le differenti varianti della BEC, come classificate nel citato Rapporto FBI, che indica cinque scenari (ove i primi due sono i più diffusi):

1. **Business tra cliente e fornitore**: richiesta di pagamento con e-mail falsificata. Viene definita – come spiegato sopra– "The Man in the Mail" ed anche "Bogus Invoice Scheme" "Supplier Swindle" o "Invoice Modification Scheme".
2. "**CEO Fraud" o "Business Executive Scam"**: una richiesta di bonifico bancario viene inviata dall'account compromesso di un dirigente aziendale di alto livello (CEO o Chief Financial Officer) a un dipendente all'interno dell'azienda che è in genere responsabile dell'elaborazione di tali richieste. È la variante di phishing definita anche "whaling", perché punta al "pesce grosso".
3. **Business Contacts through Compromised E-mail**: avviene quando un

dipendente di un'azienda ha la sua e-mail personale violata e dal suo indirizzo mail vengono inviate richieste di pagamenti di fatture a conti bancari controllati da frodi a più fornitori identificati dall'elenco dei contatti di questo dipendente.

4. **Business Executive and Attorney Impersonation**: le vittime vengono contattate da truffatori che di solito si identificano come avvocati o rappresentanti di studi legali e sostengono di trattare questioni riservate o urgenti. Le vittime vengono spinte dal truffatore ad agire rapidamente o segretamente in un trasferimento di fondi. Questo tipo di truffa BEC spesso si verifica alla fine della giornata lavorativa o della settimana lavorativa, perché è programmata per coincidere con la chiusura delle attività delle istituzioni finanziarie internazionali.
5. **Data Theft** (furto di dati): le richieste fraudolente vengono inviate utilizzando l'e-mail compromessa di un dirigente. I destinatari della richiesta sono figure dell'organizzazione aziendale che conoscono dati importanti, come Risorse umane, contabilità o auditing. Queste richieste in genere si verificano prima di una richiesta fraudolenta di bonifico bancario.

Esaminiamo ora come proteggerci da queste frequenti e temibili truffe.
Come sempre è importante avere la consapevolezza del rischio e non sottovalutarlo. Vediamo quindi quali sono gli accorgimenti da adottare:

- Usare **credenziali di accesso alle mail robuste e sicure**, quindi impostare una corretta gestione delle **password**.
- **Non utilizzare in azienda indirizzi e-mail basati su webmail**, più facilmente accessibili e attaccabili.
- **Leggere le mail con attenzione**, soprattutto quelle che si riferiscono a pagamenti, e, nel dubbio, fare verifiche con mezzi diversi: è cioè molto importante **non chiedere la conferma usando lo stesso indirizzo**, perché ci risponderebbe il truffatore; usare piuttosto il telefono, o contattare direttamente il mittente utilizzando l'indirizzo presente nella rubrica aziendale oppure un altro indirizzo e-mail della cui credibilità siamo certi.
- **Controllare bene il mittente delle e-mail**: un dettaglio (anche solo una lettera!) potrebbe fare la differenza. Alcuni esempi di come è facile indurre in

inganno con un indirizzo e-mail modificato ad arte: l'e-mail reale info@pippodomus.com potrebbe essere trasformata dal truffatore in info@pippodornus.com con la sostituzione della lettera "*m*" con "*rn*", difficilmente distinguibile a colpo d'occhio (e chi legge l'e-mail va sempre di fretta...); oppure potrebbe essere modificata in info@pipp0domus.com sostituendo la lettera "o" con il numero "0", pressoché identico; o anche in info@pippo-domus.com (un segno meno che passerà facilmente inosservato). E molte altre: l'inventiva degli attaccanti è illimitata...

E soprattutto: evitare di pensare "figurati se una cosa del genere può succedere a me!". Può succedere a chiunque, se non si è attenti e consapevoli. In altre parole: come sempre è il fattore UMANO che può fare la differenza.

6.7 Gli strumenti informatici per proteggersi dal phishing

Gli attacchi di phishing potrebbero essere difficili da prevenire e rilevare, soprattutto se sono mirati e costruiti con cura, senza errori vistosi, come è il caso dello spear phishing.

Manca l'oggetto della minaccia cibernetica: un link malevolo, un malware, ecc.: quei segnali che i normali programmi antispam o antivirus sono in genere in grado di rilevare.

Inoltre, a causa della citata debolezza del protocollo SMTP e del fatto che i principali client di posta elettronica mostrano solitamente solo il nome del mittente, è complicato per chi riceve i messaggi capire che si tratta di un cyber attacco.

In realtà, le e-mail di spoofing lasciano sempre qualche traccia, ma per vedere l'indirizzo reale del mittente (o quanto meno il server da cui sono partite) bisogna compiere alcune azioni, che l'utente medio non conosce e che solo chi ha una certa esperienza di cybersecurity riesce a mettere in pratica.

Quando si sospetta la ricezione di messaggi contraffatti, il modo migliore di verificarne la reale identità del mittente sarebbe quello di **leggere le informazioni contenute nell'header dell'e-mail ricevuta**. Oppure rivolgersi a qualcuno in grado di farlo...

FAQ ▶ COSA È L'HEADER DI UN MESSAGGIO DI POSTA?

Sono le intestazioni del messaggio stesso e contengono le informazioni relative a tutta la storia dell'e-mail, dal momento in cui viene inviata all'accettazione da parte del server destinatario, oltre alle informazioni che riguardano l'autore del messaggio stesso.
Tutti i client che usiamo per la posta elettronica (p.es. Outlook o Thunderbird) hanno l'opzione per visualizzare l'header di un'e-mail ricevuta. Il comando in genere si chiama **"Mostra intestazioni"**, o qualcosa di simile. Attivando il comando, potremo accedere alla parte "nascosta" dell'e-mail e vederne molti dettagli.
Per esempio: il campo "Received From" indica il server mittente, da cui è partito il messaggio (questa informazione potrebbe svelarci lo spoofing)

Saper leggere l'header di un'e-mail non è facile e non si può pretendere che lo faccia un normale utente, senza specifiche competenze IT. Nella figura 23 [Vedi Figura 23], dove è rappresentato proprio un header, ci rendiamo conto delle complessità di lettura.

In questo esempio, nel campo "Received... from..." si potrebbe capire se il server di invio (nomedominio.ext) è quello corrispondente all'indirizzo del mittente (che potrebbe invece essere stato falsificato).
Sono estremamente utili, per superare questo tipo di difficoltà, i software antispam più avanzati, moderni e aggiornati, che implementano alcuni controlli: in pratica, fanno in modo automatico quelle verifiche che l'utente medio non sarebbe in grado di fare da solo.
Questi antispam riescono a prevenire lo spoofing delle e-mail in entrata utilizzando tecnologie quali:

- **Sender Policy Framework (SPF)**: consente di verificare che una e-mail inviata da un dato dominio arrivi effettivamente da uno degli host abilitati dai gestori del dominio stesso.
- **DomainKeys Identified Mail (DKIM)**: permette ai gestori di un dominio di aggiungere una firma digitale tramite chiave privata ai messaggi di posta elettronica. DKIM aggiunge quindi un ulteriore strumento per verificare la

corrispondenza tra mittente e relativo dominio di appartenenza. DKIM e SPF non sono due tecniche alternative ma piuttosto complementari.
- **Domain-based Message Authentication, Reporting and Conformance** (DMARC): è un sistema di validazione dei messaggi di posta elettronica. Le caratteristiche di DMARC sono state definite nella RFC 7489 del marzo 2015.

In pratica, queste tecnologie eseguono una serie di controlli di validazione dell'header dei messaggi di posta e sono in grado di scoprire eventuali anomalie.

Consiglio caldamente di valutare l'adozione dei programmi antispam con queste funzionalità: sarà un saggio investimento, tenuto conto che è proprio dalla posta elettronica che arriva in azienda la maggior parte dei guai...

6.8 PEC e posta crittografata

Per un'e-mail più sicura si possono usare strumenti più avanzati, rispetto all'antiquato e insicuro protocollo SMTP:

- La PEC (posta elettronica certificata).
- La posta crittografata PGP (Pretty Good Privacy).

La PEC viene rilasciata all'utente dai gestori del servizio PEC, che devono essere accreditati presso un ente centrale, il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione). Il CNIPA attesta l'identità del gestore.

Come noto, ha valore legale e certifica che il messaggio è stato recapitato correttamente (come per una Raccomandata A/R); inoltre garantisce l'autenticità e l'integrità dei dati, attraverso le firme digitali del gestore. Svantaggi: è uno standard esclusivamente italiano (non c'è interoperabilità con paesi stranieri).

Manca inoltre la conferma di lettura del messaggio.

Prima di parlare di PGP, citiamo anche un'altra possibile soluzione, meno diffusa, per una posta sicura: **ProtonMail**[34], che si definisce nella sua homepage "Email sicura basata in Svizzera". Si tratta di un servizio che è stato fondato nel 2013 da scienziati che si sono incontrati presso il CERN di Ginevra.

Tutti i server si trovano in Svizzera: "tutti i dati dei nostri utenti sono protetti dalle severe leggi svizzere sulla privacy".
Utilizza la crittografia End-to-End, richiede la creazione di un account dedicato nomeutente@protonmail.com, ma tutto è anonimo: "Non è necessaria alcuna informazione personale per creare il suo account di posta elettronica sicura. Per impostazione predefinita, non conserviamo alcun log IP che possa essere collegato al suo account e-mail anonimo. La sua privacy viene prima".

6.8.1 PGP (Pretty Good Privacy)

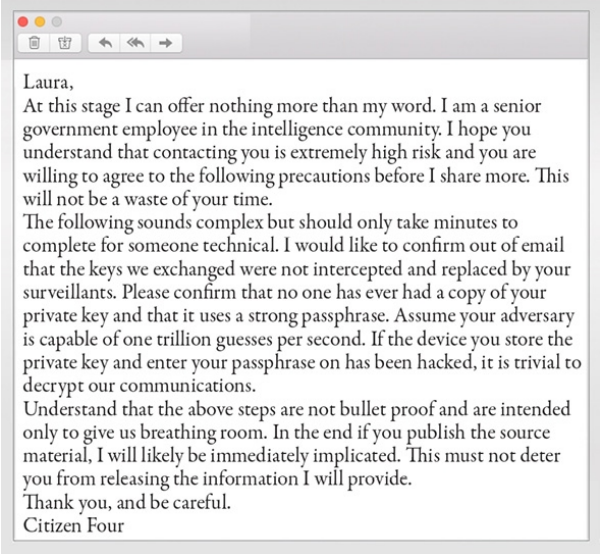
Esiste un sistema di posta crittografata che costituisce uno standard codificato a livello globale, la PGP (**Pretty Good Privacy**). È il software libero di crittografia e firma digitale più usato al mondo.

Introduciamo l'argomento con una storia vera, splendidamente raccontata nel film *Snowden* del 2016, scritto e diretto da Oliver Stone, che ci fa capire l'importanza di questo strumento.

Nel giugno del 2013 il trentenne **Edward Snowden**[35] decise di rivelare al mondo il programma di sorveglianza di massa creato dalla NSA con strumenti come PRISM e Tempora. Per fare questo fuggì dagli USA e in un albergo di Hong Kong incontrò Glenn Greenwald, giornalista del "Guardian" [Vedi Figura 24], e Laura Poitras, regista e documentarista americana. Con il documentario *Citizenfour*, che racconta la storia di Snowden e lo scandalo NSA, la Poitras ha poi vinto l'Oscar 2015 per il miglior documentario.
Tutto era cominciato nel gennaio 2013, quando Laura Poitras ricevette una e-mail crittografata da uno sconosciuto che si firmava "Citizen Four"[36] e che le offriva informazioni riservate sulle intercettazioni di massa – illegali – condotte dalla National Security Agency (NSA) e da altre agenzie di intelligence. Dopo 6 mesi di contatti con il misterioso ma credibile Citizen Four, nel giugno 2013 Laura Poitras, assieme al giornalista investigativo Glenn Greenwald e al reporter del "Guardian" Ewen MacAskill, vola ad Hong Kong dove al Mira Hotel incontra lo sconosciuto, che si rivela essere Edward Snowden.

Durante alcuni giorni di interviste, Snowden fece rivelazioni clamorose che "The Guardian" ed il "Washington Post" pubblicarono per primi e per le quali nel 2014 vinsero entrambi il Premio Pulizter.

Nella prima e-mail inviata alla Poitras, Citizen Four/Snowden scriveva:



Laura,
At this stage I can offer nothing more than my word. I am a senior government employee in the intelligence community. I hope you understand that contacting you is extremely high risk and you are willing to agree to the following precautions before I share more. This will not be a waste of your time.
The following sounds complex but should only take minutes to complete for someone technical. I would like to confirm out of email that the keys we exchanged were not intercepted and replaced by your surveillants. Please confirm that no one has ever had a copy of your private key and that it uses a strong passphrase. Assume your adversary is capable of one trillion guesses per second. If the device you store the private key and enter your passphrase on has been hacked, it is trivial to decrypt our communications.
Understand that the above steps are not bullet proof and are intended only to give us breathing room. In the end if you publish the source material, I will likely be immediately implicated. This must not deter you from releasing the information I will provide.
Thank you, and be careful.
Citizen Four

In particolare, Snowden le raccomandava:

> Vorrei la conferma tramite e-mail che le chiavi che ci siamo scambiati non siano state intercettate e sostituite da chi ti sorveglia. Conferma che nessuno ha mai avuto una copia della tua chiave privata e che la tua password è sicura. Se il dispositivo in cui hai archiviato la chiave privata e nel quale inserisci la tua passphrase è stato violato, è un gioco da ragazzi (per i tuoi sorveglianti) decifrare le nostre comunicazioni.

Cosa significano queste parole? Che Snowden stava rischiando la vita a scrivere quelle e-mail e voleva avere la certezza che nessun altro (in particolare la potentissima NSA) potesse intercettarle e leggerle. Proprio per questo, le e-mail erano **crittografate con il sistema** PGP. E Snowden decise di scrivere proprio alla Poitras, invece che a Greenwald, perché questi non usava la PGP (fu poi la Poitras a contattare Greenwald).

PGP è stato creato nel 1991 da Philip R. Zimmermann[37]. Originariamente concepito come uno strumento per i diritti umani, da PGP è nato poi OpenPGP, che è uno standard Internet "open source" per l'interoperabilità dei messaggi

protetti tramite crittografia asimmetrica (detta "a chiave pubblica"), basato sulla generazione di una coppia di chiavi, una "privata" e una "pubblica", che non coincidono.

La crittografia asimmetrica (conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica), fu introdotta nel 1976 da Whitfield Diffie[38] e Martin Hellman[39], rispettivamente un matematico e un ingegnere della Stanford University. Per questo progetto, Diffie ed Hellman hanno vinto il premio Alan Turing 2015.

PGP risolve una debolezza insita nella crittografia simmetrica: il fatto che per cifrare e decodificare un messaggio occorre una chiave segreta in possesso sia del mittente che del destinatario. Ma queste due persone potrebbero trovarsi a notevole distanza tra di loro o addirittura non conoscersi affatto e pertanto, se non esiste un canale sicuro per scambiarsi i codici di cifratura, occorre avvalersi di canali (e-mail, chat, posta convenzionale) attraverso i quali la chiave potrebbe essere intercettata.

PGP, essendo un programma di "crittografia a chiave pubblica", si basa sulla generazione di una coppia di chiavi: una "segreta" (o "privata") e l'altra "pubblica". L'utente tiene al sicuro la propria chiave segreta mentre diffonde e rende disponibile la chiave pubblica.

Quando si parla di "chiave pubblica", si intende una chiave che viene resa pubblica a tutti: per esempio Apple pubblica la sua chiave PGP al link https://support.apple.com/en-us/HT201214 per chiunque volesse inviare messaggi crittografati. Lo stesso fanno molti altri siti importanti.

Spieghiamo il funzionamento di PGP usando il classico esempio di due ipotetici personaggi, Bob ed Alice, che si scambiano un messaggio via e-mail.

1. Bob scrive il messaggio e lo cripta con la chiave pubblica di Alice (chiave che Alice ha precedentemente inviato a Bob).
2. Alice riceve il messaggio criptato da Bob e lo decripta con la sua chiave privata [Vedi Figura 25].

In sintesi:

- la chiave pubblica di Bob codifica il messaggio e la sua chiave privata lo firma
- la chiave privata di Alice consente di decodificare il messaggio che è stato cifrato con la sua chiave pubblica
- la chiave privata di Bob consente di apporre al messaggio una "firma" che identifica univocamente il mittente.

In modo più elementare si può spiegare il funzionamento di PGP paragonando l'invio di un'e-mail crittografata alla spedizione di una lettera, come rappresentato in figura.

La busta della lettera viene chiusa da Bob con il lucchetto che Alice ha fatto arrivare a Bob, cioè la chiave **pubblica** di Alice. Il lucchetto può essere aperto solo con la chiave **privata** che possiede Alice (la chiave che non verrà mai messa in rete). Quindi l'apertura della busta può avvenire solo grazie al possesso di **entrambe le chiavi**, che sono differenti, ma collegate (perché generate dallo stesso algoritmo crittografico).

Il sistema PGP consente di risolvere le due debolezze tipiche delle e-mail tradizionali, di cui abbiamo già parlato (v. par. [6.4 Come funziona la posta elettronica]), e che sono:

1. **riservatezza del contenuto**: il messaggio viene crittografato e reso illeggibile per i terzi che non posseggono le chiavi
2. **autenticità del mittente:** la chiave pubblica del mittente (che è stata precedentemente inviata al destinatario) potrà combaciare solo con la sua chiave privata. Questa funzione ci dà la certezza della provenienza del messaggio.

Il sistema descritto può sembrare complicato (e in parte lo è), ma rispetto alla PEC ha il vantaggio di non richiedere la creazione di un indirizzo dedicato e quindi non ha alcun costo. In pratica, si invia il messaggio attraverso il consueto indirizzo di posta (per es. Gmail).

All'interno del messaggio ci sarà un allegato che è il messaggio crittografato PGP, creato con il programma PGP e che può essere letto dal destinatario solo con un altro client PGP.
Esiste un solo vincolo per utilizzare PGP: deve essere usato contemporaneamente da mittente e destinatario.

PGP è diventato un protocollo standard non proprietario, quindi sono stati creati nel corso degli anni molti software per utilizzarlo con i diversi sistemi operativi più diffusi. Nel sito ufficiale di **OpenPGP**[40] sono indicati quali sono i software che utilizzano tale protocollo.

In alternativa si può consultare **GnuPG**[41], che è un software libero progettato per sostituire la suite crittografica PGP e che è completamente compatibile con gli standard PGP.
Elenco qui i principali programmi per usare PGP con i diversi sistemi operativi (ne esistono molti altri):

- **Gpg4win**[42] (per Windows)
- **GPGTOOLS**[43] (per macOS)
- **Enigmail**[44] (per il client di posta Mozilla Thunderbird)
- **Guardian project**[45] e **OpenKeychain**[46] (per Android)
- **iPGMail**[47] e **Hushmail**[48] (per iOS)

6.9 Quando ricorrere alla posta crittografata

Sicuramente l'e-mail "tradizionale" – mi piace definirla così – rimane uno strumento talmente semplice e familiare che sarà difficile sostituirla integralmente con un sistema crittografato come PGP.

PGP non sarà l'e-mail per tutti e in tutti i casi, ma vista l'importanza – sempre maggiore – dei dati che usiamo e che trasmettiamo, sarà bene valutare accuratamente l'uso di protocolli di criptazione, almeno per proteggere i nostri dati più delicati.

Concludiamo questo capitolo con le parole di Philip R. Zimmermann, nell'intervista che rilasciò nel 2015 a Wired[49]: chi meglio di lui può farci capire l'importanza della crittografia per la sicurezza e anche per la protezione dei diritti civili?

> Nelle aziende c'è la tendenza a enfatizzare cose come i firewall o i sistemi di detenzione delle intrusioni. Di certo c'è bisogno di tutto questo, ma è chiaro che queste cose possono essere violate o non sono sufficienti a garantire la protezione necessaria. Quello che serve è la crittografia, serve PGP per criptare le mail e lo stesso va fatto con tutti i tipi di documenti che vengono reputati importanti o sensibili.

---

[28] http://www.giorgiosbaraglia.it/cyberspionaggio-il-caso-eye-pyramid/

[29] https://www.securityinfo.it/2018/08/16/gli-rubano-i-bitcoin-e-lui-fa-causa-al-gestore-telefonico-per-240-milioni/

[30] http://www.repubblica.it/cronaca/2017/09/30/news/beffa_a_bruxelles_mister_confindustria_truffato_e_licenziato-176906111/

[31] https://www.ic3.gov/media/2017/170504.aspx

[32] https://www.ic3.gov/media/2018/180712.aspx

[33] https://www.cnbc.com/2017/04/27/facebook-and-google-were-victims-of-a-100-million-dollar-phishing-scam-fortune.html

[34] https://protonmail.com/it/

[35] https://it.wikipedia.org/wiki/Edward_Snowden

[36] https://www.wired.com/2014/10/snowdens-first-emails-to-poitras/

[37] https://it.wikipedia.org/wiki/Phil_Zimmermann

[38] https://it.wikipedia.org/wiki/Whitfield_Diffie

[39] https://it.wikipedia.org/wiki/Martin_Hellman

[40] http://openpgp.org/software/

[41] https://www.gnupg.org/download/index.html

[42] https://www.gpg4win.org/index.html

[43] https://gpgtools.org/

[44] https://enigmail.net/index.php/en/

[45] https://guardianproject.info

[46] https://www.openkeychain.org

[47] https://ipgmail.com

[48] https://www.hushmail.com/ios/

[49] https://www.wired.it/mobile/app/2015/03/13/phil-zimmermann-crittografia/

7

I ransomware

7.1 Che cosa sono i ransomware

Con la parola **ransomware** viene indicata una classe di malware che rende inaccessibili i dati dei computer infettati e chiede il pagamento di un riscatto, in inglese *ransom*, per ripristinarli. Tecnicamente sono Trojan horse crittografici e hanno come unico scopo l'estorsione di denaro, attraverso un "sequestro di file" realizzato mediante la cifratura che, in pratica, rende i file inutilizzabili.

Come fare a pagare il riscatto? Dietro all'industria del ransomware non ci sono semplici hacker, ma vere e proprie organizzazioni criminali che hanno raggiunto un alto livello di efficienza ed organizzazione: quindi, dopo averci criptato tutti i file, comparirà nel computer attaccato una schermata dove vengono date dettagliate istruzioni (spesso in buon italiano!) per accedere alla rete TOR e pagare il riscatto.

I numeri sono preoccupanti e – sebbene il fenomeno si sia stabilizzato rispetto alla crescita impetuosa registrata fino al 2016 – non ci sono segnali che ne facciano supporre un ridimensionamento.

Riassumiamo dunque **qualche dato**:

- Lo **scopo** è esclusivamente l'**estorsione**.
- I ransomware colpiscono **soprattutto i sistemi Windows**, ma anche MacOS (Apple) e Linux, in misura ovviamente minore perché si tratta di sistemi operativi meno diffusi. Ricordiamo che, secondo quanto riportato da Netmarketshare[50], Windows nelle varie versioni detiene circa 88% del mercato mondiale, MacOS ha il 9% e Linux il 2%.
- L'Italia è protagonista: subisce circa il 7% degli attacchi effettuati nel mondo con aumento nel 2016 del 120% rispetto al 2015 (come detto il 2016 è stato l'anno di maggior crescita). **L'Italia è il tra i primi tre paesi più colpiti nel mondo dopo gli** USA.

- I più recenti ransomware, oltre a criptare i file, fanno **anche upload** (esfiltrazione dei file), per rivenderli o chiedere un ulteriore riscatto.
- Il 93% di chi subisce attacchi ha accusato **downtime** (blocco o rallentamento delle attività aziendali) e/o perdita di dati.
- Si stima che il 5% di tutte le PMI del pianeta abbia subito un attacco ransomware fra il 2016 e il 2017.
- Il 34% delle aziende colpite dichiara di aver **pagato il riscatto almeno una volta**.
- Il **riscatto** richiesto varia in genere **da poche centinaia di euro fino a diverse migliaia**. Nell'81% dei casi il riscatto non supera i 1.000 €. Questi numeri non sono casuali, ma sono frutto di un'analisi "di marketing": i criminali sanno che se l'importo è basso e alla portata di qualunque azienda (e anche di un privato), molti pagheranno, anche qualora abbiano un backup disponibile. Questo perché un ripristino da backup potrebbe essere lungo e quindi più costoso del pagamento di un modico riscatto.
- Il **riscatto** è richiesto **in Bitcoin o altra criptovaluta**.
- Solo un incidente su 4 viene denunciato alle autorità.

7.2 Il primo ransomware

Era il 1989, quando quello che viene considerato il primo ransomware della storia ha fatto il suo debutto. Battezzato "PC Cyborg", perché i pagamenti erano diretti a una fantomatica "PC Cyborg Corporation", fu realizzato da Joseph Popp. Fu diffuso a un congresso sull'Aids mediante floppy disk infetti consegnati ai partecipanti: inserendo il floppy disk il virus si installava e criptava i file [Vedi Figura 26].

Il malware bloccava il funzionamento del computer giustificandolo attraverso la presunta "scadenza della licenza" di un non meglio specificato software. Si chiedevano 189 $ per far tornare tutto alla normalità, da pagarsi presso un ufficio postale di Panama.

Questo ransomware ebbe una diffusione estremamente limitata, perché poche persone usavano un personal computer, si trasmetteva via floppy disk (Internet

era una rete per pochi addetti ai lavori), la tecnologia di criptazione era limitata e i pagamenti erano molto più macchinosi.

[Torna al capitolo] 7.3 Un po' di storia dei ransomware

Dopo la parentesi del 1989, la vera esplosione dei ransomware comincia nel 2011-2012 e da allora non si è più fermata.

All'inizio i ransomware si limitavano a bloccare il computer, visualizzando una falsa schermata delle forze dell'ordine, dove si veniva accusati di una "attività illegale" e si intimava il pagamento di una "multa" (in genere modesta, dell'ordine dei 100 euro), per sbloccare il PC. Erano i Lockscreen Ransomware [Vedi Figura 27], il più famoso dei quali è stato il Trojan.Win32.FakeGdF (la cui prima apparizione risale al 2011), che visualizzava una finta schermata della Guardia di Finanza.

I Lockscreen Ransomware erano facilmente rimuovibili senza pagare il riscatto, anche perché il pagamento non garantiva lo sblocco del computer.

Quindi la cybercrime S.p.A. ha cambiato tecnica e verso la fine del 2012 sono comparsi i ransomware che cifravano i file.

Il capostipite fu **DocEncrypter**, ma il più famoso è stato **CryptoLocker**, la cui prima apparizione risale a settembre 2013. Il CryptoLocker è divenuto così famoso che molti media identificano con questo nome qualsiasi ransomware che cifra file.

Negli anni successivi sono comparsi **CryptoWall** (ad aprile 2014) e poco dopo **CTBLocker** (luglio 2014).

Nel 2015 fa la sua prima apparizione nel mese di febbraio TeslaCrypt 1.0, a cui seguiranno le versioni 2.0 (fine 2015), poi la 3.0 e 4.0 (2016).

Per i cybercriminali l'attività si rivela sempre più redditizia e i nuovi ransomware si moltiplicano: nel solo anno 2016 sono state create 62 nuove "famiglie" di ransomware e di queste 47 (pari al 75%) sono state sviluppate da cybercriminali russi.

Dopo la crescita esponenziale dei primi anni, nel 2018 il fenomeno ransomware sembra essersi stabilizzato. In parte questo è dovuto a un aumento di consapevolezza da parte degli utenti (ma ancora del tutto insufficiente...), per altra parte sono nate altre tipologie di attacchi, tra i quali il Cryptojacking (v. cap. 3 "Perché ci attaccano").

Comunque anche nel 2018 si sono registrati alcuni attacchi clamorosi: il comune di Atlanta[51] (Georgia) è stato colpito a inizio marzo dal ransomware SamSam, lo stesso che due mesi prima aveva bloccato l'ospedale Hancock Health in Indiana[52], che in quell'occasione aveva deciso di pagare il riscatto di 55.000 $, nonostante avesse a disposizione il backup dei dati.

La città di Atlanta ha avuto bloccati la maggior parte dei suoi servizi online per oltre dieci giorni: pagamento dei biglietti dei parcheggi, convocazioni in tribunale, rapporti della polizia, pagamento delle bollette e accesso alla documentazione.

Il municipio avrebbe ricevuto una richiesta di riscatto con modalità diversificate: 6.800 $ per ogni singola macchina o un "forfait" di 51.000 $, ma – a differenza dell'ospedale Hancock Health – ha scelto di non pagare e di ripristinare i sistemi con i propri backup, con costi stimati di alcuni milioni di dollari!

A fine marzo è toccato a Boeing, colpita da WannaCry (ne parliamo in seguito).

Ad agosto 2018 i ricercatori di sicurezza del MalwareHunterTeam hanno individuato un nuovo ransomware, battezzato Ryuk, usato per attacchi mirati a un numero limitato di vittime di alto profilo negli Stati Uniti ed in Germania. La richiesta di riscatto è esorbitante: fino a 50 Bitcoin, (circa 276.000 euro). Si sospetta che dietro a questi attacchi ci sia il gruppo Lazarus, gli hacker di stato della Corea del Nord.

Quindi il ransomware, da epidemia virulenta, si è trasformato in un fenomeno endemico, che continua in ogni modo a fare vittime. Questi i ransomware più famosi:

- **Cryptolocker**: 2013.
- **CryptoWall**: inizio 2014.
- **CTB-Locker**: metà 2014. Ha migliaia di varianti.

- **TorrentLocker**: febbraio 2014.
- **Ransom32**: fine dicembre 2015.
- **TeslaCrypt**: febbraio 2015. A maggio 2016 gli autori hanno rilasciato la chiave Master Key e hanno chiuso il progetto.
- **Locky**: febbraio 2016 (via macro in file Word).
- **CryptxxX**: inizio 2016 (attraverso **pagine Web** compromesse).
- **Petya**: marzo 2016.
- **Cerber**: marzo 2016.
- **PokemonGo**: agosto 2016. Nella richiesta di riscatto si presentava con l'immagine di Pokemon, allora molto di moda.
- **Popcorn**: fine 2016 (dilemma: pagare o diffonderlo?).
- **WannaCry** (maggio 2017): il più veloce a propagarsi, grazie a una vulnerabilità di Windows.
- **NotPetya** (giugno 2017): probabilmente quello che ha creato i danni maggiori a livello mondiale.
- **Bad Rabbit** (ottobre 2017).

7.4 T [Torna al capitolo] ipi ed esempi di ransomware

CryptoLocker - TorrentLocker

È famoso al punto che spesso si parla di "Cryptolocker" per definire un ransomware.

Compare a settembre 2013, cripta i file con estensione .encrypted attraverso un algoritmo "forte" come AES (Advanced Encryption Standard). La richiesta di riscatto è di 300/600 euro (in Bitcoin), da pagarsi attraverso la rete TOR su siti con dominio ".onion" (nel Dark web).

Generalmente si diffonde attraverso un allegato di posta elettronica che sembra provenire da istituzioni legittime. Si presenta in genere come un allegato zip che contiene un file eseguibile (anche se sembra un word o un pdf).

Il file non è visibile come ".exe" perché l'attaccante sfrutta il fatto che i sistemi Windows non mostrano di default le estensioni dei file e un contenuto così creato viene visualizzato come .pdf nonostante sia un eseguibile, inducendo gli utenti ad

aprirlo ed eseguirlo. Una volta installato, il malware inizia a cifrare i file del disco rigido e delle condivisioni di rete mappate localmente con la chiave pubblica e salva ogni file cifrato in una chiave di registro.

Nel 2014 CryptoLocker è stato sostituito da un nuovo prodotto con il nome di TorrentLocker.

CryptoWall

Appare nel 2014 in aprile, l'estensione dei file è varia, utilizza l'algoritmo (a doppia chiave o asimmetrico) RSA-2048 e richiede un riscatto di 500/1000 $ (in Bitcoin).

CTBLocker (Curve Tor Bitcoin Locker)

È stato uno dei più diffusi a partire da luglio 2014. Utilizza un'estensione causale, ma di 7 caratteri, con crittografia AES e riscatto di 1-2 Bitcoin, ovviamente da pagare via rete TOR.

TeslaCrypt

Comparso a febbraio 2014, dalla versione 1.0 è arrivato fino alla versione 4.0. Poi a maggio 2016 gli autori hanno rilasciato la chiave Master Key e hanno chiuso il progetto. Ma fino al quel momento è stato quello che ha realizzato il maggior fatturato: nei primi 5 mesi del 2016 ha avuto una diffusione del 35% di tutti i ransomware. Utilizzava l'algoritmo AES con richiesta di riscatto pari a 500/1000 $.

Locky

Rilasciato a febbraio 2016, veicolato in genere attraverso macro in file Word, utilizzava una doppia crittografia: l'algoritmo (a doppia chiave o asimmetrico) RSA-2048 e quello simmetrico AES-128. Richiedeva un riscatto di 0,5-1 Bitcoin.

In poco tempo è diventato famoso per gli attacchi portati ad alcuni ospedali americani, come l'Hollywood Presbyterian Medical Center in Los Angeles a febbraio 2016 e il Methodist Hospital in Henderson (Kentucky) a marzo 2016.

Nel caso dell'Hollywood Presbyterian Medical Center, dopo un completo blocco dell'operatività per dieci giorni, l'ospedale ha pagato un riscatto di 40 Bitcoin

(circa 17.000 dollari), come ha dichiarato in un comunicato ufficiale Allen Stefanek, presidente e CEO dell'ospedale.

Petya

La prima versione, con schermata rossa [Vedi Figura 28], risale a marzo 2016. Poi sono seguiti le versioni Petya.B (schermata verde) a maggio 2016, la Petya.C (ancora verde) a luglio 2016, e la Petya.D "GoldenEye" (schermata gialla) a dicembre 2016.

Oltre a cifrare i file, cifrava (è il primo caso) anche la Master Boot Record (MBR) del disco rendendo impossibile anche l'avvio del computer, con algoritmo Salsa20. Richiesta di riscatto di 0,99 Bitcoin.

Prendeva di mira soprattutto gli utenti aziendali poiché veniva distribuito tramite e-mail di spam che fingevano di contenere domande di assunzione.

Popcorn

Compare a fine 2016 e ha una caratteristica che dimostra l'evoluzione del "marketing" dei ransomware. In pratica per riavere i propri file (la richiesta di riscatto è di 1 Bitcoin e ci sono 6 giorni per pagare) viene "consigliato" di inviare un link infetto ad altre persone: se almeno due pagheranno, "tu riavrai i tuoi file gratis". Una vera e propria istigazione a delinquere! I cybercriminali si dichiarano "studenti siriani" e dicono di farlo per acquistare "cibo e medicine" [Vedi Figura 29].

WannaCry

Un altro attacco che ha occupato le cronache internazionali è stato WannaCry[53], ovvero "voglio piangere". A maggio 2017, esattamente venerdì 12, il virus ha inchiodato i computer di mezzo mondo, grazie a una falla che si trovava nella funzionalità SMB Server di Windows: un "buco" noto e anche già "tappato" dall'azienda di Redmond con una cosiddetta patch, la numero MS17-010.

I computer infettati, quindi, non avevano installato l'aggiornamento di sicurezza.
La peculiarità originale di WannaCry, rispetto ad altri ransomware più "classici", è che si tratta di un malware costituito da due componenti che operano in successione:

1. Un exploit (un malware realizzato appositamente per sfruttare una "falla" di un sistema) **che sfrutta la vulnerabilità SMBv1** (un protocollo di condivisione di file di rete, Server Message Block, usato da sistemi Microsoft Windows) per attaccare il computer obiettivo. In questo modo WannaCry si propaga in modo automatico agli altri computer e questo spiega l'altissima velocità di diffusione.
2. Un ransomware vero e proprio che esegue la cifratura dei files.

La richiesta di riscatto era di 300 $, da pagarsi in Bitcoin su uno dei tre conti indicati.

Molti ricercatori del settore hanno considerato WannaCry "un attacco di proporzioni mai viste". Kaspersky Lab, firma illustre nel mondo della sicurezza informatica, ha registrato più di 300.000 attacchi in 150 nazioni, incluse Russia, Cina, Italia, India, Egitto e Ucraina.

Europol, agenzia dell'Unione europea impegnata nel contrasto alla criminalità, ha parlato di "un attacco senza precedenti che richiede indagini internazionali".

Uno dei paesi più colpiti, in termini di conseguenze, è stato il Regno Unito, dove WannaCry ha bloccato almeno 25 ospedali e messo in crisi l'intero sistema sanitario britannico. Questo è stato possibile proprio perché negli ospedali del Regno Unito c'erano ancora molte migliaia di computer con Windows XP (sistema non più supportato da parte di Microsoft dall'aprile 2014). Un'indagine condotta da Motherboard[54] (effettuata nel 2016) aveva rilevato almeno 42 strutture del National Health Service (NHS) che stavano usando XP.

Ma si sono registrati attacchi in tutta Europa e nel resto del mondo. Tra gli altri Nissan e Renault in Francia, la società di telecomunicazioni Telefonica, Iberdrola e le banche BBVA e Santander in Spagna, FedEx in USA e molti altri. In Germania sono stati colpiti i computer della Deutsche Bahn (le ferrovie tedesche). In Giappone è toccato a Hitachi, Nissan e East Japan Railway. In Russia colpiti RZD (Russian Railroad), la banca VTB, Megafon. Anche l'Italia entra nell'elenco con l'Università Bicocca a Milano (che a quanto risulta è stata attaccata attraverso una chiavetta USB contenente il malware).

Si stima che sia costato, nel mondo, tra i 4 e gli 8 miliardi di dollari.

Ma, nonostante la propagazione a macchia d'olio, WannaCry è stato considerato un flop dal punto di vista economico: l'ammontare dei ricavi raccolti dai cybercriminali si aggira intorno ai 100mila dollari (dato rilevato due settimane dopo l'attacco, analizzando i movimenti dei tre conti Bitcoin utilizzati).

Una cifra modesta, soprattutto considerato che in genere i malware hanno come obiettivo proprio il pagamento di un riscatto. Questo fa ritenere che l'attacco non sia stato fatto per soldi, ma più probabilmente a scopo destabilizzante o dimostrativo. Il principale sospettato è la Corea del Nord, con il suo gruppo di hacker noti con il nome Lazarus. A sostenerlo sono Symantec e Kaspersky Lab, che hanno rilevato nel codice del malware alcune similitudini con precedenti attacchi: quello alla Banca Centrale del Bangladesh del 2016 (il più grande furto informatico di sempre, 82 milioni di dollari rubati), ma soprattutto quello alla Sony Pictures Entertainment, la casa di produzione attaccata per aver prodotto *The interview*, film satirico contro il leader nordcoreano Kim Jong-un.

Nel 2018 WannaCry ha colpito ancora: a marzo è stata attaccata Boeing[55], il principale produttore di aeromobili al mondo. L'azienda ha confermato l'accaduto, specificando però che il problema ha riguardato solo un numero limitato di sistemi della divisione commerciale, non quelli dell'impianto produttivo.

NotPetya (o EternalPetya)

NotPetya[56] esplode in modo violento martedì 27 giugno 2017. Sfrutta, al pari di WannaCry, la vulnerabilità di Windows SMB e l'exploit Eternalblue creato da NSA, la National Security Agency americana, per propagarsi nelle reti aziendali. Si è diffuso soprattutto in Ucraina, ma l'Italia è risultato essere il secondo paese più colpito.

Il riscatto richiesto è di 300 $. Ma la richiesta di riscatto di NotPetya era solo un espediente: l'obiettivo del malware era puramente distruttivo. Crittografava in modo irreversibile le Master Boot Records dei computer, bloccandoli. Qualsiasi pagamento di riscatto da parte delle vittime era inutile.

È ritenuto il più distruttivo cyberattacco mai compiuto con danni stimati per circa 10 miliardi di dollari. "Non ci sono state perdite di vite umane, ma è stato

l'equivalente di una bomba nucleare per ottenere una piccola vittoria tattica", ha dichiarato Tom Bossert, che all'epoca dell'attacco era il funzionario più anziano del presidente Trump incaricato alla cybersecurity.

Vengono attaccati tra gli altri: la Merck (settore farmaceutico) che ha subito l'interruzione delle operazioni a livello mondiale, la Reckitt Benckiser che ha denunciato mancate vendite per circa 110 milioni di sterline. E poi la Banca centrale dell'Ucraina, il gigante russo Rosneft, il gruppo di pubblicità WPP, la TNT Express, la multinazionale francese Saint-Gobain...

Una delle aziende più pesantemente colpite è stato il colosso danese dei trasporti navali Moller-Maersk[57], che ha dichiarato danni per 250-300 milioni di dollari (4.000 server e 45.000 computer da reinstallare!). Questo è quello che si racconta di quel pomeriggio di giugno a Copenaghen quando uno dei più grandi gruppi di spedizioni marittimi del mondo ha cominciato letteralmente a "perdere la testa":

> In tutti i quartier generali di Maersk Ship Management B.V. la crisi stava cominciando a diventare chiara. Nel giro di mezz'ora, i dipendenti di Maersk stavano correndo per i corridoi, urlando ai loro colleghi di spegnere i computer o disconnetterli dalla rete di Maersk prima che il software dannoso potesse infettarli.
>
> Alcuni addetti del dipartimento IT presero d'assalto le sale riunioni per disconnettere qualsiasi macchina collegata in rete, altri membri dello staff scavalcavano i cancelli con chiave magnetica bloccati dal malware misterioso per diffondere l'avviso ad altre sezioni dell'edificio.
>
> La disconnessione dell'intera rete globale di Maersk aveva richiesto allo staff IT dell'azienda 2 ore di lavoro (probabilmente di panico...).
>
> Alla fine di tale processo, a ogni dipendente era stato ordinato di spegnere il computer e lasciarlo sulla scrivania. Anche i telefoni digitali erano stati resi inutilizzabili durante l'arresto della rete di emergenza.

Questo è quello che è successo in una grande azienda, che ha 800 navi che trasportano decine di milioni di tonnellate di merci e che rappresenta quasi un quinto della capacità di trasporto navale di tutto il mondo...

Per questo attacco i governi di Stati Uniti e Gran Bretagna nel febbraio 2018 hanno accusato la Russia[58], i cui hacker vicini al governo ed in particolare al GRU, il servizio segreto militare, sono sempre molto attivi.

Bad Rabbit

Bad Rabbit[59] [Vedi Figura 30] compare martedì 24 ottobre 2017. Cifra i file e il disco fisso e presenta notevoli somiglianze con NotPetya. Il principale vettore di infezione sono i siti compromessi (mediante un finto installer di Adobe Flash Player) con la tecnica del drive-by-download. Come il suo predecessore, anche Bad Rabbit colpisce prevalentemente reti aziendali. Si ha notizia di attacchi a più di 200 aziende in diversi paesi nel mondo, prevalentemente in Russia, Ucraina (la metropolitana di Kiev e l'aeroporto di Odessa), Germania, Giappone, e Turchia.
La richiesta di riscatto era di 0,05 Bitcoin (circa 235 euro).

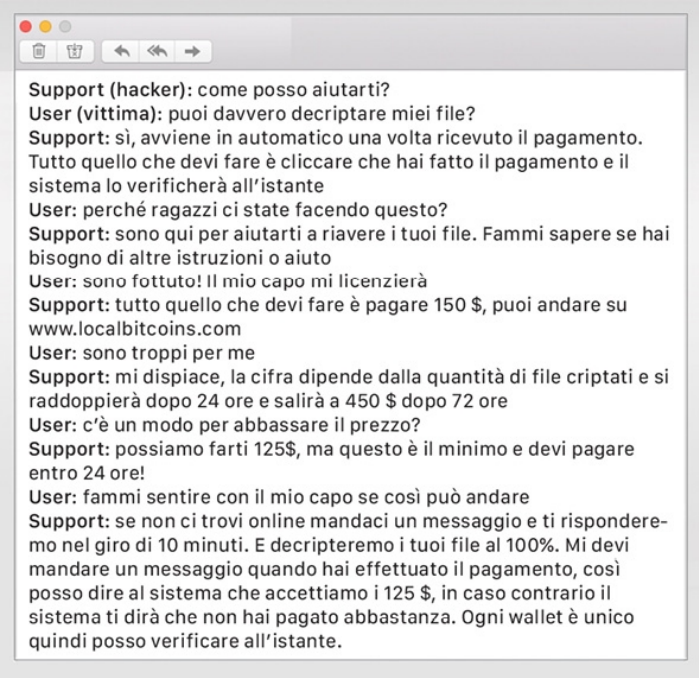
7.5 L'evoluzione dei ransomware: R&D e marketing

Il business legato ai ransomware funziona molto bene e quindi, come succede nelle aziende, anche nella cybercrime S.p.A. la ricerca e lo sviluppo sono attivi per incrementare il "fatturato".

7.5.1 In chat con il nemico

Poiché un buon servizio di customer care è alla base di ogni business di successo, alcuni hacker si sono attrezzati con servizio clienti via chat (non siamo ancora al numero verde!).
Quella che segue è la trascrizione di una chat realmente avvenuta tra una vittima del ransomware JIGSAW (**User**) e il cyber criminale di turno (**Support**).

Come si può vedere, l'hacker risponde in modo cortese e professionale, ma è anche pronto a tagliare corto quando le domande diventano troppo insistenti.



7.5.2 Ransomware as a Service (RaaS)

Un altro sviluppo – inquietante – di questo fenomeno è il "Ransomware as a Service"[60].

Oggi nel Dark web, attraverso la rete TOR, vengono offerti software ransomware che chiunque può "acquistare", personalizzare e diffondere per infettare vittime, criptare i loro documenti e chiedere un riscatto. Il tutto a condizioni molto vantaggiose: nel caso di Princess Evolution l'acquirente si trattiene il 60% del ricavato del riscatto. Gli autori del codice malevolo, invece, si "accontenteranno" del restante 40%.

Satan [Vedi Figura 31] è ancora più "conveniente": gli sviluppatori trattengono solo il 30% dei riscatti (la percentuale può essere ridotta se gli "incassi" sono alti!), il resto va al "cliente".

Alcune di queste piattaforme offrono un "configuratore" per poter personalizzare il malware secondo i propri gusti e anche un pannello di controllo che mostra in tempo reale il numero di utenti infettati, il numero di ransomware che l'utente ha messo in circolazione e l'ammontare di denaro accumulato fino a quel momento.

Il grave rischio del Ransomware-as-a-Service è che contribuisca ad abbassare la soglia d'ingresso al cybercrime, permettendo anche a persone poco esperte, ma

spregiudicate, di compiere estorsioni e attacchi informatici. Dall'altra parte, i veri criminali (quelli bravi!) hanno modo di ampliare il loro business creando una rete capillare di "rivenditori" del loro prodotto.

7.6 Come si prende un ransomware: i vettori d'infezione

I vettori d'infezione utilizzati dai ransomware sono sostanzialmente i medesimi usati per gli altri tipi di attacchi malware. Li elenchiamo qui, partendo da quelli più frequenti:

1. **Con e-mail di phishing** (di cui abbiamo già ampiamente parlato): è il più diffuso, perché purtroppo funziona molto bene. Attraverso questa tecnica, che sfrutta il social engineering, vengono veicolati oltre il 75% dei ransomware. A tutti noi sarà capitato di ricevere e-mail da spedizionieri, o con allegate false bollette. Sono evidentemente e-mail di phishing, ma le statistiche ci dicono che nel 30% dei casi questi messaggi vengono aperti dagli utenti e addirittura in oltre il 10% dei casi vengono cliccati anche gli allegati o i link presenti nelle e-mail, permettendo così l'infiltrazione del malware!
2. **Attraverso la navigazione su siti compromessi**: il cosiddetto "*drive-by download*" (letteralmente: scaricamento all'insaputa) da siti nei quali sono stati introdotti (da parte di hacker che sono riusciti a violare il sito) Exploit kit che sfruttano vulnerabilità dei browser, di Adobe Flash Player, Java o altri. Si presentano, per esempio, come banner pubblicitari o pulsanti che ci invitano a cliccare. A quel punto verremo indirizzati su siti malevoli, diversi dall'originale, ove avverrà il download del malware.
3. **All'interno (in bundle) di altri software** che vengono scaricati, per esempio programmi gratuiti che ci promettono di "crackare" software costosi per utilizzarli senza pagare. È una pratica che oggi è diventata assai pericolosa, perché il crack che andremo a scaricare sarà un eseguibile (.exe), dentro il quale ci potrebbe essere una brutta sorpresa.
4. **Attraverso il desktop remoto RDP** (Remote Desktop Protocol, in genere sulla porta 3389): sono attacchi di tipo "brute force" per scoprire le password utilizzate per accedere al server via Desktop Remoto. Individuata la password

d'accesso, l'attaccante si "logga" con le credenziali della vittima ed esegue il ransomware manualmente sul computer. Quindi è molto importante utilizzare password robuste e disabilitare il servizio di desktop remoto se non utilizzato. Uno dei ransomware più noti è LOKMANN.KEY993.

7.7 La dinamica dell'attacco

Nella infografica di figura 32 [Vedi Figura 32] è illustrata in dettaglio la modalità di attacco di un ransomware veicolato attraverso e-mail (il caso più frequente). Le caselle in rosso stanno a indicare le fasi nelle quali i nostri sistemi di difesa (antispam ed antivirus) falliscono e non riescono a bloccare l'attacco, come purtroppo frequentemente accade.

Illustriamo in dettaglio le fasi dell'attacco:

1. **L'utente riceve e-mail (di phishing) con un allegato o un link.**
2. **Il software antispam non la blocca:** in genere i migliori antispam hanno un'efficacia molto elevata (fino al 99%), ma può accadere che un'e-mail riesca a passare e sarà quella costruita meglio, quindi più subdola.
3. **Il file allegato può essere un file malevolo:** un eseguibile (exe, com, scr, js, vbs), un file compresso (.zip o altro) o anche un file di Office (.docx, .xlsx, ecc.) contenente una macro. In realtà i file potenzialmente pericolosi sono molti, quindi sarà sempre opportuno fare attenzione prima di tentare di aprirlo. Nel dubbio è consigliabile fare una "preview" (sola visualizzazione) senza eseguirlo, utilizzando le funzioni di visualizzazione che sono disponibili (es. Office Viewer di Microsoft o il comando "barra spaziatrice" in Apple).
4. **L'utente clicca sul link o apre l'allegato e attiva il trojan:** ci deve essere sempre l'intervento (l'errore!) umano. Come già detto, limitarsi alla lettura del testo dell'e-mail non crea danni.
5. **L'antivirus non blocca il file malevolo:** questo passaggio rappresenta l'ultima linea di difesa, prima che l'attacco possa avere effetto. Avere un antivirus è importante, ma dobbiamo essere consapevoli che non ci potrà proteggere da tutte le minacce. I normali software antivirus sono "signature based", cioè

operano facendo il confronto tra il file da analizzare e un loro archivio in cui sono schedate le "firme" (signature) di tutti i malware conosciuti a quel dato momento. La firma (detta anche "fingerprint") individua univocamente il file come se fosse la sua impronta digitale. Per superare i controlli antivirus sono comparsi i malware "**polimorfi**": in pratica è sufficiente modificare anche pochi byte di un virus perché la sua firma sia totalmente diversa e quindi l'antivirus non la riconosca. Vengono generate (ed è un procedimento facile ed estremamente veloce) infinite varianti dello stesso malware e queste per un certo tempo oltrepasseranno l'antivirus. Fino a che questi non le riconoscerà e le schederà nel proprio database.

6. **A questo punto l'attacco ha inizio**: l'agent trojan (detto anche "dropper"), che è stato scaricato, è entrato nel computer della vittima e inizia a compiere alcune operazioni. Queste non sono sempre le stesse per tutti i malware, ma qui ne riassumiamo le più diffuse: il malware si collega a un server C&C (Command & Control) dal quale scaricherà i file più utili per eseguire la criptazione; nei ransomware più raffinati (e ce ne sono!) verranno scelti gli strumenti più adatti, dopo aver analizzato il sistema della vittima (quale sistema operativo usa, quali sono i software di protezione installati, ecc.).
7. **Il criptatore agisce**: chiude i processi di sistema importanti, elimina i punti di ripristino, cancella le "shadow copies" di Windows, cripta i file delle estensioni più note (Office, pdf, cad, db, img, audio, video, ecc.). Ed in genere procede per cartelle, spesso – ma non è una regola – seguendo l'ordine alfabetico. Fa questo sulla macchina attaccata e sui dischi e computer a essa collegati in rete. I file criptati vengono modificati con algoritmi crittografici e talvolta ne viene modificata l'estensione (alcuni esempi: ".encrypted", ".micro", ".locky", ".zepto", ecc.). Questo processo può impiegare ore se i file sono numerosi, quindi il fattore tempo è una variabile importante: se sospettiamo che sia in corso un attacco del genere, sarà utile **scollegare il computer dalla rete** (per evitare che ne vengano infettati altri) e addirittura **spegnerlo**. Così facendo potremmo riuscire a salvare almeno una parte dei file.
8. **Compare la richiesta di riscatto:** quando il ransomware ha completato il suo "sporco lavoro" – e solo allora – viene presentata la richiesta di riscatto, spesso anche in lingua italiana. Come trovarla? State tranquilli, faranno in modo che la

vediate bene: la richiesta di riscatto spesso addirittura viene inserita in ogni cartella criptata, oppure si modifica lo sfondo del desktop. Nella richiesta di riscatto vengono riportati l'ID della vittima, l'indirizzo del wallet (portafoglio) in Bitcoin dove pagare la somma richiesta, il link TOR-Onion (nel Dark web) con le istruzioni per il pagamento e quanto tempo ci viene concesso per farlo (in genere da 3 a 6 giorni, dopodiché o i file vengono distrutti in modo definitivo o il prezzo raddoppia).

FAQ ▶ COME VIENE FATTA LA CRITTOGRAFIA DEI FILE?

Non è possibile generalizzare, perché, come in tutte le opere dell'ingegno umano, ci sono i ransomware costruiti meglio e quelli più scadenti.
In quelli migliori si utilizza Salsa20 (come nel caso di Petya), ma soprattutto l'algoritmo AES (Advanced Encryption Standard), che esegue una crittografia simmetrica, a chiave singola (con chiavi a 128, 192, 256 bit). Con una chiave a 256 bit il numero delle combinazioni possibili è 2256: in pratica un numero con 77 zeri!
Viene utilizzato anche l'algoritmo RSA (crittografia asimmetrica a doppia chiave) quando il ransomware si collega ai server di C&C (Command & Control) per lo scambio delle chiavi.
Quindi se i file sono stati cifrati con algoritmi come AES, RSA o Salsa20, è impossibile decriptarli, a meno che non si conosca la chiave di cifratura utilizzata o che il ransomware presenti dei bug (quali, per esempio, chiave con cifratura debole o salvata nel computer della vittima).
Talvolta succede, ma gli hacker sono veloci a correggere i bug e aggiornano i programmi: TeslaCrypt era arrivato alla versione 4.0 (prima di chiudere), anche Petya ha avuto 4 versioni, di Cerber esistono almeno 5 aggiornamenti.

7.8 Come proteggersi dai ransomware: la prevenzione

Nonostante la virulenza e la diffusione dei ransomware, ci sono regole, spesso anche piuttosto semplici, che ci possono aiutare a evitarli. Per molte di esse, parlerei di norme di "cyber hygiene", azioni che dovrebbero entrare nei nostri comportamenti abituali. Anche perché queste attenzioni ci proteggono non solo dai ransomware, ma da qualsiasi tipo di cyber attacco. Le elenchiamo qui in

sintesi:

- **Non aprire mai gli allegati di e-mail di dubbia provenienza**. Nel dubbio è consigliabile chiedere al mittente (non con un rispondi allo stesso indirizzo!) se quella e-mail è autentica!
- **Fare attenzione alle e-mail provenienti anche da indirizzi noti**: potrebbero essere stati hackerati secondo la modalità di falsificazione nota come "spoofing".
- **Abilitare l'opzione "Mostra estensioni nomi file"** nelle impostazioni di Windows: i file più pericolosi hanno l'estensione .exe, .zip, js, jar, scr, ecc. Se questa opzione è disabilitata, non riusciremo a vedere la reale estensione del file.
- **Disabilitare la riproduzione automatica ("autorun") di chiavette USB, CD/DVD e altri supporti esterni** e, più in generale, **evitare di inserire questi oggetti nel nostro computer se non siamo certi della provenienza**. Questa modalità di attacco si chiama "**baiting**": consiste nell'utilizzare un'**esca** (*bait*) per ingannare una persona in grado di accedere a un determinato sistema informatico (una sorta di cavallo di Troia). In pratica viene lasciato incustodito in un luogo comune (ingresso dell'azienda, mensa, bagno) un supporto di memorizzazione come una chiavetta USB o un hard disk contenenti malware che si attiveranno appena l'oggetto sarà collegato al computer. E la curiosità umana fa sì che in molti casi questa esca funzioni e la persona inserisca la chiavetta sconosciuta nel proprio computer. Come vedremo al cap.9.2.3. con una chiavetta USB sono riusciti a far saltare una centrale nucleare in Iran!
- **Disabilitare l'esecuzione di macro** (che sono veri e propri programmi incorporati in un file) **da parte dei programmi Office** (Word, Excel, PowerPoint). Una macro malevola potrebbe essere contenuta in un allegato in formato Office e attivarsi automaticamente non appena il file viene aperto.
- **Aggiornare sempre i sistemi operativi e i browser**. In generale è buona regola installare sempre e subito le "patch" (gli aggiornamenti) di sicurezza che ci vengono proposte dai produttori dei software che abbiamo installato. Un browser aggiornato è più sicuro e rappresenta esso stesso una protezione.
- **Utilizzare** – quando possibile – **account senza diritti da amministratore**: se viene violato un account con privilegi e accessi di amministratore, l'attaccante potrà acquisire gli stessi privilegi per compiere più azioni e fare maggiori danni.

Viceversa, un utente non-amministratore ha privilegi limitati e le stesse limitazioni si trasferiranno all'attaccante (v. par. [14.5 POLP: il principio del Minimo Privilegio]).

- **Installare servizi antispam efficaci ed evoluti**: gli antispam non riusciranno a bloccare tutte le e-mail di phishing, ma i migliori riescono a raggiungere un'efficienza comunque vicina al 99%.
- **Implementare soluzioni di tipo "User Behavior Analytics"** (UBA) (v. par. 14.2) sulla rete aziendale. Questi strumenti rappresentano oggi la protezione più avanzata contro i ransomware. È noto infatti che questi malware presentano una serie di comportamenti tipici (accesso/scrittura a cartelle di sistema, collegamento a server esterni per il download dei file di criptazione, ecc.). Gli UBA analizzano perciò il comportamento di ciascun computer dell'azienda e sono in grado di capire se si stanno verificando eventi "anomali" (quali per esempio un traffico dati superiore alla media, l'accesso a indirizzi IP classificati come malevoli, l'accesso e la scrittura in cartelle di sistema che non dovrebbero essere utilizzate). Alla rilevazione di eventi anomali e sospetti, possono isolare il computer incriminato e bloccare, o quantomeno circoscrivere, l'attacco.
- **Implementare l'uso di Sandboxing**: questi strumenti sono in genere presenti nei sistemi UBA (di cui al punto precedente) e consentono di analizzare in un ambiente isolato (appunto la "Sandbox") i file sospetti in entrata.
- **Assicurarsi che i plug-in che si utilizzano** (Java, Adobe Flash Player, ecc.) **siano sempre aggiornati**: questi plug-in rappresentano una via d'ingresso preferenziale per la maggior parte dei cyber attacchi; averli sempre aggiornati riduce le vulnerabilità di cui sono affetti, anche se non le elimina completamente.
- **Fare sempre attenzione prima di cliccare su banner o finestre pop-up in siti non sicuri**: come ho già spiegato, i ransomware ci possono colpire non solo attraverso il phishing, ma anche visitando siti che siano stati "infettati", con la modalità definita "drive-by download".
- **Backup frequente dei propri dati**. Questa è una regola fondamentale: se nonostante tutto un ransomware riesce a colpirci – e potrebbe succedere – l'unica salvezza è avere i propri dati salvati in un altro luogo. Ed è importante che il backup venga eseguito spesso e in modo completo. In assenza di un

backup rimane solo l'opzione di pagare il riscatto... (v. cap.21.3 L'importanza del Backup: 3-2-1 Backup Strategy).

In conclusione:

In ogni cyber attacco c'è sempre almeno un ERRORE UMANO: il ransomware non può agire senza una nostra azione che glielo permetta!

I sistemi antivirus installati non sono più sufficienti a garantire una difesa totale (soprattutto per il fenomeno del polimorfismo).

Non sottovalutare il **fattore umano**: è importante formare il personale a tutti i livelli. Purtroppo l'errore o la trascuratezza di una sola persona può giungere a compromettere i dati di tutta l'azienda.

In sintesi: **Il miglior anti-phishing è sempre l'UTENTE.**

7.9 Cosa fare se siamo stati colpiti da un ransomware

Se sullo schermo del nostro computer compare un'immagine come quella della figura 33 [Vedi Figura 33]: è il segnale che un ransomware ha colpito ed ora ci presenta – come una sentenza – la richiesta di riscatto. Cosa possiamo fare ora di differente di farsi prendere dal panico e dalla disperazione?

Quando compare questo messaggio (in genere è un file immagine) significa che il ransomware ha già concluso il processo di criptazione dei nostri files. I dati sono stati sequestrati e ora bisogna decidere cosa fare. In questa malaugurata ipotesi, le opzioni sono sostanzialmente quattro:

1. **Ripristinare i file da un backup** (la soluzione migliore, anzi la sola che dovrebbe prendere in considerazione un'azienda ben organizzata).
2. **Cercare un "decryptor"** in rete per decriptare i file.
3. **Non fare nulla** e perdere i propri dati.
4. **Pagare il riscatto** (*ransom*).

Vediamole ora più in dettaglio.

7.9.1 Ripristinare i file da un backup

È la soluzione migliore e possiamo averla a disposizione se abbiamo operato con attenzione e ci siamo organizzati con una corretta gestione di salvataggio periodico dei nostri dati. Infatti per poter fare un ripristino è necessario avere una copia di backup che sia:

1. disponibile,
2. recente,
3. funzionante.

Ho voluto evidenziare questi tre requisiti, perché troppo spesso ci si trova in aziende che – in piena emergenza ransomware, con i computer bloccati – non hanno la certezza dello stato del backup fino a quando non vanno a esaminarlo. Salvo scoprire che: è incompleto (alcune cartelle non sono state copiate), non è aggiornato (perché da un po' di tempo non veniva più fatto...) e altre amenità del genere, purtroppo veramente accadute.
Anche nello scenario peggiore di mancanza di un backup, conviene fare un'indagine approfondita che ci potrebbe far recuperare copie dei file più importanti: per esempio all'interno delle e-mail inviate e ricevute o nel cloud.

UN PREZIOSO CONSIGLIO

Molti non conoscono questa opzione, che potrebbe "salvare la vita (dei file...)": è possibile recuperare i file grazie al cloud. Dropbox e altri servizi cloud ci possono aiutare, perché prevedono il "versionamento" (versioning) dei file, quindi si può recuperare una versione precedente, non cancellata dal ransomware.
Spieghiamo meglio come fare: la cartella (Dropbox o Google Drive o altro...) all'interno del nostro computer sarà stata criptata come tutte le altre. Essendo sincronizzata con il server cloud, anche qui i file saranno crittografati. Ma il ransomware non riesce a fare "tabula rasa": le versioni precedenti e quelle cancellate rimangono conservate sui server del servizio cloud. Basterà accedervi (via web), attivare l'opzione che ci permette di vedere i file cancellati (in Dropbox il comando è: "Mostra file eliminati") o la "cronologia delle versioni" per poi recuperarli uno per uno.

Se siamo in possesso di un backup utilizzabile, occorre però procedere prima a una bonifica della macchina (o delle macchine) infettate, prima del ripristino dei dati. La bonifica può essere fatta con più scansioni antivirus per assicurarsi che il software dannoso sia stato rimosso, ma per essere certi al 100% che non ci siano più tracce di qualsiasi tipo di malware, è consigliabile procedere a una **formattazione completa** del computer attaccato. Solo a questo punto si può procedere al ripristino dei dati da backup.

7.9.2 Cercare un "decryptor" in rete per decriptare i file

La grande proliferazione delle varietà di ransomware nel corso di questi ultimi 2-3 anni ha fatto sì che i maggiori vendor di sicurezza mondiali abbiamo cercato di trovare gli "antidoti" efficacia questi malware. E in alcuni casi ci sono anche riusciti bene: per alcune versioni di ransomware meno recenti sono stati creati (e resi disponibili in rete) programmi e tools in grado di recuperare i file crittografati.

Si tratta comunque di procedure non elementari e spesso complesse, che raramente hanno successo con i ransomware più moderni e meglio realizzati. Dopo tutto, anche gli hacker leggono gli stessi blog e forum di sicurezza e aggiornano i loro prodotti per renderli inattaccabili ai decrypter.

Per esempio: le prime versioni di Petya avevano punti deboli nella chiave di cifratura e questo permetteva di ricavare la chiave crittografica. Nelle versioni successive gli hacker hanno chiuso questa falla. Anche il ransomware TeslaCrypt (uno dei più diffusi) aveva vulnerabilità che permettevano di recuperare la chiave privata con alcuni tools appositi (TeslaDecoder, TeslaCrack, ecc.). Dalla versione 3.0 di TeslaCrypt questo difetto è stato eliminato e la crittografia AES 256 bit ha reso impossibile qualsiasi recupero della chiave di decriptazione.

Quindi questa opzione ha basse probabilità di successo (praticamente nessuna se la cifratura è stata fatta con algoritmi di crittografia forte come AES 256, Salsa20 o altri), ma può valere comunque la pena di tentare una ricerca in rete.

Segnalo a questo scopo l'utilissimo sito **"No More Ransom!"** [Vedi Figura 34]: https://www.nomoreransom.org/it/index.html

È stato creato nel 2016 dal National High Tech Crime Unit della polizia olandese, dall'European Cybercrime Centre dell'Europol e da due aziende di

sicurezza informatica, Kaspersky Lab e McAfee, con l'obiettivo di aiutare le vittime del ransomware a recuperare i loro dati criptati senza dover pagare i criminali.

Facendo una ricerca nel sito, o caricandovi un nostro file criptato, potremo trovare (se esiste!) il decryptor per decifrare – gratuitamente – i file.

7.9.3 Non fare nulla e perdere i propri dati

Non è certo una scelta entusiasmante e quasi mai la si può fare, soprattutto in un'azienda, a meno che i dati criptati non siano veramente di scarsa importanza. Anche se dovessimo optare per questa soluzione, consiglio comunque di:

- togliere dalla macchina il disco con i file compromessi e metterlo da parte: potrebbe succedere che in futuro qualcuno riesca a trovare il decryptor per decifrare quei nostri file, che potrebbero essere recuperati. Potrebbero passare mesi, ma potrebbe accadere...
- Oppure (per lo stesso motivo) fare un backup dei file crittografati, conservarli a parte e poi bonificare comunque la macchina.

7.9.4 Pagare il riscatto...

È ovviamente la soluzione peggiore dal punto di vista etico, quella alla quale non si dovrebbe mai arrivare: pagando alimentiamo la criminalità e la rendiamo ancora più ricca e forte. C'è un altro aspetto da considerare: se paghiamo, manderemo ai criminali il messaggio che siamo vulnerabili e disponibili a pagare, quindi... ci dovremo aspettare altri attacchi!

FAQ ▶ CHI PAGA OTTIENE INDIETRO I SUOI DATI?

Non si ha nessuna garanzia di riavere i propri dati: ricordiamoci sempre che dall'altra parte ci sono dei criminali. Per una politica di "brand reputation" a questi criminali conviene ridarci i file, altrimenti la loro "reputazione" sarebbe danneggiata e le persone non pagherebbero più.
Questo accade nella maggioranza dei casi, ma **esiste un 20% di probabilità che**, **anche pagando, i dati non ritornino disponibili.** Questo può verificarsi non solo per la disonestà dei malviventi, ma anche per altri motivi, quali:

- un errore nel pagamento

- un pagamento inferiore alla richiesta (un errore in cui è facile cadere: la vittima nell'acquisto dei Bitcoin non ha considerato la commissione sulla transazione)
- sito di pagamento nel Dark web non più raggiungibile (chiuso dalle forze dell'ordine)
- Decryptor non funzionante.

Se, nonostante tutto, si decide di pagare il riscatto, i passi da fare sono in genere questi (con piccole varianti a seconda del tipo di malware che ci ha colpito):

- **Leggere le istruzioni** che ci sono state inviate con la richiesta di riscatto: serve per capire qual è l'importo richiesto, quasi sempre in Bitcoin, e – soprattutto – quanto tempo abbiamo per pagare prima che i nostri file siano persi definitivamente (in genere i cybercriminali fissano una scadenza di circa 72 ore, comunque mai molto lunga).
- **Acquistare i Bitcoin** per il pagamento: individuare un sito che faccia "exchange" di questa valuta. Ce ne sono molti in rete e sono assolutamente legali.
- **Aprire un account** presso il sito prescelto: si tratta in pratica di un conto elettronico (wallet) dove saranno depositati i Bitcoin acquistati.
- Poiché il pagamento viene richiesto attraverso la rete TOR per garantire l'anonimato, occorre **installare un browser** TOR: lo si può scaricare direttamente dal sito: http://www.torproject.org. Si usa in modo del tutto simile a un browser normale (è derivato da Firefox).
- Solo con il browser TOR (e non con Chrome, Firefox o Safari) possiamo **accedere al sito indicato dagli hacker**: i siti della rete TOR si trovano nel Dark web, non sono indicizzati in Google e sono raggiungibili solo se si conosce l'esatto indirizzo, che è molto complesso. Questo è un esempio di indirizzo TOR: *7yulv7filqlrycpqrkrl.onion*.
- **Pagare il riscatto**: questo significa trasferire il denaro dal proprio Bitcoin wallet a quello degli hacker. Per raggiungerlo in genere è sufficiente seguire le istruzioni poste sul sito. Il wallet su cui eseguire il pagamento è identificato da un "wallet ID", costituito da una lunga serie di numeri e lettere come questa: *19eXu88pqN30ejLxfei4S1alqbr23pP4bd*. Questo codice traccia il pagamento

in forma solo numerica, quindi rende quasi impossibile risalire al nome dell'intestatario del wallet. Dopo aver trasferito i BTC sul conto degli hacker, riceveremo un altro codice (ancora una lunga serie di numeri e lettere) che rappresenta la conferma della transazione.

- **Ora aspettiamo e speriamo**: entro qualche ora (il tempo necessario perché la transazione sia stata processata dai sistemi) dovremmo ricevere un file con la chiave privata di decriptazione, oppure un file eseguibile (il decryptor) che procederà a decriptare i file. Affinché la decodifica dei file sia completa, occorre che manteniamo collegati tutti i dispositivi e dischi che erano connessi al momento dell'infezione, altrimenti qualche file potrebbe non venire decriptato.

FAQ ▶ COSA SI OTTIENE CON IL PAGAMENTO?

In genere viene inviato un file "decryptor", cioè che esegue il percorso inverso del ransomware che ha cifrato i dati. Il decryptor contiene la chiave di decifratura (in alcuni casi viene inviata a parte). Non sempre funziona bene: è un programma e potrebbe essere stato fatto in modo sbagliato... è successo anche questo!
Attenzione: il decryptor non rimuove il trojan, decifra solo i dati. Quindi il malware va eliminato con altri strumenti antimalware.
Esistono altri rischi potenziali da non sottovalutare:

- Il decryptor potrebbe contenere altri trojan (non è frequente, ma non possiamo essere sicuri che questo non accada).
- Per le estorsioni eseguite a seguito di attacchi "manuali" il rischio è che la cifra aumenti, cioè che i criminali facciano un "rilancio": è accaduto quando questi si sono resi conto di aver colpito bersagli importanti come grandi aziende o ospedali. È successo, per esempio, al Kansas Heart Hospital a Wichita (Kansas): dopo aver ricevuto il riscatto, gli hacker hanno solo parzialmente dato l'accesso ai dati criptati e hanno richiesto altri soldi per decifrare i dati rimanenti. L'ospedale ha rifiutato di pagare un secondo riscatto (maggio 2016).
- Minaccia di diffusione di materiale privato: come abbiamo detto in precedenza, ci sono stati alcuni casi di ransomware che hanno fatto anche un upload dei file (esfiltrazione), per rivenderli o chiedere un ulteriore riscatto.

Ovviamente (come ho già detto) dobbiamo mettere in conto che gli hacker, che sono dei cyber criminali, non rispettino i patti e non ci diano la chiave per riavere i nostri file.

Quindi:

MEGLIO PREVENIRE PER EVITARE DI CADERE NELLA TRAPPOLA DEL RANSOMWARE

ed evitare il rischio che il futuro della nostra azienda sia nelle mani di un delinquente in qualche parte del mondo.

7.10 Implicazioni giuridiche per le vittime dei ransomware

Poiché il riscatto viene dato a un cyber criminale, è opportuno chiedersi:

È lecito per la vittima pagare il riscatto?

Nel dare la risposta a questo – frequente – quesito, prescindiamo da tutti le valutazioni etiche, che ci dovrebbero portare a non pagare mai, per evitare di alimentare una criminalità che diventerebbe sempre più forte.

La valutazione esclusivamente giuridica ci dice che pagare il riscatto di un ransomware non è reato. Siamo infatti in presenza di una condotta estorsiva e il soggetto passivo che l'ha subita si configura come vittima che tutela se stesso o i suoi beni.

E se a pagare è direttamente l'azienda?

Rimangono valide le considerazioni fatte al punto precedente, tuttavia in questo caso è opportuno tenere presente il D. Lgs. 231/2001 "Responsabilità amministrativa delle società e degli enti": qualora il pagamento sia eseguito nell'interesse o a vantaggio della società che è vittima dell'estorsione, sarà opportuno che la cifra utilizzata per il pagamento venga prelevata in modo trasparente dalle casse della società.

Chi subisce l'estorsione rimane sempre e solo soggetto passivo del reato; quindi, tranne che non commetta reati autonomi – come la falsa fatturazione o

l'autoriciclaggio – per procurarsi la provvista, non ci sono rischi giuridici per chi, obtorto collo, versa il riscatto semplicemente a favore dell'autore del crimine.

Ovviamente non sarà possibile mettere a costo deducibile l'importo del riscatto.

Va invece precisato che, in ogni momento, il soggetto passivo può proporre denuncia per estorsione o tentata estorsione alla Procura della Repubblica e costituirsi parte civile nel processo penale, in caso di identificazione e rinvio a giudizio dell'estorsore.

Ma nel caso dei reati informatici del tipo del quale ci occupiamo, la possibilità di individuare e sanzionare il colpevole rimane piuttosto bassa.

E se a pagare è un'azienda terza e remunerata?

Si potrebbe scegliere di incaricare per il pagamento del riscatto un'azienda esterna, per esempio l'azienda o il consulente che gestisce la manutenzione dei computer della società.

In questo caso, sarebbe opportuno che la spesa per l'acquisto dei Bitcoin del riscatto sia tracciata: il consulente paga per i Bitcoin con denaro che gli viene passato dall'azienda cliente. Tale importo andrà giustificato contabilmente come rimborso spese non soggetto a IVA.

7.11 I reati per chi diffonde un ransomware

Elenchiamo qui, solo a titolo informativo, i **numerosi reati** in cui incorre chi diffonde un ransomware, o qualsiasi altro tipo di malware. Si va dalle fattispecie più lievi, quali:

- Art. 615 ter c.p. "Accesso abusivo a sistema Informatico"
- Art. 615 quater c.p. "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici"

Quindi anche il semplice accesso non autorizzato a un sistema informatico costituisce reato penale, finanche nel caso in cui non si compiano azioni di danneggiamento, spionaggio, ecc.

Le fattispecie di reato più gravi arrivano fino all'estorsione e al danneggiamento, con sanzioni penali importanti:

- Art 615 quinquies c.p. “Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico”
- Art. 629 c.p. “Estorsione”
- Art. 635 bis c.p.: “Danneggiamento”
- Art. 640 ter c.p. “Frode Informatica”
- Art. 648 bis c.p. “Riciclaggio”

7.12 Responsabilità per il dipendente che causa un ransomware

L’azienda può chiedere i danni a un dipendente che con la sua condotta ha fatto entrare in azienda un Ransomware?

Se all’interno della società è presente un regolamento sull’uso delle risorse informatiche aziendali che stabilisca in modo chiaro le attività permesse e quelle vietate in quanto rischiose per l’azienda (quali l’utilizzo di account personali, l’installazione di software non autorizzato, l’accesso ai social media personali, ecc.), allora il dipendente avrebbe commesso una violazione dello stesso e sarebbe soggetto a una sanzione disciplinare.

Quindi sarà opportuno – per un’azienda attenta a questi rischi, soprattutto ora in vigenza del nuovo Regolamento Europeo della Privacy (GDPR) – **fare formazione ai propri dipendenti** e poi redigere una **policy aziendale sull’uso corretto dei dispositivi informatici**. Questa policy, per essere efficace, dovrà prevedere anche delle **sanzioni per il dipendente che non la rispetti.**

Il dipendente dovrà quindi essere reso consapevole dei rischi informatici e non potrà giustificare un comportamento dannoso con il pretesto di “non sapere quello che può succedere”.

Oggi non è più ammissibile che qualcuno possa aprire un allegato e-mail senza prestare attenzione, perché questo comportamento può mettere a rischio la sopravvivenza stessa dell’azienda.

---

[50] https://netmarketshare.com

[51] https://www.ilpost.it/2018/03/29/atlanta-attacco-ransomware/

[52] https://www.securityinfo.it/2018/01/17/attacco-ransomware-allospedale-backup-pagano-lo/

[53] https://www.giorgiosbaraglia.it/wannacry-il-venerdi-nero-della-cybersecurity/; https://www.cybersecurity360.it/nuove-minacce/wannacry-come-funziona-e-come-difendersi-dal-ransomware-che-ha-fatto-piangere-il-mondo/

[54] https://motherboard.vice.com/en_us/article/nhs-hospitals-are-running-thousands-of-computers-on-unsupported-windows-xp

[55] https://www.nytimes.com/2018/03/28/technology/boeing-wannacry-malware.html

[56] https://www.cybersecurity360.it/nuove-minacce/petya-e-notpetya-i-ransomware-cosa-sono-e-come-rimuoverli/

[57] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[58] https://www.wired.com/story/white-house-russia-notpetya-attribution/

[59] https://www.certnazionale.it/news/2017/10/25/nuova-massiccia-campagna-di-diffusione-ransomware-bad-rabbit/

[60] https://www.corrierecomunicazioni.it/cyber-security/ransomware-as-a-service-nuova-frontiera-degli-hacker/

8

Le tecniche di attacco più sofisticate

Abbiamo visto nei capitoli 6 e 7 i tipi di attacchi di gran lunga più diffusi e da cui si deve difendere l'utente comune, che fanno leva soprattutto sull'errore umano.

Le tecniche d'attacco sono di molte tipologie, alcune utilizzate per attacchi molti sofisticati e verso obiettivi importanti. In questo libro le tratteremo solo sommariamente con una panoramica in questo capitolo, perché di esse si dovranno occupare soprattutto gli specialisti IT delle aziende. In questa categoria rientrano i già citati attacchi DDoS e le APT (Advanced Persistent Threat).

[Torna al capitolo] 8.1 Vulnerabilità, Exploit, Patch, Hacker: un po' di nomenclatura preliminare

Per capire meglio le dinamiche degli attacchi informatici, sarà utile fare chiarezza su alcuni termini che vengono frequentemente utilizzati in questo mondo.

Vulnerabilità (dette anche "**bug**"): ciascun programma software è – per definizione – imperfetto, proprio perché creato dall'essere umano. Per dare una misura, Microsoft Windows contiene circa 50 milioni di righe di codice, l'insieme di tutti i servizi Google addirittura 40 volte tanto. È inevitabile che all'interno di questi software si nasconda qualche difetto, più o meno grave. Queste "falle" nella sicurezza di un programma sono definite **vulnerabilità** e possono essere sfruttate per portare un attacco al sistema informatico. Praticamente qualsiasi attacco utilizza vulnerabilità per entrare nel sistema.

Le vulnerabilità note vengono classificate come **Common Vulnerabilities and Exposures** o CVE ("vulnerabilità ed esposizioni comuni"). A mantenere aggiornata questa classificazione è la **MITRE Corporation**[61], ente finanziato dalla National Cybersecurity FFRDC del Dipartimento della Sicurezza interna degli Stati Uniti.

Ciascuna vulnerabilità viene catalogata con una sintassi stabilita come: CVE – anno – numero.

Exploit: è un codice (programma) creato per sfruttare una vulnerabilità al fine di portare un attacco a un sistema informatico. Exploit significa, letteralmente, "sfruttamento".
Exploit kit: è un tool software che consente di automatizzare lo sfruttamento di una vulnerabilità ed eseguire un codice malevolo. La relativa facilità d'uso lo rende utilizzabile anche da hacker non particolarmente esperti.
I più famosi Exploit kit sono stati: Angler, Neutrino, Nuclear.

Patch: i produttori di software rilasciano periodicamente gli "aggiornamenti di sicurezza" finalizzati ad eliminare le vulnerabilità. Questi aggiornamenti sono definiti "patch" (letteralmente: "pezza" o "toppa").
Un attacco può essere bloccato se il sistema operativo, il browser e le applicazioni sul nostro computer sono stati correttamente aggiornati alle versioni più recenti, ma – viceversa – potrebbe avere successo in presenza di un sistema non aggiornato. Questa regola, molto importante, vale anche per i nostri smartphone.
Pertanto, gli aggiornamenti non devono essere visti come semplici miglioramenti delle funzioni del software o – come spesso accade – come un'inutile seccatura; al contrario, rappresentano una pratica necessaria (una "best practice").

Zero Day (0-day): una vulnerabilità non ancora scoperta o nota solo a pochi, ma sconosciuta agli sviluppatori di un software (che quindi hanno avuto "zero giorni" per ripararla) è definita "Vulnerabilità Zero-Day". Sono le più temute, perché se un attaccante – e solo lui – ne fosse a conoscenza, avrebbe in mano un'arma in grado di fare gravi danni. Gli exploit Zero-Day sfruttano queste falle.

Hacker: l'hacker (vedere anche cap. 1.4) è nella definizione di Wikipedia "un appassionato di informatica, esperto di programmazione, di sistemi e di sicurezza informatica in grado di introdursi in reti di computer senza autorizzazione o di realizzare virus informatici". Di solito si parla di "hacker" solo in senso negativo,

ma non sempre è corretto. Bisogna fare qualche distinzione tra le differenti categorie di hacker:

- **WHITE HAT hacker** o "hacker etici": sono quelli "buoni", che usano la loro competenza informatica in modo legale per scoprire le vulnerabilità di un software (p.es. con penetration test) e segnalarle – anche a pagamento! – all'azienda produttrice.
- **BLACK HAT hacker** o "hacker immorali": usano le loro conoscenze con intenti criminali e per proprio tornaconto.
- **CRACKER:** cercano di modificare un software per rimuoverne la protezione oppure di infrangere un sistema di sicurezza informatico per rubare o manomettere dei dati.

8.2 Gli attacchi DDoS

Gli attacchi DDOS (**Distributed Denial of Service**) in genere colpiscono obiettivi mirati, soprattutto organizzazioni importanti, tra cui le banche, che sono un target estremamente interessante.

Un attacco DDOS utilizza delle **botnet**, cioè decine di migliaia di dispositivi (cosiddetti "zombie") compromessi da malware, in grado di creare traffico dati verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile.

Il traffico dati utilizzato negli attacchi ha dimensioni sempre crescenti: CLUSIT ci indica che nel 2016 i DDOS avevano valori medi di attacchi pari a 11 Gbps (Gigabit per secondo), nel 2017 si è arrivati a un valore medio di 59 Gbps; un incremento importante, pari a circa 5,5 volte rispetto al dato medio registrato nell'anno precedente. Ci sono stati anche attacchi di dimensioni ben più clamorose, come quello del 21 ottobre 2016, di cui parliamo nel par. 9.2.6 "2016: Attacco DDOS Mirai contro Dyn Dns".

Per un'organizzazione importante (qual può essere un istituto bancario o finanziario, o un'azienda multinazionale), un attacco DDOS può avere conseguenze devastanti, causando ingenti perdite – in termini di mancata produttività e di calo di profitto – dovute a prestazioni ridotte dei siti web.

Immaginiamo il danno economico per una banca o per una società emittente di carte di credito che veda bloccati i propri servizi online, in genere per alcune ore (poiché oltre il 95% degli attacchi ha durata inferiore alle 3 ore).

Per prevenire e arginare tali attacchi non sono sufficienti le difese interne: occorre avvalersi di fornitori terzi in grado di "ammortizzare" e sviare il peso dell'attacco, i cosiddetti CDN (**Content Delivery Network**). Tra questi uno dei più famosi è Akamai, una società che con la sua rete gestisce una parte importante del traffico dati mondiale ed è perciò in grado di assorbire volumi anomali di traffico, che una singola azienda non sarebbe in grado di gestire.

Secondo un'indagine di Ponenon per Accenture Security [Vedi Figura 35] riportata da "Il Sole 24 Ore" il 22 maggio 2018[62], per gli istituti finanziari gli attacchi più costosi sono stati a oggi proprio quelli di Denial of Service (DOS), che hanno causato un danno medio per evento di 227.865 $, seguiti dagli attacchi portati con tecniche di phishing e social enineering (196.610 $).

Una spina nel fianco si confermano anche gli attacchi portati da dipendenti infedeli (i "malicious insiders"), che sono costati in media 169.059 $.

8.3 Gli attacchi APT

Le minacce **APT** (**Advanced and Persistent Threat**) sono attacchi sofisticati ma anche estremamente mirati, che iniziano con l'intrusione dei cybercriminali all'interno della rete aziendale presa di mira. Sono tra le minacce che oggi preoccupano di più le aziende che gestiscono dati sensibili o a rischio di spionaggio industriale.

La definizione APT deriva dal fatto che l'attacco ha caratteristiche:

- **Avanzate**: usano tecniche di hacking avanzate, con più vettori di attacco.
- **Persistenti:** un APT è un attacco lento e continuo nel tempo, che dura anche mesi, con l'attaccante che cerca di rimanere invisibile nel sistema più a lungo possibile. Chi sferra un APT difficilmente è una singola persona, ma piuttosto una struttura ben organizzata, con obiettivi, capacità e risorse economiche.
- **Minacciose** (Threat): un APT è una minaccia seria, perché gli attaccanti hanno obiettivi precisi, cercano di rubare dati e di spiare per lungo tempo.

L'APT non è un attacco dove gli hacker "sparano nel mucchio" con spam e phishing, al contrario usa tecniche di hackeraggio mirate e diversificate.

Il particolare livello di sofisticazione che caratterizza gli attacchi APT li rende **difficili da rilevare**: possono passare diversi mesi tra il momento dell'attacco iniziale e la sua scoperta e neutralizzazione.

Il tempo medio di scoperta (la cosiddetta **"finestra di compromissione"**) è di circa 220 giorni.

Gli attacchi APT si sviluppano in diverse fasi:

- ricognizione: per studiare l'obiettivo
- intrusione nella rete: in genere con tecniche di spear phishing e social engineering (questa è la medesima tecnica usata anche negli attacchi verso piccoli bersagli, sempre facendo leva sul fattore umano, che non nomineremo mai abbastanza!)
- furto di identità: accesso a credenziali utente valide
- installazione di malware di tipo RAT (Remote Administration Tool) per controllare il sistema (v. anche L'ANGOLO DEL NERD: I RAT – Remote Access Trojan o Remote Access Tool, p. 165)
- creazione di una backdoor, una "porta sul retro", ossia una soluzione tecnica che consenta di mantenere aperto l'accesso al sistema superando i normali meccanismi di protezione
- esfiltrazione dei dati: il furto dei dati, che è il vero obiettivo dell'attacco
- persistenza: gli hacker cercano di rimanere nel sistema il più a lungo possibile.

[Torna al capitolo] 8.4 I keylogger

Come indica la parola (*key*, "tasto", e *logger*, "registratore"), si tratta di sistemi capaci di intercettare e memorizzare qualsiasi input proveniente dalla tastiera, in pratica ogni tasto battuto dall'utente. In questo modo l'attaccante può rubare dati confidenziali come username, password, PIN, ecc.

I keylogger esistono sia in versione software che in versione hardware.

I primi sono piccoli programmi trojan, che si installano su computer e smartphone. L'intrusione si realizza con gli stessi metodi di altri malware: e-mail

di phishing o messaggi contenenti link che attivano il trojan. Non occorre l'accesso diretto al dispositivo della vittima, basta indurla a cliccare su un link applicando le tecniche del social engineering.

I keylogger hardware sono costituiti invece da piccoli dispositivi, simili a una chiavetta USB, ma ancora più minuscoli, che si inseriscono nel cavo di collegamento tra la tastiera e il computer. Si possono facilmente acquistare nel web a poche decine di euro. I più evoluti sono in grado di trasmettere attraverso la rete le informazioni che riescono ad ottenere, ma più frequentemente salvano i dati nella memoria interna (che sarà letta quando chi ha inserito il keylogger tornerà a riprenderselo). Sono molto facili da usare, perché non necessitano di particolari settaggi, ma richiedono l'accesso fisico alla tastiera.

Come scoprirli? Per quelli hardware è sufficiente un controllo fisico del dispositivo e della tastiera. Più complicato individuare la presenza dei keylogger software: per farlo occorre un buon antivirus, oppure se ne potrebbero individuare i "sintomi" con un attento monitoraggio del traffico di rete (visto che inviano dati all'esterno).

8.5 SQL Injection (SQLI)

SQL injection è un tipo di attacco "antico", che esiste da molto tempo: le prime apparizioni risalgono al 1998. Sfrutta le falle di sicurezza nelle tecniche di sviluppo di applicativi web inserendo delle stringhe di codice SQL (Structured Query Language: è un linguaggio standardizzato per database) malevole all'interno di campi di input. In altre parole, consiste molto semplicemente nell'inserimento di valori all'interno di campi web che alterino l'interpretazione da parte del database, generando quindi query non sicure.

A differenza di un attacco DDOS, un attacco SQLI può essere facilmente evitato con tecniche di programmazione attente. Infatti, secondo CLUSIT, è una tecnica d'attacco in forte calo e sempre meno significativa. Per questo non riteniamo utile parlarne oltre, salvo evidenziare l'importanza di avvalersi in azienda di fornitori esperti nella realizzazione dei software e degli applicativi web.

▸ L'ANGOLO DEL NERD: QUALI SONO LE FASI DI ATTACCO?

Ogni attacco informatico condivide le medesime macrofasi:
1. Riconoscimento
2. Scansione
3. Accesso ed escalation
4. Mantenimento dell'accesso
5. Mascheramento

1. Riconoscimento
Nell'attività di riconoscimento vengono ricercati gli obiettivi potenzialmente interessanti.
Molte botnet scansionano periodicamente porzioni di rete lanciando attacchi automatizzati per colpire prima o poi un qualche obiettivo casuale.

2. Scansione
Durante la scansione, l'attività malevola è volta al censimento dei servizi e delle tecnologie sul sistema potenzialmente vulnerabili. Tale attività può essere fatta tramite l'esecuzione di un software malevolo (nel caso di un malware che verifica ad esempio lo stato di aggiornamento di un sistema), o di software appositi (come *nmap* per la scansione delle porte di un host), o manualmente, sfruttando spesso i messaggi di errore. Questa attività è anche detta "fingerprinting", perché è volta a ricavare l'impronta digitale di un sistema grazie a messaggi voluti – o non voluti – rilasciati dal sistema stesso.
Conseguentemente all'attività di scansione e fingerprinting, si verificano le vulnerabilità note o si tentano nuove strade. In questa fase risulta importante l'utilizzo del CVE, o Common Vulnerability and Exposures (vedi par. 8.1 e glossario), un immenso database legale contenente la stragrande maggioranza delle vulnerabilità conosciute (ma non i modi in cui sfruttarle). L'attività di sfruttamento delle vulnerabilità può risultare enormemente tediosa, soprattutto nei confronti di sistemi ben protetti, o viceversa estremamente rapida, nel caso di sistemi vetusti e poco aggiornati.

3. Accesso ed escalation
Qualora la vulnerabilità sia sfruttata correttamente si ha accesso (a vari gradi, a seconda della gravità della vulnerabilità) al sistema attaccato.
Se il livello di accesso non è soddisfacente, si ricomincia col ciclo di riconoscimento → scansione → accesso ed escalation, per penetrare sempre più profondamente nel sistema.

4. Mantenimento dell'accesso

Una volta che la penetrazione è avvenuta con successo, è generalmente importante poter mantenere l'accesso al sistema. L'exploit (lo sfruttamento della vulnerabilità) viene quindi utilizzato per installare, o porta con sé, una backdoor, ovvero una "porta sul retro" che permette all'attaccante di riguadagnare l'accesso al sistema ogniqualvolta lo desideri. Tali backdoor possono essere scritte da zero, o utilizzando software come metrpreter, una componente del noto sistema di exploit Metasploit, tra i più completi e usati in commercio.

5. Mascheramento
Orizzontalmente a tutte le fasi tornano assolutamente utili, ma non sufficienti, gli **scanner automatici**. In caso di vulnerabilità tediose da sfruttare come ad esempio la SQL injection, in cui si procede in linea di massima per tentativi, o la scansione delle porte TCP e UDP (protocolli di rete fondamentali per il trasporto dei pacchetti dei dati) — che sono ben 65536! —, o la verifica degli header (le intestazioni, che contengono informazioni di controllo necessarie al funzionamento della trasmissione) di risposta da un server web, gli scanner automatici velocizzano gran parte del lavoro. Ne sono esempi sqlmap per automatizzare la SQL injection o, nell'attività di riconoscimento e scansione, burp suite nel mondo opensource o Acunetix o Nessus per gli applicativi commerciali.
Gli scanner automatici hanno però tre grosse pecche:

- innanzitutto sono *stupidi* perché non sono in grado di utilizzare un approccio "euristico": non riescono ad "intuire" le vulnerabilità che non conoscono, ma solo quelle che sono note; quindi non riescono a sfruttare vulnerabilità "non standard", al massimo possono essere programmati per intuire una vulnerabilità da comportamenti precisi del sistema. Sono stupidi
- Inoltre lasciano tracce indelebili e visibili sul sistema, sia nel traffico di rete che nei file di log, in quanto generalmente effettuano una ricerca massiva e hanno essi stessi un fingerprint visibile e rilevabile dai dispositivi di rilevamento o prevenzione delle intrusioni.
- Grazie agli scanner automatici l'attività malevola si priva quindi di un componente fondamentale: il basso profilo per evitare di essere rilevata e scoperta.

Ma questa è una peculiarità *di "quelli bravi"*.

8.6 Vulnerabilità e Bug Bounty

Scoprire una vulnerabilità, soprattutto se riguarda un software diffuso e usato da molti, può essere oggi molto redditizio. Esiste quindi il **Bug bounty**, letteralmente una "taglia su un baco".

Un hacker a caccia di bugs può guadagnare molto bene (in media quasi tre volte di più di un ingegnere informatico).

È nato un florido mercato di queste vulnerabilità, con prezzi che possono arrivare fino al milione di dollari e oltre. Ci sono molte aziende che – in modo più o meno trasparente – commerciano queste vulnerabilità. Secondo il ricercatore francese Philippe Langlois, si stima che ci siano nel mondo circa 200 broker di exploit. Alcuni di questi dichiarano di vendere solo ad aziende e agenzie governative, escludendo quindi di trattare con attori malevoli.

Tra queste le più note sono negli Stati Uniti: Zerodium, VBI, Absolute Zero Day (di Kevin Mitnick, famoso hacker), Immunity, Exodus Intelligence. Abbiamo poi Vupen (Francia), The Grugq (Bangkok), Gleg (Russia) e altre, in un mercato di attori che appaiono e scompaiono rapidamente.

Zerodium (fondata da Chaouky Bekrar, che prima aveva creato Vupen) è arrivata a offrire nel 2016 una taglia di 1,5 milioni di dollari per vulnerability 0-day sui sistemi iOS (quello dell'iPhone).

Recentemente Crowdfense[63], azienda di Dubai guidata dall'italiano Andrea Zapparoli Manzoni (membro del direttivo CLUSIT), ha lanciato il suo primo "Bug Bounty Program" [Vedi Figura 36] ad aprile 2018, stanziando un budget di 10 milioni di dollari per l'acquisto di vulnerabilità "0-days". Il programma si rivolge ai ricercatori di software e ha come clienti principalmente polizie, intelligence e governi.

Lo scopo dichiarato da Crowdfence è di rendere trasparente e legale il mercato della compravendita di vulnerabilità ed exploit.

---

[61] http://cve.mitre.org

[62] http://www.ilsole24ore.com/art/tecnologie/2018-05-21/finanza-mirino-triplicati-attacchi-istituti-credito--113641.shtml?uuid=AEDpstrE

[63] https://www.crowdfense.com/bug-bounty-program.html

9

Gli attacchi ai sistemi industriali (ICS)

Gli attacchi non colpiscono solo i computer, ma anche i sistemi industriali e infrastrutturali.
La Direttiva NIS (v. par. [5.1 La Direttiva NIS e i decreti che la recepiscono]) parla all'art. 4, punto 4, di **"operatore di servizi essenziali"**, dettagliando poi la definizione al successivo art. 5 in questo modo:

a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali
b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi
c) un incidente che investe un operatore di servizi essenziali avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Si parla quindi delle **infrastrutture critiche**, quelle che potrebbero mettere in crisi un'intera nazione se subissero un attacco informatico. Nell'Allegato II, la Direttiva NIS elenca quali sono questi soggetti e qual è il servizio essenziale fornito:

- **energia elettrica**: gestori della fornitura, del sistema di distribuzione e trasmissione
- **petrolio**: gestori di oleodotti, impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
- **gas**: imprese fornitrici, gestori del sistema di distribuzione, trasmissione, stoccaggio
- **trasporto aereo**: vettori aerei e gestori aeroportuali
- **trasporto ferroviario**: gestori dell'infrastruttura e imprese ferroviarie
- **trasporto per vie d'acqua**: compagnie di navigazione, organi di gestione dei porti, gestori di servizi di assistenza al traffico marittimo
- **trasporto su strada**: autorità stradali responsabili del controllo della gestione

del traffico, gestori di sistemi di trasporto intelligenti
- **settore bancario** ed infrastrutture dei mercati finanziari
- **settore sanitario**: istituti sanitari, compresi ospedali e cliniche private.
- **fornitura e distribuzione di acqua potabile**
- **infrastrutture digitali**: **IXP** (punti di interscambio internet), **DNS** (sistema dei nomi di dominio), **TLD** (registro dei nomi di dominio di primo livello).

FAQ ▶ CHE COSA È UN IXP?

Un **IXP (Internet Exchange Point, o punto di interscambio)** è una infrastruttura di rete gestita da un'unica entità allo scopo di facilitare lo scambio di traffico internet tra diversi autonomous systems; in sostanza un gruppo di router e reti sotto il controllo di una singola e ben definita autorità amministrativa.
Il più grande IXP italiano – e tra i primi in Europa in termini di traffico veicolato – è il MIX (Milano Internet Exchange) [64].

FAQ ▶ CHE COSA È IL DNS?

DNS (Domain Name System) significa "sistema dei nomi di dominio" ed è utilizzato per determinare quale indirizzo IP è associato a un certo nome di dominio. Un indirizzo IP (Internet Protocol) è costituito da 4 terne di numeri (per esempio: 195.24.65.215) e **identifica univocamente un dispositivo** collegato a una rete che utilizza l'Internet Protocol come protocollo di rete. Grazie all'IP il dispositivo (computer, stampante o qualsiasi altro oggetto in rete) può essere trovato e raggiunto.
Per gli esseri umani è più facile ricordare nomi testuali, perciò i siti in cui navighiamo in rete hanno nomi come – per esempio – google.com. Per questo si usa il DNS, che è un sistema per la risoluzione di nomi dei nodi della rete (in inglese: host) in indirizzi IP. Il servizio è realizzato tramite un database distribuito, costituito dai server DNS che gestiscono questa "conversione" da nomi a numeri e viceversa.

FAQ ▶ CHE COSA È UN TLD?

TLD (**Top-Level Domain**) significa "dominio di primo livello" ed è l'ultima parte del nome di dominio Internet. Corrisponde alla sigla alfanumerica che segue il punto più a destra dell'URL
Per esempio: l'indirizzo Internet di Google è google.com, quindi la parte

dell'indirizzo web che ricade entro il dominio di primo livello è .com (fu uno dei primi TLD creati alla nascita di Internet e indicava i siti commerciali, così come .gov è riservato ai siti governativi degli Stati Uniti).
I TLD possono essere anche legati alla nazione: quello dell'Italia è .it, quello della Francia .fr, quello del Regno Unito .uk ecc.

Quindi è ormai forte la consapevolezza di quanto siano critici – e vulnerabili – questi servizi, sui quali si regge il funzionamento della nostra civiltà. Non sono quindi solo i computer (in quanto contenitori di dati) a essere obiettivi attaccabili, ci sono anche gli impianti industriali e le infrastrutture. La storia recente, con molti incidenti già accaduti, ci dimostra quanto questi rischi siano reali.

9.1 Cosa sono gli ICS e perché sono vulnerabili

Internet delle cose – in inglese **IOT: Internet of Things** – è un termine riferito all'estensione di Internet al mondo degli oggetti. Fu introdotto nel 1999 da Kevin Ashton, cofondatore e direttore esecutivo di Auto-ID Center.

Oggi si usano – sempre di più – dispositivi IOT connessi in rete. Si ritiene che ce ne siano già oltre 6 miliardi nel mondo e questo numero è destinato ad aumentare molto rapidamente. Secondo stime di Gartner (società multinazionale leader mondiale nella ricerca e analisi nel campo dell'Information Technology), nel 2020 ci saranno 26 miliardi di oggetti connessi in tutto il mondo.

FAQ ▶ COSA SONO I DISPOSITIVI IOT?

Qualsiasi dispositivo elettronico dotato di un processore, di un sistema operativo e di una connessione internet è – a tutti gli effetti – equiparabile a un computer. Da qui il termine "Internet degli Oggetti".
Sono tanti i tipi di dispositivi IOT oggi già presenti nelle aziende e nelle nostre case: router, televisori, elettrodomestici, termostati, webcam, automobili, serrature, impianti industriali, ecc.
Il collegamento alla rete rende possibile il controllo di questi dispositivi da remoto.
Quindi, se questi dispositivi non sono adeguatamente protetti, possono

essere attaccati e rappresentare una minaccia reale, ancora più grave quando gli attacchi vanno a colpire impianti industriali e infrastrutture critiche.

Veniamo dunque agli ICS, acronimo di **Industrial Control Systems**, sistemi di controllo industriale.

Sono dispositivi, sistemi, reti e controlli utilizzati per operare e/o automatizzare i processi industriali, presenti in quasi ogni settore: oil and gas, centrali e reti elettriche, autostrade, porti, aeroporti, stazioni ferroviarie; in sostanza, le infrastrutture critiche elencate dalla Direttiva NIS.

Gli ICS comunicano con i sistemi e le reti SCADA (Supervisory Control and Data Acquisition) che forniscono i dati per le attività di supervisione e di controllo nella gestione dei processi.

Le vulnerabilità di cui sono affetti i sistemi ICS/SCADA sono state la causa di molti attacchi mirati, di cui parleremo nel seguito di questo capitolo. Infatti, pur essendo veri e propri sistemi IT, i sistemi ICS/SCADA differiscono notevolmente da questi nel modo di valutare l'importanza della sicurezza: mentre nelle reti IT (i "computer") si pone in primo piano la protezione dei dati, nei dispositivi ICS/SCADA si tende a privilegiare l'affidabilità e l'accessibilità dei dati per non compromettere la produttività degli impianti (dimenticandosi che anche questi sono "computer"), quindi i rischi informatici vengono tipicamente sottovalutati.

Inizialmente (i primi SCADA risalgono agli anni 1940-50) i sistemi industriali avevano caratteristiche che li rendevano immuni dalle minacce cyber, dato che non erano collegati in rete IP e utilizzavano per lo più protocolli proprietari.

Quando gli ICS sono stati connessi a Internet, assieme agli innegabili vantaggi, sono comparsi rischi importanti per la loro sicurezza: da un lato, i sistemi connessi sono più flessibili in termini di reazione rapida alle situazioni critiche e di implementazione degli aggiornamenti; ma, dall'altro lato, queste infrastrutture, che gestiscono servizi vitali, hanno dimostrato la loro vulnerabilità agli attacchi cyber.

Possiamo considerare gli anni Duemila come il momento d'inizio di questi attacchi, quando con la standardizzazione della connettività dei sistemi industriali (SCADA, PLC, ecc.) attraverso i protocolli TCP/IP(v. par. [6.4 Come

funziona la posta elettronica]) si è realizzata la convergenza dell'IT con l'OT (Operational Technology).

Secondo la ricerca Kaspersky Lab ICS CERT, le aziende del settore dell'energia sono state le più esposte a cyberminacce negli ultimi 6 mesi del 2017 e le loro infrastrutture di controllo hanno rilevato almeno un tentativo di attacco malware all'anno nel 38,7% dei casi. Uno degli attacchi più famosi è stato BlackEnergy, che ha colpito l'Ucraina il 23 dicembre 2015.

Ma quasi nessun settore è stato risparmiato, vediamo quindi quali sono stati gli attacchi più noti... fino a oggi.

Ne parleremo in modo sintetico, ben sapendo che alcuni di questi meriterebbero una trattazione più approfondita.

9.2 Gli attacchi ICS più famosi

9.2.1 2003: SQL Slammer

In questa storia entrano due protagonisti: uno è Microsoft SQL Server, un database relazionale, per il quale nel giugno 2002 Microsoft rilasciò una patch per chiudere una vulnerabilità nota: si trattava di un errore di "buffer overflow", in pratica la situazione in cui si trova un sistema quando non riesce a gestire la mole di dati che riceve.

Molti ritennero non necessario installare la patch di sicurezza, così 6 mesi dopo, a gennaio 2003, entrò in azione il secondo protagonista.

SQL Slammer è un "piccolo" malware di tipo worm (cioè progettato per replicarsi il più velocemente possibile all'interno del sistema attaccato), grande appena 376 byte (poche righe di comando). Essendo così piccolo, riusciva ad arrivare, come singolo pacchetto UDP (User Datagram Protocol, uno dei protocolli Internet di trasmissione dei pacchetti dati), a interrogare SQL Server 2000, per accedere ai database gestiti da questo. Ma essendo la richiesta di SQL Slammer "malformata", SQL Server (se non patchato con l'aggiornamento già rilasciato) andava in buffer overflow. A questo punto il sistema era infettato, con un effetto simile a quello di un attacco "denial of service". Il worm SQL Slammer continuava la sua azione

replicandosi a grande velocità e generando in automatico indirizzi IP su cui propagarsi.

Con questa tecnica, semplice ma efficace, SQL Slammer riusciva a raddoppiare le macchine infettate ogni 8,5 secondi. Dopo 10 minuti dalla sua uscita, aveva già attaccato e infettato 75.000 server. In appena 5 giorni, nei soli Stati Uniti, ha generato perdite economiche tra 950 milioni e 1,2 miliardi di dollari. Sono state colpite banche (Bank of America in particolare), ci sono stati disagi per il traffico aereo e la stessa rete Internet mondiale ha subito un rallentamento.

SQL Slammer è nato in anni nei quali i concetti di cyberwarfare e cyberterrorismo erano ancora in embrione. Probabilmente era stato creato come malware generico, per attacchi di massa e non mirati. Nella pratica si è trasformato in un "cyberweapon" (un'arma cibernetica) in grado di mettere in crisi un'intera nazione.

9.2.2 2007: Estonia

È stato il primo cyber attacco noto di una nazione contro un'altra.

I rapporti tra Russia ed Estonia sono sempre stati complicati, sin da quando quest'ultima ha acquisito la totale indipendenza nel 1991, a seguito del crollo dell'URSS.

Per dare un segno dell'autonomia conquistata, il 27 aprile 2007 la statua del soldato di bronzo con l'uniforme dell'Armata rossa (un monumento alto più di due metri, eretto nel 1947 in memoria dei soldati russi caduti nella seconda guerra mondiale), viene spostata dal centro della capitale Tallin a un cimitero militare. Per questo gesto, il governo estone temeva una rappresaglia militare da parte della Russia, ma non successe nulla, a parte qualche protesta della minoranza russofona.

Nulla sul piano "convenzionale", perché pochi giorni dopo si scatenò un cyber attacco senza precedenti.

Una massiccia ondata di attacchi DDoS bloccò i computer di banche, strutture governative e media nazionali che erano connessi in rete. La novità era che questi attacchi utilizzavano botnet, cioè insiemi di computer di ignari cittadini, infettati da un malware in grado di farli passare sotto il controllo degli hacker. Gli attacchi

furono lanciati a sciami, anche a distanza di giorni, e si susseguirono su larga scala per tre settimane.

I servizi estoni si ritrovarono più volte nel totale blackout e per ripristinare tutto servirono poi diversi mesi. Gli investigatori estoni tentarono di percorrere a ritroso il cammino compiuto dagli attacchi: molti computer operavano dagli USA, ma l'Estonia faceva parte della NATO ed era ormai filo-americana, quindi un attacco organizzato dagli Stati Uniti non avrebbe avuto senso. Molti altri computer, però, erano collocati in Russia, il principale indiziato.

Tallin ha incolpato la Russia dell'accaduto, ma senza mai spingersi a un'accusa ufficiale, per non alzare ulteriormente la tensione con l'ingombrante vicino di casa. Anche USA e NATO, malgrado la disponibilità a prestare la loro assistenza tecnica e militare al Paese baltico, non hanno mai formalmente sostenuto le accuse.

Quell'attacco del 2007 ha segnato una svolta. L'Estonia, oggi, è lo stato più digitale dell'Unione Europea: migliaia di WI-FI pubblici velocissimi, consultazioni politiche on line, il 90% delle transazioni bancarie eseguite via Internet, Il 100% delle scuole e degli uffici pubblici dotati di computer e il 97% degli affari conclusi online.

L'intera nazione è cablata in fibra ottica. Non a caso, il nome dello Stato viene spesso ironicamente deformato in "**e-stonia**".

La lezione del 2007 è stata utile...

9.2.3 2010: Stuxnet nella centrale di Natanz

Stuxnet ha rappresentato una pietra miliare nel cyberwarfare (guerra cibernetica), oltre che un esempio famoso di attacco ICS. Quando si dice "la guerra del Terzo millennio non si combatterà con i carri armati ma con i computer", con Stuxnet questo è già accaduto.

Fu una vicenda complessa, con risvolti "da film". Ed in effetti l'attacco Stuxnet è raccontato anche nel film documentario *Zero Days* (2016) del regista premio Oscar Alex Gibney.

Nel gennaio 2010, nella centrale nucleare di Natanz in Iran [Vedi Figura 37], le centrifughe dedicate all'arricchimento dell'Uranio235 (per separarlo dall'isotopo

238) impazzirono, andando fuori controllo: da 1.064 giri/minuto passarono a 1.410 giri/minuto ed esplosero. Questo mise fuori uso almeno 1.000 delle 5.000 centrifughe e comportò un ritardo di alcuni anni per il programma nucleare iraniano. Cosa era successo?

Andiamo indietro al 2006, quando già il programma nucleare iraniano preoccupava Stati Uniti e Israele. Il presidente Bush diede l'ordine segreto di preparare un cyber attacco contro le centrali iraniane per danneggiare il programma atomico iraniano senza scatenare una guerra convenzionale. Questa operazione, con nome in codice "Giochi Olimpici", fu poi proseguita dal presidente Barack Obama.

L'attacco fu affidato a esperti americani della National Security Agency (NSA), in collaborazione con tecnici informatici israeliani (la mitica Unit 8200 dell' IDF, Israel Defense Force).

Fu creato un malware micidiale, denominato Stuxnet, che era in grado di agire sui PLC Siemens Simatic S7-300, adibiti al controllo delle centrifughe utilizzate per separare materiali nucleari come l'uranio arricchito. Le centrifughe nell'impianto di Natanz erano di tipo P-1, basate su vecchi progetti che il governo iraniano aveva acquistato dal Pakistan.

Stuxnet agì nei primi mesi del 2010, nonostante la prima versione del software sembra essere datata – secondo Kaspersky – giugno 2009.

Ovviamente gli iraniani non erano così sprovveduti da mettere in rete le loro segretissime centrali. Il problema per gli attaccanti era perciò quello di riuscire a far entrare il malware a Natanz.

Ormai sembra assodato che l'inizio del contagio da parte di Stuxnet sia avvenuto dall'interno della centrale stessa tramite una **chiavetta USB infetta** data in mano a un ignaro tecnico iraniano.

Con l'utilizzo della chiavetta su vari PC, l'infezione si è poi propagata negli impianti, cercando il software industriale Step7, realizzato dalla Siemens, che controllava i PLC (gli hardware che eseguono un programma per gestire un processo industriale) della centrale e modificandone il codice.

Sempre nel 2010, versioni successive del virus Stuxnet colpirono altre cinque organizzazioni iraniane, con l'obiettivo di controllare e danneggiare la

produzione iraniana di uranio arricchito. Oltre il 60% dei computer infettati da Stuxnet nel 2010 erano in Iran.

Successivamente all'infezione del virus nella centrale di Natanz, Stuxnet si è diffuso al di fuori dello stabilimento nucleare. Sembra che sia stato Israele a voler potenziare il virus per renderlo più aggressivo e capace di propagarsi più facilmente. Forse troppo: al punto che un computer portatile contagiato nella centrale di Natanz avrebbe poi portato il malware fuori dai sistemi interessati, provocando danni importanti su altre reti che utilizzavano i PLC Siemens Simatic e che non dovevano essere assolutamente tra gli obiettivi. Stuxnet non avrebbe mai dovuto uscire da Natanz e invece, andato fuori controllo, ha iniziato a diffondersi su internet. Obama si sentì dire: "Abbiamo perso il controllo del virus". A fine 2010 Stuxnet, o una sua variante, era venduto al mercato nero nel Darkweb.

Ormai scoperto, rilevato e analizzato dalle maggiori società di cybersecurity (Kaspersky, F-Secure, Symantec nel suo rapporto "W32.Stuxnet dossier Version 1.3", November 2010), Stuxnet è stato immediatamente considerato come un virus "anomalo", troppo sofisticato per essere stato creato da normali pirati informatici.

I sospetti si sono subito concentrati su i servizi di intelligence americani e israeliani, gli unici in grado di realizzare un software con caratteristiche simili.

"The NSA and Israel wrote Stuxnet together": nel luglio 2013 Edward Snowden ha confermato che Stuxnet è stato progettato dalla NSA con la collaborazione dell'intelligence israeliana[65], tramite un corpo speciale noto come Foreign Affairs Directorate (FAD).

Questa vicenda, ormai analizzata in ogni dettaglio, ha aspetti che la fanno assomigliare a un inquietante film di guerra o di spionaggio.

Come ha scritto Raoul Chiesa: "quanti soldati, missili e carri armati sarebbero stati necessari per ottenere lo stesso risultato?"

Nessuno ha mai rivendicato l'attacco né messo la propria firma su Stuxnet. Ma in realtà, forse questa "firma" esiste veramente.

Quando gli analisti hanno sezionato il codice di Stuxnet hanno trovato diverse funzioni. Tra queste c'è la funzione numero 16 che contiene una variabile il cui valore è 19790509. Poiché a questa variabile, di puro controllo, poteva essere assegnato qualunque valore, perché proprio quel numero? Qualcuno ha scoperto che 19790509 corrisponde alla data 9 maggio 1979, che ha un significato molto preciso sia per l'Iran che per Israele: in quel giorno nella piazza di Teheran venne giustiziato Habib Elghanian, il capo della comunità ebraica iraniana. Fu una delle prime esecuzioni di ebrei da parte del nuovo regime khomeinista iraniano.

Non solo: in quel periodo, c'erano alcune centrifughe del tipo P-1 (come quelle di Natanz), installate, guarda caso, nella centrale israeliana di Dimona, nel deserto del Negev: poche per scopi produttivi, ma sufficienti per fare dei test in un impianto pilota. E fornite a Israele proprio dagli Stati Uniti, che le avevano recuperate dal programma nucleare libico[66].

9.2.4 2012: Shamoon

Saudi Aramco è la compagnia di stato saudita per la produzione di petrolio, la maggiore al mondo. Lo era anche nell'agosto 2012, quando, alle 11:08 ora locale del 15 agosto, i dipendenti della compagnia si accorgono che alcuni file dei loro computer vengono cancellati sotto i loro occhi. In poche ore, Saudi Aramco non è più in rete.

Ancora più devastanti le conseguenze per i pagamenti, per i quali la rete è ormai indispensabile: chilometri di camion-cisterna pieni di petrolio fermi, per il semplice motivo che non c'è modo di far pagare il loro contenuto. Solo i sistemi di estrazione, del tutto automatizzati e indipendenti da Internet, continuano a funzionare.

Viene scoperta la causa del problema da Seculert, la società israeliana che aveva individuato per prima Mahdi (un malware del 2011, con finalità di sabotaggio politico). Il malware viene dapprima denominato Disttrack, per prendere poi il nome di Shamoon.

Ancora una volta l'infiltrazione è avvenuta attraverso e-mail di spear phishing, che hanno portato con sé il nuovo malware.

Shamoon aveva un'elevata capacità di replicarsi e diffondersi ed era in grado di trasferire file dal computer della vittima a quello dell'attaccante, per poi

cancellarli nel sistema originario. Come la maggior parte di questi prodotti, era un malware modulare, formato da tre moduli:

- Shamoon Dropper, il modulo utilizzato per entrare nel sistema attaccato e introdurvi (drop) gli altri due componenti
- Shamoon Wiper, il componente distruttivo (Wiper significa tergicristallo o anche strofinaccio), che installava un driver per sovrascrivere i dati riuscendo a scrivere nel Master Boot Record (MBR) del computer, rendendo così inservibile il computer stesso
- Shamoon Reporter, che riportava indietro all'attaccante le informazioni sui file che erano stati sovrascritti.

Saudi Aramco ha impiegato 10 giorni (fino al 25 agosto) per ripristinare gli oltre 30.000 sistemi basati su Windows che erano stati sovrascritti da Shamoon.

Chi è stato l'autore di un attacco del genere? È stato rivendicato da "Cutting Sword of Justice", un gruppo di hacker islamici che chiedeva migliori condizioni di lavoro per i dipendenti di Saudi Aramco.

Chiunque sia stato, si è trattato di un cyber attacco perfetto nella tecnica e soprattutto nella capacità di colpire una risorsa economica mondiale: il petrolio. Il caso conferma che gli attacchi ai sistemi industriali prediligono il settore energetico.

Secondo Symantec, Shamoon è ricomparso a sorpresa nel novembre 2016 ed è stato coinvolto in un nuovo attacco il 23 gennaio 2017. Si è parlato di Shamoon 2.

9.2.5 2015: BlackEnergy in Ucraina

Sebbene non abbia generato danni importanti, lo citiamo perché si è trattato di un attacco ICS "da manuale".

23 dicembre 2015 ore 15:35: la Ukrainian Kyivoblenergo, un distributore regionale di elettricità, subisce un attacco hacker. Vengono poi in breve tempo colpiti i sistemi di almeno 3 operatori elettrici regionali.

7 sottostazioni a 110 kV e 23 a 35 kV vengono disconnesse per oltre tre ore. La metà delle abitazioni nella regione di Ivano-Frankivsk rimane senza corrente. Si stima che siano state colpite circa 225.000 persone [Vedi Figura 38].

L'attacco, proveniente da un paese straniero, prende il controllo da remoto dei sistemi SCADA delle centrali. Per ripristinare il servizio, i gestori sono dovuti passare al controllo manuale degli impianti.
L'agente usato è stato il trojan BlackEnergy con funzionalità backdoor. È un malware modulare che può scaricare varie componenti per completare specifiche attività. Nel 2014 era stato usato per una serie di attacchi di cyber spionaggio verso bersagli di alto profilo legati al governo ucraino.
Secondo il dettagliato rapporto redatto da E-ISAC e SANS "Analysis of the Cyber Attack on the Ukrainian Power Grid" (18 Marzo 2016)[67], gli attaccanti hanno dimostrato di conoscere e saper sfruttare un ampio campionario di tecniche per portare a termine l'offensiva:

- l'uso di e-mail di spear phishing per accedere alle reti aziendali dei tre gestori (e qui ritorna, come in qualsiasi attacco, il fattore H, l'errore umano)
- l'introduzione della variante del malware BlackEnergy 3 in ciascuno dei gestori interessati, utilizzato in combinazione con il nuovo plug-in KillDisk (Win32/KillDisk) dotato di capacità distruttive (overwriting di oltre 4.000 tipologie di file), in grado quindi di sovrascrivere il sistema operativo e bloccare un sistema
- il furto di credenziali dalle reti aziendali
- l'uso di reti private virtuali (VPN) per accedere alla rete ICS
- la manipolazione dei documenti di Microsoft Office che contenevano il malware per inserirsi nelle reti IT delle aziende elettriche
- la capacità di prendere il controllo dei sistemi UPS per generare un'interruzione del servizio: in almeno uno dei gestori colpiti, gli aggressori hanno scoperto una rete collegata a un UPS e l'hanno riconfigurata in modo che, quando c'è stata l'interruzione di corrente, si è interrotta anche l'alimentazione degli edifici o dei centri dati/armadi dell'azienda energetica
- un attacco di tipo DoS telefonico al call center, per bloccare i collegamenti telefonici.

È stato quindi un attacco "corale", ben progettato e condotto da specialisti. I servizi segreti dell'Ucraina hanno subito incolpato dell'incidente la Russia, anche

a causa dei pessimi rapporti tra i due paesi (poco prima c'era stata l'annessione della Crimea da parte della Russia). Ma come quasi sempre in questi eventi, è difficile arrivare a un'attribuzione certa, perché gli attacchi non vengono mai rivendicati. Al contrario, spesso vengono seminate ad arte false tracce, per depistare le indagini.

Non è chiaro neppure perché siano stati scelti proprio quei tre gestori, se cioè gli obiettivi siano stati selezionati in base alle tecnologie comuni utilizzate, alle architetture di sistema o, forse, in base al territorio.

Questi incidenti dovrebbero essere classificati di basso impatto, poiché l'interruzione ha colpito un numero relativamente ridotto (225.000) di consumatori di energia e la durata è stata limitata (alcune ore). In realtà, è lecito che le imprese colpite considerino questi incidenti come gravi o critici per l'affidabilità dei loro sistemi e per il danno commerciale subito.

Ma l'aspetto più grave è che BlackEnergy ha dimostrato di poter colpire i sistemi SCADA e bloccarli, con rischi molto forti in termini di sicurezza nazionale.

Oltre a poter eliminare i file di sistema per impedirne il riavvio, questa variante (KillDisk) conteneva un codice ideato specificamente per sabotare sistemi industriali, sovrascrivendo i file dei programmi eseguibili.

Nel dicembre 2016[68] l'attacco si **è ripetuto**, l'impatto è stato più leggero rispetto a quello del 2015, con un blackout di circa un'ora. Pare che sia stato portato dagli stessi dell'anno prima, non per creare danni, ma più probabilmente come test per future azioni.

9.2.6 2016: Attacco DDoS Mirai contro Dyn Dns

21 ottobre 2016: almeno due attacchi DDOS vengono sferrati contro Dyn, azienda del New Hampshire che fornisce la gestione dei DNS, utilizzando una botnet denominata Mirai. Questa botnet sfrutta oltre 500.000 dispositivi di IOT (webcam, termostati, lampadine, ecc.) ed è in grado di generare traffico dati con l'impressionante potenza di circa 1.200 Gbps. Molti siti web sono stati resi inaccessibili: Twitter, eBay, New York Times, Financial Times, Spotify, Github, alcuni circuiti Visa, Netflix, Reddit e molti altri.

La botnet Mirai (in giapponese significa “futuro”) sembra sia stata creata da un hacker di nome Anna-Senpai. Passa al setaccio Internet andando a caccia di apparecchi IOT. Quando ne trova, verifica se nome utente e password di accesso al software di gestione siano quelli predefiniti di fabbrica. E, se è così, entra e ne prende il controllo, sfruttando, come sempre in questi attacchi, le password deboli e non univoche.

Del mezzo milione di dispositivi violati da Mirai, il 29% si trova negli Stati Uniti, il 23% in Brasile e l’8% in Colombia. Si sospetta che l’attacco sia venuto dalla Russia.

9.2.7 2017: Triton e Triconex (Schneider Electric)

Negli ultimi mesi del 2017, viene scoperto da FireEye (un’azienda statunitense di sicurezza di reti informatiche) un sofisticato malware chiamato Triton[69], con il quale è stato attaccato il sistema di sicurezza di una non specificata “infrastruttura critica”, probabilmente una centrale elettrica. Non è stato chiarito di che tipo di infrastruttura si tratti né della sua ubicazione: la società di sicurezza informatica Dragos[70] dice che gli hacker hanno attaccato un’organizzazione in Medio Oriente, mentre una seconda azienda, CyberX, ha affermato che la vittima si trovava in Arabia Saudita.

Si sospetta comunque che si tratti dell’ennesimo “virus di stato” creato ad hoc per portare azioni di sabotaggio mirate.

Triton prende di mira i dispositivi SIS (Safety Instrumented System) Triconex di Schneider Electric, utilizzati nel settore energetico (da qui il sospetto che l’attacco sia stato condotto contro una centrale elettrica).

Schneider ha confermato l’incidente e ha dichiarato di aver emesso un avviso a tutti coloro che usano i sistemi Triconex, in quanto Triton è programmato per provocare incidenti all’interno di impianti industriali.

Nell’evento descritto da FireEye, i sistemi hanno reagito all’attacco avviando una procedura di fermo di emergenza che ha impedito danni più gravi. Ma nel caso in cui l’attacco avesse avuto successo i danni fisici (forse anche in termini di vite umane) sarebbero stati decisamente “importanti”.

FireEye nel suo report spiega che Triton è un malware che utilizza due distinti moduli: Triton.exe e Library.zip. Il file eseguibile usa i dati contenuti nell'archivio compresso per eseguire i comandi diretti ai componenti Triconex. Questo viene fatto utilizzando il protocollo TriStation, cioè quello usato normalmente per gestire i controller SIS.

Questo significa che gli autori hanno avuto la possibilità di creare Triton, utilizzando informazioni riservate riguardo alle tecnologie utilizzate dai dispositivi SIS Triconex.

Una situazione che ricorda molto da vicino l'attacco Stuxnet (di cui abbiamo parlato precedentemente), dove i servizi segreti statunitensi e israeliani avevano preparato con cura il malware, testandolo in una centrale nucleare "pilota", creata appositamente con le stesse caratteristiche della centrale di Natanz, che era l'obiettivo dell'attacco.

9.3 Come proteggere gli iCS

L'architettura SCADA è nata negli anni '50, molto prima della comparsa della rete internet.

Erano sistemi isolati, controllati da PLC, ma senza alcuna connessione; per questo si definivano "**monolitici**". Nelle successive generazioni SCADA i sistemi sono stati connessi alla rete, ma spesso senza essere progettati con meccanismi in grado di prevenire accessi non autorizzati o di affrontare la continua evoluzione delle minacce derivanti da reti interne ed esterne.

In altre parole: le reti industriali sono divenute sempre più complesse, con decine e a volte centinaia di dispositivi connessi (PLC, sensori, PC, switch, router, ecc.), ma senza un progetto preciso.

Si trascurano le "best practices" che vengono applicate nelle normali reti aziendali e si realizzano quindi reti "piatte", prive di segmentazione e di segregazione degli asset più critici.

Spesso queste reti non vengono neppure protette dai firewall che agiscono invece sulla rete dei computer aziendali.

I sistemi SCADA frequentemente vengono installati su vecchi PC e "dimenticati": si trascurano le patch di aggiornamento, con sistemi operativi ormai obsoleti.

È ancora molto presente Windows XP (non più supportato da Microsoft dall'aprile del 2014) e Windows Server 2003 (supporto terminato dal luglio 2015). Il caso WannaCry ne è un esempio molto evidente. (v. par. [7.4 Tipi ed esempi di ransomware]).

E inoltre: a volte mancano antivirus/antimalware, perché non previsti o non compatibili con le applicazioni. Oppure si pensa di avere l'antivirus attivo, ma in realtà le definizioni non vengono più aggiornate.

E quasi mai la rete viene "chiusa": ci sono porte USB accessibili, le porte di sistema vengono lasciate aperte (magari per l'accesso remoto di manutentori) o addirittura dimenticate aperte.

In conclusione: l'approccio con cui si progettano e si gestiscono gli ICS è molto di tipo "industriale" e molto poco rivolto alla sicurezza, come se questi impianti fossero ambientati in un mondo dove il cyber rischio ancora non esisteva.

È necessario cambiare completamente questo atteggiamento e **considerarli alla pari delle reti informatiche, con la consapevolezza che – in caso di attacco – l'impatto potrebbe essere addirittura più grave**.

La Direttiva NIS, come spiegato, va proprio in questa direzione. Metterla in pratica avrà un'importanza strategica per l'Europa e per tutto il mondo. Trascurarla o sottovalutarla potrebbe essere un errore mortale per la nostra civiltà.

---

[64] http://www.mix-it.net

[65] https://www.rt.com/news/snowden-nsa-interview-surveillance-831/

[66] http://www.giorgiosbaraglia.it/la-guerra-cibernetica-caso-piu-famoso/

[67] https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[68] https://nulltx.com/ukraines-power-grid-hacked-twice-in-one-year/

[69] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[70] https://dragos.com/blog/trisis/TRISIS-01.pdf

GLI ATTACCHI AI DISPOSITIVI MOBILI E ALLE RETI WI-FI

Un’opera di street art dell’artista cileno Dasic Fernández nel quartiere Wynwood di Miami.

10

Malware su dispositivi mobili

10.1 Mobile malware: un po' di storia

Oggi lo smartphone è diventato "il telecomando della nostra vita", un oggetto utilizzato più dello stesso computer e nel quale conserviamo dati sempre più importanti.

Questi nostri smartphone sono perciò miniere di informazioni preziose per i cybercriminali che li attaccano con tecniche sempre più nuove e sofisticate, soprattutto da quando, nel **2016**, il **traffico Internet da mobile ha superato** – per la prima volta – **quello da fisso** [Vedi Figura 39].

Questo è vero soprattutto nei paesi meno sviluppati, non lo è – ancora – in Europa e in USA (dove il traffico da fisso è maggioritario), ma è un trend inarrestabile che porterà sempre di più alla prevalenza dei dispositivi mobili.

Quindi per la regola del "piatto ricco mi ci ficco...", anche il cybercrime guarda con interesse ai dispositivi mobili.

I malware su mobile sono relativamente giovani. Il **primo caso di mobile malware** risale al **2004**: si chiamava **Cabir** e colpiva i sistemi Symbian serie 60 (si diffondeva attraverso il bluetooth), poi sono seguiti Ikee and Duh (2009, colpiva gli iPhone con jailbreak), FakePlayer (2010, il primo malware Android che riusciva a rubare soldi attraverso l'invio di sms a numeri a pagamento in Russia) [Vedi Figura 40].

Nel 2011 arriva DroidDream, il primo attacco massivo che colpiva su Google Play, utilizzando applicazioni contenenti un malware. Vedremo in seguito come l'**utilizzo di applicazioni "infette"** sia **uno dei principali vettori di malware nel mondo mobile**.

La minaccia è diventata forte negli ultimi anni, soprattutto con la crescita esponenziale dei dispositivi Android e la conseguente espansione del mercato

delle **app Android**, un mondo scarsamente regolamentato (anche se ultimamente Google si è resa conto della necessità di potenziare i controlli sulle app presenti nel suo Play Store). Android oggi rappresenta circa l'85% del mondo mobile (con Apple iOS che ha il restante 15%), quindi è ovviamente il "bersaglio grosso" più facile da attaccare.

Secondo il rapporto di G DATA Security Labs[71] [Vedi Figura 41], nel quarto trimestre del 2017 sono stati rilevati 744.065 nuovi malware per Android, ossia 8.225 al giorno, mentre nel solo primo trimestre 2018 sono stati 846.916, circa il 12% in più rispetto al primo trimestre del 2017. Una media di 9.411 nuovi malware al giorno: **una nuova app dannosa ogni 10 secondi!**[72].

Per i cyber criminali, i dispositivi mobili sono diventati una potenziale miniera d'oro di dati personali (e qui troviamo gli "spyware", v. par. [10.7 Gli spyware]), oltre che un modo estremamente facile per colpire gli utenti sfruttando tecniche di ingegneria sociale per rubare denaro con le modalità che poi vedremo.

10.2 Android vs iOS: qual è il più sicuro?

Come detto, attualmente il metodo più sfruttato dal malware per infiltrarsi in un dispositivo mobile è tramite il **download di un'app malevola**, che non sia stata sottoposta ad adeguati controlli.

I criminali informatici realizzano applicazioni contenenti funzionalità malevole nascoste, nel tentativo di eludere il rilevamento dei processi di controllo dello store.

Il **96% dei malware mobili colpiscono Android**.

La piattaforma Google Android è diventata un bersaglio molto più diffuso di quanto non lo sia Apple iOS, il cui ecosistema è sottoposto a controlli molto più rigidi. Infatti, grazie alla sua natura open source, Android può essere infettato con molta facilità dagli hacker.

Rispetto a iOS, che permette di installare le applicazioni solamente dall'App Store, su Android ci sono molte alternative al Google Play Store. Molti produttori di smartphone (ad esempio Samsung) hanno un proprio store online

dove gli utenti possono scaricare le applicazioni, ma esistono anche **negozi digitali gestiti da terze parti**. E proprio in questi luoghi si annidano gli hacker: su questi store pubblicare applicazioni dannose è molto più semplice, perché i controlli sono minori rispetto a Google Play Store e Apple AppStore.

I **casi di malware in ambiente Android** sono molto numerosi. Ne citiamo alcuni tra i più famosi, o semplicemente più gravi per l'impatto che hanno avuto:

- **Stagefright**: si veicolava con l'invio di un messaggio multimediale (MMS) contenente un particolare set di istruzioni. Google ha subito rilasciato la patch (aggiornamento di sicurezza).
- **DressCode**: era presente in 3.000 app Android, aveva come finalità quella di infiltrarsi nelle reti aziendali.
- **Gooligan**: ha infettato più di un milione di account Google in tutto il mondo, circa 13 mila ogni giorno. L'infezione avveniva in diversi modi: con download di un'app infetta, oppure attraverso un link malevolo inserito all'interno di un messaggio sms di phishing.

Viceversa, il "walled garden" dell'Apple App Store, dove le applicazioni sono sottoposte a severi controlli prima di essere messe a disposizione dei clienti, si è dimostrato abbastanza efficace nel prevenire gli attacchi di malware rivolti agli utenti di IOS. Ricordiamo che per un iPhone non è possibile scaricare un'applicazione se non dall'App Store ufficiale, a meno che il dispositivo non sia stato sprotetto con un jailbreak (una pratica altamente sconsigliata e sempre meno utile, come vedremo anche al par. 10.8 "Le buone regole per la prevenzione dei mobile malware").

In quanto punto di distribuzione centralizzato, l'App Store garantisce agli utenti la (quasi...) certezza che le app sono state testate e certificate da Apple. Siccome Apple non mette le API (Application Programming Interface) a disposizione dei developer, è legittimo ritenere che il sistema operativo IOS abbia meno vulnerabilità, sebbene non sia al 100% inespugnabile.

Esistono infatti casi molto noti di **malware su** IOS veicolati attraverso applicazioni infette.

Il caso più famoso a oggi è **XcodeGhost**, accaduto nel settembre 2015. Il malware nasceva da una versione modificata dell'ambiente di sviluppo Apple Xcode, il software Apple che gli sviluppatori devono usare per creare le applicazioni: a causa delle basse velocità di download dai server USA, era stato creato in Cina un repository con una versione modificata di Xcode contenente un codice malevolo. Gli sviluppatori che hanno usato questa versione di Xcode hanno inconsapevolmente pubblicato app infette sull'App Store. In questo modo sono state generate più di 300 applicazioni con malware, tra cui la famosa WeChat (simile a WhatsApp e usata da oltre un miliardo di cinesi). Appena scoperto il problema, Apple ha velocemente ritirato le app infette dal suo AppStore.

In altri casi, come con **KeyRaider**, le app infette colpivano solo gli iPhone soggetti a Jailbreak.

10.3 I blocker e i fake antivirus

A differenza di quello che accade con i computer, nel mondo mobile i classici ransomware (che criptano i file) hanno avuto poco successo, in quanto gli smartphone effettuano il backup su cloud (iCloud per iPhone e Google Drive per Android).

Se gli utenti eseguono regolarmente il backup, non ci sarà bisogno di pagare un riscatto per riavere i propri file, sarà sufficiente recuperali dal backup. Per questo i cybercriminali non hanno trovato conveniente questo tipo di attacco.

I **blocker**, noti anche come "**Lockscreen ransomware**" (v. par. [7.3 Un po' di storia dei ransomware]), viceversa, sono uno dei principali metodi d'infezione dei dispositivi Android.

Non fanno altro che sovrapporsi all'interfaccia di qualsiasi app e bloccare lo smartphone rendendolo inutilizzabile. Poi chiedono un riscatto (in genere piuttosto basso, meno di 100 dollari), ma non criptano i dati.

Su PC è abbastanza facile sbarazzarsi di un blocker: bisogna soltanto staccare l'hard disk, collegarlo a un altro computer e cancellare i file del blocker. Non è così semplice su uno smartphone, perché la scheda di memoria è saldata alla

scheda madre. Per questo motivo i blocker rappresentano il **99% dei mobile ransomware sul "mercato"**.

Altri malware su Android sono i "**fake antivirus**", che inducono gli utenti a effettuare un versamento per rimuovere malware inesistente, utilizzando stratagemmi di social engineering.

A lato ne è raffigurato un esempio: scoperto a giugno 2013 da Rowland Yu, ricercatore di Sophos[73], **Android Defender** [Vedi Figura 42] è un'app ibrida fake antivirus/ransomware che esige un pagamento di $ 99,99 per ripristinare l'accesso al dispositivo Android. Visualizza sullo schermo un avviso relativo a un'infezione, indipendentemente da cosa cerchi di fare l'utente. Non cifra i dati, ma blocca lo schermo.

10.4 [Torna al capitolo] I dispositivi non aggiornati sono più vulnerabili

Concludiamo questa parte rimarcando come le applicazioni malevole possono avere effetto solo se il sistema operativo è affetto da vulnerabilità. E in questo campo Android è il sistema di gran lunga più "fragile": i ricercatori di CVE Details[74] hanno registrato 842 vulnerabilità in Android nel 2017 (contro le 387 di Apple IOS). Nel 2018 ne sono già state scoperte 298 (IOS è a 85).

Quindi è estremamente **importante mantenere sempre aggiornati i propri smartphone**. Purtroppo questa scelta non sempre è possibile per l'utente finale, a causa della complessità della filiera di Android, che richiede fino a cinque fasi prima dell'arrivo dell'aggiornamento sullo smartphone dell'utente [Vedi Figura 43]:

1. Android (Google) realizza l'aggiornamento.
2. Android invia l'aggiornamento ai produttori di processori (per es. Qualcomm) che lo devono adattare ai propri hardware specifici.
3. Poi viene inviato ai produttori di smartphone (Samsung, LG, Huawei, ecc.) che personalizzano la nuova release.
4. Successivamente potrebbe passare anche ai provider (le c.d. Telco, quali Vodafone, TIM, ecc.) che vendono i dispositivi mobili direttamente ai clienti, e che possono apportare ulteriori modifiche al software.

5. Solo a questo punto la nuova versione del sistema operativo viene rilasciata al pubblico.

Questo processo ha tempi molto lunghi, con la conseguenza che gli utenti ricevono gli aggiornamenti a distanza di mesi o persino di anni da quando le vulnerabilità sono state scoperte. Addirittura, per i modelli più datati, il rischio è che l'aggiornamento non venga neppure fatto, perché ritenuto antieconomico dai produttori, considerata la vastità di tipi di smartphone Android presenti sul mercato, oltre 20.000.

Verranno quindi aggiornati solo i modelli più recenti e costosi. Si può considerare che gli smartphone con più di due anni dall'uscita sul mercato (e di fascia bassa, con hardware già obsoleto) non godranno di aggiornamenti, ovviamente a discapito della sicurezza.

Questo è probabilmente il maggior punto debole di Android. Google se ne è resa conto e – con Android 8.0 "Oreo" – ha presentato il suo "Project Treble", che dovrebbe semplificare e velocizzare tutto il processo degli aggiornamenti.

Nel sistema Apple iOS la filiera è invece estremamente corta e verticale: da Apple gli aggiornamenti arrivano direttamente all'utente (con un solo passaggio) e interessano un numero di modelli estremamente limitato. Questo fa sì che oggi, nel 2018, anche uno smartphone nato nel 2013 come iPhone 5S sia ancora supportato, a distanza di 5 anni.

E non si pensi che gli aggiornamenti siano fatti solo per aggiungere nuove funzionalità: nell'aggiornamento iOS 11.3 (rilasciato a marzo 2018), per esempio, sono state chiuse oltre 50 vulnerabilità, come si può vedere nel documento tecnico emesso da Apple: "About the security content of iOS 11.3"[75].

Quindi **non trascuriamo mai gli aggiornamenti**.

10.5 Smartphone e Social: una miscela pericolosa

Cominciamo mettendo in evidenza due aspetti:

- sui social media le persone abbassano le difese (e non c'è neppure l'antispam...)
- i social media sono utilizzati soprattutto sul mobile: nel mondo ci sono 3.196 miliardi di utenti attivi sui social (In Italia sono 34 milioni); di questi 2.958 miliardi lo fanno da mobile (30 milioni in Italia)[76].

Per questo per un cyber criminale è **ancora più facile attaccarci attraverso Facebook, LinkedIn o gli altri social**. E le tecniche sono tante e anche fantasiose.

Un primo esempio, piuttosto diffuso: l'utente riceve un messaggio su Facebook Messenger da un amico [Vedi Figura 44]. Il messaggio comprende la parola "video", il nome del mittente, un'emoticon e un link accorciato (Bitly o simili):

La tentazione di cliccarci sopra è molto forte: fare leva sulla curiosità è uno degli strumenti del social engineering e del phishing, come abbiamo già spiegato (v. cap. 6). Ma si rischia di far entrare un malware (tipo trojan). Una volta cliccato sul video, il malware si propaga e gli hacker entrano in possesso dei nostri dati sensibili (password, ecc.). Oppure lo stesso video potrebbe essere inviato "a raffica" a tutti i nostri contatti (senza che ce ne rendiamo conto).

A questo punto diventate "spammer" e Facebook vi blocca il profilo!

Un altro tipo di attacco di phishing meno noto ma ancora più subdolo è noto come "**URL padding**"[77] ("imbottitura dell'URL") e si diffonde sugli smartphone attraverso i messaggi.

Un messaggio che appare sul display di uno smartphone con un link "camuffato" così sembrerà un link a Facebook [Vedi Figura 45]:

http://m.facebook.com----validate---step1.rickytaylk.com/sign_in.html

Ma, se cliccato, ci indirizzerà verso un sito "fake" del tutto simile a Facebook, dove ci verrà chiesto di inserire le nostre credenziali Facebook (username e password), che finiranno evidentemente nelle mani sbagliate...

Una regola aurea, sempre valida e da non dimenticare mai: **non diamo le nostre credenziali – di qualunque servizio si tratti – a chiunque ce le chieda**.

[Torna al capitolo] 10.6 Le truffe attraverso WhatsApp

WhatsApp è l'**applicazione di messaggistica istantanea più usata al mondo**: a fine 2017 gli utenti attivi mensili erano arrivati a 1,5 miliardi. Quindi rappresenta un ottimo terreno di caccia per i cyber criminali. Chi non ha ricevuto "offerte speciali" via WhatsApp?

Per esempio (e sono casi reali): Ikea (concorso con buono da 500 €), Zara (Coupon da 150 €), H&M (buono sconto da 100 €), Apple (iPhone 7 a prezzi stracciati), Carrefour (buono spesa da 100 €) [Vedi Figura 46].

Se si clicca sul link, si accederà a una pagina con un questionario da compilare per avere diritto allo "sconto", nella quale lasceremo i nostri dati personali, che ci verranno rubati.

In altri casi ci verrà richiesto di inoltrare il messaggio ad almeno 10 contatti per sbloccare la promozione. Oppure si potrebbero attivare servizi in abbonamento che prelevano fino a 5 euro settimanali dal credito telefonico.

Recentemente il phishing dei "buoni sconto" viene veicolato anche attraverso **volantini promozionali contenenti QR Code**: per avere lo sconto viene richiesto di inquadrare con lo smartphone il QR Code, che però ci linkerà a un sito malevolo, diverso da quello che ci attendiamo. Ricordiamo che **dai QR Code, così come dai link abbreviati, è molto difficile capire a quale sito verremo indirizzati.**

FAQ ▶ COSA SONO I LINK ABBREVIATI?

Sono URL lunghi, che vengono accorciati mediante i cosiddetti "**URL shortener**", servizi che consentono di comprimerli, riducendoli a una lunghezza che non supera quasi mai i 20 caratteri. Ogni URL così creato rimanda in modo univoco all'indirizzo originale.

Tra i tanti servizi di URL shortener, quelli più utilizzati sono **bit.ly** (Bitly), **ow.ly** (di Hootsuite) e **goo.gl** (servizio del quale Google ha annunciato la cessazione), oltre a **T.co**, URL shortener automatico di Twitter (che può però essere utilizzato solo all'interno di questo social network).

I link abbreviati nascondono delle insidie: di fronte a un URL di questo tipo: *goo.gl/H8HBThc* oppure *t.co/R2wRvwjfhF* non abbiamo idea su quale sito andremo a finire, perché il link originale è nascosto. Dietro uno short URL potrebbe essere nascosto un sito pericoloso, contenente malware, e scoprirlo dopo averci cliccato potrebbe essere troppo tardi per la nostra

sicurezza.
Per questo motivo esistono anche dei **servizi per allungare gli short URL** (riportandoli all'originale), che consentono di rivelare le parti nascoste e non correre rischi.

[Torna al capitolo] 10.7 Gli spyware

10.7.1 Una storia molto istruttiva: "The Million Dollar Dissident"

Per introdurre gli spyware e per comprenderne meglio l'importanza e la pericolosità, cominciamo raccontando una vicenda accaduta nel 2016: l'incredibile storia di Ahmed Mansoor, il "dissidente da 1 milione di dollari", preso di mira dai software spia di tre diverse società.

Ahmed Mansoor è un ingegnere e blogger degli Emirati Arabi Uniti, noto difensore dei diritti umani, critico verso le politiche del governo degli Emirati. Per questo è stato perseguitato dal suo paese e arrestato per alcuni mesi nel 2011, malgrado avesse ricevuto da Amnesty International un premio come difensore dei diritti umani.

Il 10 e 11 agosto 2016 Mansoor riceve sul suo iPhone 6 due sms [Vedi Figura 47] che promettono rivelazioni sulle torture nelle carceri degli Emirati. Gli SMS contengono anche un link. Anche stavolta si punta sul social engineering per convincere la vittima ad abboccare al phishing. Ma Mansoor, sapendo di essere nel mirino, si insospettisce e invia gli SMS a Citizen Lab[78], un laboratorio di cybersecurity dell'università di Toronto. Qui i messaggi vengono analizzati – in collaborazione con un'altra società di cybersicurezza, Lookout Security[79] – scoprendo che il link avrebbe attivato "Pegasus": un micidiale malware per IOS che sfruttava 3 gravi vulnerabilità zero-days (Trident IOS Exploit Chain), presenti sugli iPhone.

I ricercatori hanno quindi avvisato Apple che si è mossa velocemente e ha chiuso le tre vulnerabilità con un importante e urgente aggiornamento di sicurezza, IOS 9.3.5, rilasciato a fine agosto 2016. Vulnerabilità come queste sul mercato degli attacchi informatici erano valutate intorno a 1 milione di dollari (v. anche par. 8.6 "Vulnerabilità e Bug bounty").

Il malware Pegasus (realizzato dagli israeliani di NSO Group, che lo commercializza a stati e polizie a prezzi di centinaia di migliaia di dollari) era uno **spyware**: un software malevolo, in grado di violare un iPhone da remoto, senza che su questo fosse stato fatto precedentemente un jailbreak. Lo scopo dello spyware è di sorvegliare l'attività della vittima: telefonate, WhatsApp e SMS, chat, uso silente del microfono e della videocamera, geolocalizzazione del dispositivo.

Il coinvolgimento di NSO Group che venderebbe solo a stati e il tipo di vittima fanno concludere ai ricercatori di Citizen Lab che dietro l'azione ci possa essere il governo degli Emirati Arabi Uniti.

Anche perché Mansoor aveva già subito in precedenza altri due attacchi analoghi, portati da società simili a NSO Group: nel 2011 da FinFisher e nel 2012 dall'italiana Hacking Team.

Cosa ci insegna questa vicenda?

- Gli spyware possono essere molto pericolosi, anche se in genere colpiscono obiettivi mirati.
- Anche gli iPhone (nonostante siano ritenuti più sicuri) possono essere vulnerabili, soprattutto se non sono mantenuti aggiornati.
- Da un messaggio (SMS o WhatsApp che sia) possono arrivare minacce importanti.
- Come sempre il fattore umano fa la differenza: se Mansoor fosse stato meno attento (o meno consapevole dei rischi) l'attacco avrebbe avuto successo e per lui sarebbero stati grossi guai.

10.7.2 Cosa sono gli spyware

Oggi i nostri smartphone contengono tante informazioni e vengono usati in modo continuo, quindi per il cybercrime (ma non solo!) può essere più utile spiare il dispositivo piuttosto che rubarlo.

Lo **spyware** è un particolare tipo di malware che consente di farlo: è un'applicazione di monitoraggio (spionaggio!) che viene introdotta in uno smartphone all'insaputa del proprietario. Può essere installata:

1) **con accesso diretto al dispositivo**: bisogna quindi fare sempre attenzione a non lasciare lo smartphone incustodito senza un codice di blocco.

2) **da remoto**: le tecniche per riuscire a installare l'applicazione (con tutti i permessi necessari) passano ancora una volta attraverso il phishing, il social engineering e la navigazione web (le modalità d'intrusione sono sempre le stesse...), come nel caso di Ahmed Mansoor. Oppure i malware possono essere nascosti all'interno di applicazioni o giochi gratuiti.

Una volta installato, lo spyware può inviare all'esterno i dati contenuti nello smartphone – telefonate, messaggi, e-mail, foto – e attivare funzioni, all'insaputa dell'utente, come fotocamera e microfono.

Il mondo degli spyware è vario e complesso: si va da quelli "artigianali" reperibili nel web a poco prezzo, fino a prodotti altamente sofisticati, realizzati da aziende specializzate (come NSO Group), che li vendono alle polizie e agli enti governativi. In questo caso si parla di "captatori informatici", utilizzati a fine di indagine per l'intercettazione di comunicazioni o conversazioni in dispositivi elettronici portatili.
Su questo delicato tema è stato approvato a fine 2017 un decreto (D. Lgs. n.216, c.d. Decreto Orlando, dal nome del ministro della Giustizia) allo scopo di regolamentarne l'utilizzo ed impedire gli abusi[80].

▸ L'ANGOLO DEL NERD: I RAT (REMOTE ACCESS TROJAN O REMOTE

Per **RAT** (o **captatori informatici**) si intendono quei malware, afferenti alla classe dei trojan (ovvero software maligni che sono installati nascondendosi all'interno di un software apparentemente benigno, come i greci all'interno del Cavallo di Troia), che permettono il controllo da remoto. La loro architettura è di tipo client-server: il client installato sul dispositivo mobile e il server, chiamato Server C&C (Command & Control), che si occupa di impartire i comandi all'agente installato e ricevere i dati.
Attività tipiche dei RAT sono anche quelle degli spyware: il controllo da remoto del microfono, della tastiera, della fotocamera, l'intercettazione tra presenti e la geolocalizzazione del telefono. Il tutto anche a schermo spento.
È quindi palese che i RAT rappresentino uno strumento potente, dallo spionaggio industriale all'intercettazione per fini sentimentali, fino al controllo per pubblica sicurezza.
Parlando proprio degli aspetti di pubblica sicurezza, i RAT sono utilizzabili, con

alcuni importanti limiti.
Innanzitutto, non rientrano a pieno titolo tra le ispezioni (Art 244 c.p.p.) essendo l'ispezione un'indagine palese, al contrario dell'attività del captatore. Non rientrano nemmeno nelle perquisizioni tradizionali (Art. 247 c.p.p.), essendo il captatore oggetto di un atto non conoscibile né depositato. Non rappresentano nemmeno un atto di sola intercettazione (Art. 266 c.p.p.) in quanto l'attività del RAT è ben più ampia della captazione occulta, ma ricade anche nell'attività perquisitoria.
Pertanto il RAT per fini di indagine è utilizzabile solo all'interno della cosiddetta "**prova atipica**", valutabile caso per caso dal giudice e, secondo la sentenza della Suprema Corte 28/04.1/07 2016 n° 26889, unicamente per i reati di tipo associativo, secondo le modalità della cosiddetta "riforma Orlando", legge n. 107 del 23 Giugno 2017.

Dal punto di vista tecnico l'infezione avviene quasi sempre con l'accesso fisico al dispositivo o l'induzione, tramite social engineering, al download di un file eseguibile ritenuto "sicuro". È possibile nascondere un RAT all'interno di un'applicazione perfettamente attendibile.
Una volta avvenuta l'installazione il RAT si maschera nel sistema tramite:

- Injection: il processo malevolo prende il nome e le sembianze di un processo benevolo
- DLL injection: vengono alterate delle librerie utilizzate dal processo benevolo per nascondere il RAT all'interno della memoria allocata dal processo benevolo stesso, rendendo il RAT difficile da rilevare e mitigare.

Per evitare tutto questo, è sempre importante installare solo software da fonti attendibili, firmati digitalmente con certificati veritieri. E, non ci stancheremo di ripeterlo, non cadere nelle trappole del social engineering.

10.7.3 I sintomi degli spyware

Non è facile capire se uno smartphone è stato infettato da uno spyware. Per i prodotti più sofisticati (come quelli realizzati da NSO Group nel caso di Mansoor), potrebbe non bastare neppure il reset del telefono alle condizioni di fabbrica. Comunque la presenza dello spyware può essere quantomeno sospettata in presenza di sintomi quali:

- riduzione della durata della batteria
- interruzione della chiamata in corso

- aumento anomalo del traffico dati
- aumento dei costi non motivato
- prestazioni rallentate e più in generale comportamento anomalo del cellulare.

10.8 Le buone regole per la prevenzione del mobile malware

Le aziende tendono a sottovalutare i rischi provenienti dagli smartphone, anche perché sono dispositivi relativamente giovani. Spesso le imprese, soprattutto le PMI, proteggono i server e le reti dei computer fissi, ma non gli smartphone che a queste reti si collegano.
Riassumiamo qui le regole per difendersi dal mobile malware:

1. **Installare app provenienti solo da fonti attendibili**, quali Google Play, Apple App Store. Evitare (per Android) le applicazioni provenienti da repository (archivi nel web) di dubbia reputazione. Controllare feedback e recensioni degli utenti.
2. **Non fidarsi di e-mail o SMS che ci consigliano di installare un'applicazione.**
3. **Non cliccare su link o allegati in e-mail o messaggi testuali.** Evitare URL sospetti o di provenienza non nota.
4. Verificare i permessi richiesti dalle app durante l'installazione. **Non installare app che richiedono permessi sospetti e non necessari** per il loro funzionamento.
5. **Non abilitare l'opzione per installare app da sorgenti sconosciute** (Android).
6. **Effettuare sempre il log out dalle applicazioni**: non basta chiudere l'applicazione, in molti casi se non facciamo il logout saremo ancora connessi quando la riapriremo.
7. **Mantenere il sistema operativo (e anche le applicazioni!) sempre aggiornati.**
8. **Non fornire mai informazioni personali e credenziali tramite e-mail o messaggi.**
9. **Non utilizzare connessioni Wi-Fi pubbliche per effettuare transazioni o scambio di dati riservati** (v. par. 12.1 [12.1 Le reti Wi-Fi pubbliche])
10. Non eseguire il **Jailbreak (iOS) o il rooting (Android) del dispositivo.** Con il termine jailbreaking o rooting si definisce il processo di rimozione delle

limitazioni di sicurezza imposte dal vendor del sistema operativo. "Jailbreaking" o "rooting" significa ottenere pieno accesso al sistema operativo e alle sue funzionalità e consentire a tutte le app, incluse quelle malevole, l'accesso ai dati inseriti nelle altre applicazioni. Jailbreak e rooting del dispositivo ne riducono drasticamente la sicurezza.

11. **Eseguire regolarmente il backup dei dati del dispositivo**. Se possibile eseguire **backup crittografati**: iTunes e gli equivalenti programmi per smartphone Android permettono questa opzione.
12. **Cifrare i dispositivi**. Il rischio di smarrire un dispositivo è oggi sempre più elevato di quello legato alle infezioni di malware. Proteggere i dispositivi con una cifratura significa renderne estremamente difficile la violazione e il conseguente furto dei dati: impostare una password sicura per il dispositivo è diventata una necessità. Purtroppo ancora oggi molte persone non mettono una password di blocco, sebbene l'utilizzo del touch-ID (e più in generale di qualsiasi sistema di riconoscimento biometrico) renda questa opzione estremamente comoda.
13. Nelle aziende, implementare sistemi di Mobile Device Management (MDM) che regolamentano, attraverso policy aziendali, l'uso corretto degli smartphone. In pratica con gli MDM si può realizzare la separazione tra dati aziendali e dati personali, il controllo centralizzato degli aggiornamenti automatici, il blocco all'installazione di applicazioni malevole (white list e black list delle app) e la cifratura dei dati.

---

[71] https://www.gdata.it/notizie/2018/30522-un-2017-di-fuoco-343-nuovi-malware-per-android-all-ora

[72] https://www.gdata.it/notizie/2018/android-primo-trimestre-2018-una-nuova-app-dannosa-ogni-10-secondi

[73] https://www.sophos.com/it-it.aspx

[74] https://www.cvedetails.com/top-50-products.php?year=2017

[75] https://support.apple.com/en-us/HT208693

[76] Fonte: Hoosuite, "We are social", gennaio 2018: https://wearesocial.com/it/

[77] https://info.phishlabs.com/blog/the-mobile-phishing-threat-youll-see-very-soon-url-padding

[78] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[79] https://blog.lookout.com/trident-pegasus

[80] https://www.agendadigitale.eu/sicurezza/intercettazioni-con-captatori-informatici-trojan-tutto-cio-che-bisogna-sapere/

11

Messaggistica istantanea (IM): ci possiamo fidare?

11.1 La diffusione della messaggistica istantanea

Ripensiamo a dieci, quindici anni fa: i nostri "telefonini" erano "feature phone"[81], con caratteristiche e funzionalità molto semplici; ancora non erano diventati gli "smartphone" di oggi, potenti come veri computer.

Questi apparecchi servivano per fare telefonate, ma anche per inviare i messaggi (e poco altro...): allora c'erano gli SMS (sigla in inglese che significa Short Message Service). Comparvero negli anni novanta (**1993**), quando la rete cellulare passò da ETACS al GSM (noto anche come 2G). Usavano infatti la rete cellulare, perché internet sui telefonini era ancora qualcosa di molto "rudimentale" e poco fruibile.

L'uso dei messaggi SMS si è diffuso molto velocemente in tutto il mondo: nel 2004 furono inviati, in tutto il mondo, circa 500 miliardi di SMS, che sono cresciuti nel 2008 fino a circa 4.100 miliardi di SMS in un anno.

Ma alla fine del primo decennio del XXI secolo, la supremazia degli SMS come strumento di messaggistica istantanea viene messa in crisi irreversibile dalla comparsa di nuove applicazioni.

Cosa è successo? Nel **2009** nasce **WhatsApp Messenger**, un'applicazione di messaggistica istantanea multipiattaforma (cioè disponibile per i differenti sistemi operativi) per smartphone. A differenza degli SMS utilizza la rete internet e questo rappresenta un decisivo abbattimento del costo per l'utilizzatore.

È l'applicazione di messaggistica più diffusa, avendo ormai superato quota 1,5 miliardi di utenti attivi mensili nel mondo e, assieme alle applicazioni simili (Telegram, iMessage, WeChat, Signal, Facebook Messenger e molte altre) ha demolito il monopolio degli SMS, oggi sempre meno utilizzati. Infatti, già nel 2015, secondo uno studio dell'Economist, sono stati inviati mediamente ogni

giorno nel mondo circa 20 miliardi di SMS e 30 miliardi di messaggi tramite WhatsApp.

Perché parlare delle applicazioni di Messaggistica istantanea (IM) in un libro che tratta di cybersecurity?

Per almeno due ottimi motivi:

1. perché, a causa della loro enorme diffusione, sono diventate un obiettivo appetibile anche per il cybercrime
2. perché sempre di più – grazie alla loro indiscutibile praticità – vengono usate anche per comunicazioni aziendali, in alternativa alle e-mail.

11.2 I rischi della messaggistica istantanea

Queste comode applicazioni sono utilizzate da tutti: chiunque abbia uno smartphone avrà installato WhatsApp o una app equivalente e spesso più di una. Tutti le usano, ma quasi sempre in modo superficiale e senza alcuna attenzione alla sicurezza (e alla privacy!).

Sempre più spesso riscontro l'uso della messaggistica istantanea per trasmettere messaggi e anche documenti all'interno delle aziende, soprattutto quelle che hanno molte sedi e filiali in giro per il mondo.

Abbiamo spiegato quanto la posta elettronica sia insicura, poiché utilizza ancor oggi un protocollo di trasmissione (SMTP) molto antiquato (v. par. [6.4 Come funziona la posta elettronica]). La messaggistica istantanea, nata in tempi recenti, è senz'altro molto più sicura. Ma questo non significa che possiamo abbassare la guardia. Anche perché, a differenza dell'e-mail, nella messaggistica non c'è neppure l'antispam...

Quindi tutto quello che ci viene inviato, arriva. Sta a noi (al fattore umano, come sempre!) distinguere tra il buono ed il cattivo.

11.3 Usare WhatsApp in modo sicuro

Abbiamo già parlato nel par. [10.6 Le truffe attraverso WhatsApp] di come questa applicazione venga utilizzata per portarci attacchi.
Questa applicazione, come qualsiasi altra simile, va utilizzata seguendo alcune buone regole di sicurezza:

- **Proteggere lo smartphone con una password di blocco** (**forte!**): lasciare uno smartphone incustodito e non bloccato può significare che chiunque potrebbe prenderlo e appropriarsi di dati riservati. Purtroppo, tante persone sottovalutano questa misura, dimenticando che negli smartphone sono conservate tante nostre informazioni. Uno smartphone non protetto potrebbe essere anche manomesso, con l'installazione al suo interno di programmi spia (gli spyware, vedi par. 10.8).
- **Non cliccare su link nei messaggi di WhatsApp:** come abbiamo spiegato, i link potrebbero essere finalizzati a veicolare truffe o malware.
- **Disattivare opzione: "Salva nel rullino foto" per impedire il salvataggio automatico delle foto di WhatsApp nel rullino dello smartphone:** se trasmettiamo immagini riservate, sarà bene evitare di duplicarle nel rullino foto dello smartphone; oltre a riempire la memoria del telefono, avremo esposto dati riservati in un altro luogo che potrebbe essere a sua volta spiato.
- **Attenzione al backup della chat sul Cloud**: esiste l'opzione che ci permette di fare il backup della chat di WhatsApp sul cloud (iCloud per gli iPhone, Google Drive per gli Android). Vale la considerazione fatta al punto precedente: duplicando queste informazioni (nel cloud) andremo a creare un altro possibile punto di esposizione e di attacco, contravvenendo la regola – sempre valida – di "ridurre il perimetro d'attacco". Ovviamente questo consiglio vale qualora siano presenti dati riservati e non le solite chiacchiere delle chat di messaggistica!

▸ L'ANGOLO DEL NERD: IL VALORE PROBATORIO DELLA CHAT DI WHATSAPP

Le chat di WhatsApp, che sono cifrate, salvate dopo qualche anno su database criptati, hanno valore di prova? La questione è assai spinosa avendo WhatsApp rimpiazzato numerosi veicoli di comunicazione, ed essendo spesso custode di illeciti, scappatelle e involontarie confessioni. Più di un matrimonio è saltato a causa di WhatsApp...
Vediamo di fare chiarezza:

La semplice trascrizione dei messaggi di WhatsApp non ha valore probatorio in quanto, secondo il codice di procedura penale, il documento prodotto è da considerarsi come prova documentale ben lungi dal garantire la paternità e immodificabilità di quanto trascritto.
Però c'è la possibilità di veder riconosciuto il contenuto di una chat di WhatsApp acuendone il valore probatorio.
A fare chiarezza arriva la Suprema Corte con sentenza 49016/2017, riguardante un caso di stalking, ove veniva richiesta dalla difesa la trascrizione delle chat di WhatsApp evidenzianti una relazione pre-esistente tra imputato e vittima.
La Cassazione ha sentenziato che la chat di WhatsApp abbia sì validità probatoria, unicamente a fronte di una corretta acquisizione della stessa, ovvero secondo un procedimento forense che garantisca una copia non ripudiabile del telefono e delle chat di WhatsApp nella loro integrità; il tutto corroborato dalla relazione tecnica del perito incaricato, evidenziante le tecniche e metodologie utilizzate, per trasparenza e replicabilità di quanto fatto.

11.4 I principali sistemi di messaggistica istantanea: quali sono i più sicuri?

Ormai tutte le principali applicazioni di messaggistica hanno implementato la **crittografia "end-to-end"** (WhatsApp l'ha fatto a metà del 2016), quindi sono intrinsecamente più sicure della tradizionale posta elettronica che – come già ampiamente spiegato – utilizza protocolli di trasmissione (SMTP) più antiquati e meno protetti.

FAQ ▶ CHE COSA È LA CRITTOGRAFIA "END-TO-END"?

La crittografia end-to-end (letteralmente "da un estremo all'altro") è un sistema di comunicazione cifrata nel quale solo il mittente e il destinatario possono leggere i messaggi.
Serve a impedire l'attacco "Man in the Middle" (MITM), che punta a rubare dati e informazioni personali "intercettando" le comunicazioni tra due utenti.
Si fonda sulla crittografia asimmetrica (detta "a chiave pubblica"), basata sulla generazione di una coppia di chiavi, una "privata" e una "pubblica"

che sono differenti. Ogni utente utilizza una chiave pubblica e una chiave privata, legate tra loro in maniera indissolubile.
Il doppio paio di chiavi crittografiche è necessario per cifrare e decifrare i messaggi in partenza e in arrivo: la chiave privata è destinata a rimanere sul dispositivo dei due "comunicanti" e serve a decrittare i messaggi in arrivo; la chiave pubblica, invece, viene condivisa con l'interlocutore ed è utilizzata per crittografare i messaggi in uscita (ne abbiamo spiegato il funzionamento anche nel par. 6.8.1 "PGP (Pretty Good Privacy).
Grazie alla crittografia end-to-end, creata nel 1976 da Whitfield Diffie e Martin E. Hellman, le comunicazioni, pur viaggiando attraverso canali "scoperti" e potenzialmente intercettabili, saranno leggibili solo dal dispositivo che ospita la chiave privata legata alla chiave pubblica utilizzata nel processo di crittografia.

Tuttavia questo non è sufficiente a garantire la totale sicurezza di un sistema di comunicazione che oggi è sempre più utilizzato nel mondo. La vulnerabilità di queste applicazioni può mettere a rischio anche la libertà e la sicurezza delle persone.
Le parole di Sherif Elsayed-Ali, direttore del programma "Tecnologia e diritti umani" di Amnesty International ci fanno capire bene l'importanza del problema:

> Chi pensa che i servizi di messaggistica istantanea (IM) siano privati, si sbaglia di grosso: le nostre comunicazioni sono sotto la costante minaccia della cybercriminalità e dello spionaggio di stato.
> Sono soprattutto i giovani, i più inclini a condividere fotografie e informazioni personali su app di messaggistica, quelli più a rischio.

Amnesty International ha stilato una "Classifica della privacy dei messaggi" [Vedi Figura 48], esaminando le 11 più popolari applicazioni di messaggistica e valutandole su una scala di punteggio da 1 a 100 rispetto a cinque parametri, fra cui il riconoscere le minacce online e l'utilizzo di default della crittografia end-to-end.
Amnesty l'ha fatto soprattutto per il rispetto dei diritti umani e della libertà di espressione in senso più ampio, ma i risultati di questo studio riguardano anche l'utilizzo che ne facciamo noi tutti.

Riportiamo qui i risultati del rapporto denominato “For your eyes only”.

A dimostrazione di quanto queste applicazioni di messaggistica siano diventate importanti (per la loro diffusione), ma nello stesso tempo esposte a rischi, anche EFF (**Electronic Frontier Foundation**), associazione che si occupa della difesa dei diritti della rete, le ha analizzate in un corposo rapporto[82].

La stessa EFF esplicita l’avvertenza che il rapporto, realizzato nel 2014, è da intendersi solo a scopo informativo ed in parte è superato, poiché successivamente alcune di queste applicazioni hanno subito cambiamenti e migliorie.

Essendo tuttavia molto interessante e dettagliato, lo abbiamo qui sintetizzato [Vedi Figura 49], selezionando solo i prodotti usati in Europa (non quelli diffusi in Cina e in Oriente).

Alcune considerazioni a commento del quadro (ove il simbolo verde significa che l’applicazione soddisfa il requisito indicato nella colonna relativa):

- tutte utilizzano ormai la crittografia end-to-end
- non tutte garantiscono che il provider del servizio possa accedere ai dati del messaggio
- poche garantiscono l’autenticità dell’interlocutore (quindi c’è il rischio che il mittente venga falsificato)
- una sola (Signal) risponde a tutti i requisiti.

Per concludere questa analisi, ricordiamo che l’utilizzo della crittografia end-to-end non esclude che per ogni messaggio l’applicazione ne conservi i “metadati”: trattasi di una serie di informazioni a corredo del messaggio, quali la localizzazione (geotag), le date e gli orari dei messaggi, i riferimenti al mittente ed al destinatario.

Da questi dati, che la maggior parte delle applicazioni traccia e conserva, si possono ricavare molte informazioni che – si può comprendere – riducono sensibilmente la riservatezza del messaggio, quantunque questo sia crittografato end-to-end.

Solo poche applicazioni di messaggistica **non tengono traccia dei metadati** e sono quindi più sicure e riservate. Tra queste citiamo **Signal di Open Whisper**[83], **Silent Phone**[84] e **Wickr Me**[85]: sono applicazioni poco note, pochissimo utilizzate, ma da tenere in considerazione qualora volessimo trasmettere messaggi con la maggior sicurezza possibile.

---

[81] Con questo termine si intendono i cellulari privi delle funzionalità avanzate degli smartphone.

[82] Versione integrale in https://www.eff.org/node/82654

[83] https://signal.org

[84] https://www.silentcircle.com/products-and-solutions/silent-phone/

[85] https://wickr.com

12

I pericoli delle reti Wi-Fi

[Torna al capitolo] 12.1 Le reti Wi-Fi pubbliche

I nostri smartphone sono affamati di Gigabit e il traffico dati dei nostri contratti non è mai abbastanza. Questa necessità si accentua nei mesi estivi, quando ci troviamo lontani da casa o dall'ufficio.

Le reti Wi-Fi pubbliche, quasi sempre gratuite e libere (cioè non protette da password) ci sembrano di grande aiuto. Ma è meglio fare attenzione! Utilizzare reti Wi-Fi pubbliche è sicuramente comodo, ma può comportare dei rischi: connessioni non protette infatti celano una serie di pericoli che è bene conoscere.

Per un malintenzionato, spiare il nostro traffico dati attraverso queste reti Wi-Fi è veramente semplice, alla portata anche di chi non è dotato di particolari conoscenze informatiche.

Ad esempio, se un utente accede mediante la connessione Wi-Fi gratuita di un aeroporto, di un albergo o di un centro commerciale, i suoi dati rischiano di essere intercettati, con la tecnica nota come MITM ("Man In the Middle").

Per fare tutto questo non occorre essere un hacker di alto livello, basta un semplice apparecchio, acquistabile sul web a 99,99 $, il Pineapple Nano di Hak5[86] [Vedi Figura 50]. L'uso ufficiale per il quale viene commercializzato è "per fare Penetration test", ma in realtà le finalità sono ben altre e meno lecite.

Nell'ultima versione è disponibile anche con una simpatica custodia mimetica (Nano Tactical) per nasconderlo meglio!

L'apparecchio è dotato di due schede di rete Wi-Fi, una in entrata e una in uscita, si collega a un computer e con l'ausilio di alcuni software appositi permette di "sniffare" i pacchetti dati che intercetta.

Tra i software in genere si usa Kali Linux (è una distribuzione Linux), che include al suo interno tutti gli strumenti per superare le protezioni delle reti wireless, in abbinamento con Wireshark[87], che è un software per analisi di protocollo o

“packet sniffer” (letteralmente annusa-pacchetti) utilizzato per la soluzione di problemi di rete. È distribuito con licenza Open Source per Linux, macOS e Windows, quindi disponibile per chiunque. Un altro packet sniffer usato è Firesheep.

Tramite le sue due schede di rete wireless il Pineapple è in grado di collegarsi a una rete Wi-Fi esistente (aperta o di cui si conosce la password) come client e, tramite bridge, può fornire in maniera trasparente la connettività ai client che si collegheranno alla sua scheda di rete secondaria che è impostata come access point libero (cioè senza password di accesso).

I nostri smartphone – per impostazione di default – si connettono automaticamente alle reti Wi-Fi libere [Vedi Figura 51] (che non richiedono cioè alcuna password di accesso), quindi Pineapple riesce ad ingannarli.

In pratica il dispositivo si interpone in maniera trasparente [Vedi Figura 52] tra il device dell’utente e l’access point regolare (facendo da “bridge”), quindi vede e intercetta tutti i pacchetti dati trasmessi e ricevuti, pacchetti che saranno poi analizzati con Wireshark.

Ovviamente, per fare tutto questo, l’attaccante deve trovarsi fisicamente nel raggio d’azione del Wi-Fi della vittima.

In alternativa, qualora la rete Wi-Fi pubblica sia protetta da password non conosciuta, l’hacker può creare con Pineapple un fake access point, cioè un’altra rete “free” e malevola – naturalmente dal nome simile a quella esistente – al quale gli inconsapevoli utenti si connetteranno, automaticamente e con grande piacere.

Pensiamo alle nostre (distratte...) abitudini: se in luogo pubblico il nostro smartphone trova una rete “free”, magari con la parola “free” ben evidente nel nome SSID (service set identifier) della rete, chi si pone qualche dubbio sulla sicurezza, prima di collegarsi? Ci troveremo collegati (in automatico) senza esserci fatti nessuna domanda...

Per evitare questi rischi, è consigliabile disattivare la possibilità del proprio smartphone (o computer) di collegarsi automaticamente a reti Wi-Fi aperte.

Soprattutto, bisogna **evitare di connettersi a siti con cui si scambiano informazioni riservate (banca, azienda, ecc.) quando si naviga sotto rete** Wi-Fi

gratuita: in questi casi ci troveremmo in uno spazio libero, non criptato, incontrollato, dove le nostre password, la nostra identità digitale e in generale i nostri movimenti possono essere agevolmente captati e decifrati.

In particolare, è pericoloso fare qualsiasi operazione bancaria, inserire il proprio numero di carta di credito o il ccv, ma anche effettuare pagamenti tramite PayPal, così come controllare il proprio estratto conto.

Per lo stesso motivo, dobbiamo evitare di inserire password per accedere a social network, mail o account condivisi (Dropbox, Google Drive o altri) per non consentire a sconosciuti di rubarci le credenziali.

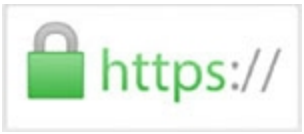
Piuttosto conviene **utilizzare la rete cellulare e accertarsi anche che il sito sia in HTTPS**.

FAQ ▶ CHE COSA È IL PROTOCOLLO HTTPS?

HyperText Transfer Protocol over Secure Socket Layer (HTTPS) è un protocollo utilizzato su Internet per la comunicazione sicura attraverso una rete di computer.

Integra il protocollo standard HTTP con un meccanismo di crittografia di tipo Transport Layer Security (SSL/TLS): i pacchetti dati viaggiano all'interno di una connessione crittografata da TLS e non possono essere intercettati attraverso attacchi del tipo "Man in the middle" (MITM).

I siti web che utilizzano il protocollo HTTPS sono dotati di un certificato preinstallato che ne attesta la proprietà. I certificati vengono rilasciati da Certificate Authority (CA).



Se il sito è dotato di certificato HTTPS, compare un pulsante a forma di lucchetto accanto all'indirizzo del sito. Cliccando sul lucchetto, si potrà vedere il certificato e da quale CA è stato rilasciato.

In alternativa si possono **usare sistemi di connessione sicura come i servizi VPN** per cifrare i dati in transito.

FAQ ▶ CHE COSA SIGNIFICA VPN?

VPN (Virtual Private Network) è una rete di telecomunicazioni privata,

instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet. La connessione VPN crea un tunnel "virtuale" (protetto e sicuro) che viaggia attraverso la rete pubblica come fosse un cavo fisico. In questo modo la comunicazione end-to-end tra utenti rimane a livello logico confinata all'interno della rete privata stessa.
Si utilizza VPN quando serve una connessione di rete sicura da remoto: in questo modo si possono utilizzare le risorse di rete aziendali (cartelle, sistemi informatici gestionali, posta elettronica) senza rischi. L'accesso alla VPN deve essere protetto da un processo di autenticazione forte.

12.2 Connessioni Wi-Fi mediante Captive Portal

In molti luoghi pubblici, soprattutto negli alberghi, la connessione alla rete Wi-Fi è sì gratuita, ma richiede un'autenticazione mediante il sistema del **Captive Portal**.

Come funziona: appena connessi alla rete Wi-Fi (che si presenta come libera, cioè senza password), veniamo reindirizzati su una pagina web, appunto il Captive (letteralmente "bloccato") portal, che si apre nel browser e ci chiede un login. In genere viene mostrato un messaggio di benvenuto, che ci informa delle regole di accesso e ci invita all'accettazione di determinate condizioni (EULA: End User License Agreement). Solo dopo aver fatto questo, la navigazione Wi-Fi sarà sbloccata e attiva. Per questo motivo, non si riesce a navigare attraverso le applicazioni dello smartphone, se prima non si è passati attraverso la pagina del browser del Captive Portal.

Questo sistema è senz'altro più sicuro, ma tuttavia non esente da rischi.

L'accesso con Captive Portal è infatti attaccabile tramite un semplice "packet sniffer" (come il software Wireshark di cui abbiamo parlato in precedenza), mediante il quale l'attaccante riesce a ottenere IP e indirizzi MAC di altri dispositivi già autenticati e connessi.

Con una tecnica di spoofing, cioè falsificando le proprie credenziali con quelle degli utenti autorizzati, l'attaccante riuscirà a connettersi, pur non avendo l'autorizzazione.

12.3 Attacchi alle reti Wi-Fi protette

Anche le reti Wi-Fi protette potrebbero essere attaccate, soprattutto se non adottiamo corrette misure di sicurezza.

Diciamo intanto che le reti wireless sono dotate di differenti protocolli di sicurezza: WEP, WPA, WPA2 E WPA3. Vediamo cosa significano queste sigle.

WEP (Wired Equivalent Privacy): è un protocollo di sicurezza ormai obsoleto che non offre una vera protezione, per la debolezza dell'algoritmo crittografico utilizzato: un attaccante appena esperto riuscirà a rubare la password d'accesso e a entrare nella rete. Per farlo potrà utilizzare Aircrack-ng, un programma per craccare le password WEP (recuperandole dallo sniffing dei pacchetti) e WPA-PSK (con tecnica "brute force").

La suite Aircrack è composta da diverse utility: airmon-ng, airodump-ng (per monitorare le reti Wi-Fi esistenti), airbase-ng.

WPA (Wi-Fi **Protected Access**): per superare le debolezze del WEP, nel 2003 è stato implementato dalla Wi-Fi Alliance il nuovo standard WPA, che è un poco più sicuro del precedente, una sicurezza che è legata alla forza della password utilizzata.

WPA2 (Wi-Fi **Protected Access 2**): rilasciato nel 2004 con lo standard IEEE 802.11i, è il protocollo attualmente più sicuro, anche se nel 2017 è stata pubblicata la notizia di una sua vulnerabilità all'attacco KRACK (Key Reinstallation Attack). WPA2 utilizza la crittografia AES (Advanced Encryption Standard), che è, ad oggi, lo standard di crittografia simmetrica (a chiave privata) ritenuto più sicuro, utilizzato come standard dal governo USA e dalla NSA (National Security Agency) per i documenti classificati Top Secret.

WPA3: la Wi-Fi Alliance ha ratificato a giugno 2018 il nuovo standard WPA3, con il quale le reti Wi-Fi saranno finalmente criptate, sicure e molto più semplici da configurare. È la terza versione del protocollo WP. A breve quindi arriveranno sul mercato nuovi dispositivi compatibili con WPA3.

12.4 Proteggiamo le nostre reti Wi-Fi

Vediamo, in conclusione, cosa fare per rendere sicure le nostre reti Wi-Fi.

1. Come spiegato in precedenza, sarà **necessario utilizzare lo standard più avanzato disponibile, quindi il WPA2 (o il WP3 in futuro)**. Oggi qualsiasi router e access point lo supporta.
2. Scelto il WPA2, non vanifichiamone l'efficacia. Quindi, per evitare intrusioni nelle proprie reti wireless è estremamente importante **utilizzare una chiave di sicurezza (la password della rete** Wi-Fi) **complessa e forte**, come spiegheremo in seguito nel cap. [13 – Imparare a usare le password]. Evitiamo password banali, con riferimenti a informazioni personali, se non vogliamo che nel nostro WI-FI si intrufoli il vicino di casa (è realmente successo!).
3. Consiglio poi la **disattivazione del** WPS (Wi-Fi Protected Setup), una comoda funzionalità per connettere velocemente i dispositivi all'access point. È un sistema creato per semplificare l'autenticazione: i dispositivi si autenticano al router WI-FI fornendo il codice a otto cifre identificativo PIN. Nel protocollo WPS è stata individuata una falla di sicurezza. Con un attacco di tipo "brute force" è possibile in poche ore scoprire la chiave di sicurezza utilizzata, come ha scoperto nel 2011 il ricercatore Stefan Viehbock[88].
4. Network Access Control (NAC): **creare una rete WI-FI Guest** in azienda, **alla quale si potranno collegare gli ospiti**, in modo da non entrare nella rete aziendale principale. Questa comoda opzione è disponibile ormai anche nei router per uso domestico: la consiglio quindi anche per la nostra rete Wi-Fi di casa.
5. Veniamo infine all'errore più banale, e grandemente sottovalutato. Molti lo commettono, per pigrizia o mancanza di consapevolezza. I router che acquistiamo o che ci fornisce l'Internet Service Provider (ISP), sono dotati di credenziali standard. Quindi potrebbero avere come username e password la "formidabile" accoppiata "admin/admin" oppure "admin/password", o altre amenità.

Ma anche quando troviamo (in genere stampigliate in un'etichetta sotto il router) password di fabbrica del tipo: "*E02dte53kz0*" o "*Telecom-94939567*", non illudiamoci che siano sicure, tutt'altro!

Le chiavi di rete predefinite sono create dai costruttori di router con algoritmi (non certo in modo manuale), a partire dal nome del dispositivo, che in genere è quello dell'SSID (Service Set Identifier). Tali algoritmi sono stati ampiamente scoperti e decodificati e nel Web si trovano software (anche opensource) che danno questo servizio: si inserisce marca e modello del router, l'SSID e si ottiene la password.

Quindi chiunque, dal nome SSID della nostra rete WI-FI può risalire alla password preimpostata. E se non abbiamo avuto l'accortezza di cambiarla (con una password forte, repetita juvant!), ci entrerà dentro con grande facilità. **Quindi la prima cosa da fare è cambiare la password di rete.**

---

[86] https://hakshop.com/collections/wifi-pineapple-kits/products/wifi-pineapple?variant=81044992

[87] https://www.wireshark.org

[88] https://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/.

COME DIFENDERSI

Un graffito nel quartiere Wynwood di Miami.

[Torna al capitolo] 13

Imparare a usare le password

13.1 Gli errori più comuni con le password

Oggi possiamo veramente affermare che "le password sono le chiavi della nostra casa (e del nostro ufficio) digitale", una "casa" costituita da computer, smartphone, tablet, nella quale custodiamo dati sempre più numerosi e importanti. Ma poiché è noto che "la tecnologia corre più veloce della nostra capacità di assimilarla", ancora oggi usiamo le password in modo totalmente insicuro. Nessuno lascerebbe la chiave sulla porta, uscendo di casa, ma con le password facciamo proprio questo...

Secondo l'analisi fatta dal "Verizon 2017 Data Breach Investigations Report"[89], **le violazioni degli account sono state causate nell'81% dei casi da password rubate e/o deboli**. E avere un account violato significa che qualcuno è entrato nel nostro computer o nel nostro profilo, per spiarci o per rubarci i dati o – ancora peggio – per sostituirsi a noi, perpetrando quello che è uno dei rischi maggiori del web: il furto d'identità.
Questa è la classifica delle password più utilizzate nel mondo (e anche le peggiori!) nel 2017 (fonte Splash Data[90]):

1. **123456** (al primo posto dal 2013)
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football

10. iloveyou

Non serve aggiungere altro... Utilizzare password siffatte equivale a lasciare la chiave sulla porta di casa: sarà fin troppo facile, per chiunque, entrare e rubare.

Sono molti altri gli errori che vengono fatti nell'uso delle password. Uno dei più frequenti è quello di utilizzare la medesima password in molti siti diversi. Ricordare password complesse, con il solo aiuto della memoria, non è semplice. Quindi la maggior parte di noi preferisce utilizzare la **stessa password** (magari anche abbastanza forte) in un gran numero di servizi sul web.

Questa è una **pessima e pericolosa abitudine**, per i motivi che andrò ad illustrare.

Cominciamo con una storia, vera e molto istruttiva.

13.1.1 Una storia molto istruttiva: come è stato hackerato Mark Zuckerberg

Attacco a LinkedIn: nel 2012 il sito del noto social fu violato e vennero resi pubblici nel Dark web 6,5 milioni di account degli utenti iscritti a LinkedIn.

Tutto sembrò finire così, ma invece, quattro anni dopo, nel maggio del 2016 un hacker di nome Peace mise in vendita sul Dark web, per l'importo di 5 Bitcoin (circa 3.000 $) 164 milioni di credenziali (login+password) di LinkedIn. Questi dati risalivano allo stesso data breach di quattro anni prima.

Pochi giorni dopo, a giugno 2016, gli account LinkedIn, Twitter (@finkd) e Pinterest di Mark Zuckerberg (il fondatore di Facebook) furono violati da un gruppo di hacker di nome OurMine Team: si può vedere [Vedi Figura 53] il tweet (evidenziato nel riquadro rosso) scritto dagli hacker sul profilo Twitter di Zuckerberg.

Come è stato possibile?

Mark Zuckerberg, un personaggio che grazie al web è diventato ad appena trent'anni uno degli uomini più ricchi del mondo, usava per tutti i suoi account social la stessa password di LinkedIn (quella del 2012), e questa password era nientemeno che "dadada"!

Negli stessi giorni, i medesimi hackers OurMine Team hanno violato l'account Twitter di Jack Dorsey (@Jack), il fondatore di Twitter, con il messaggio: "*Hey,*

its OurMine, we are testing your security" e quello Quora e Twitter di Sundar Pichai (CEO di Google). Anche in questi casi la violazione degli account è stata possibile perché gli utenti (non persone qualunque, ma esponenti di spicco della Silicon Valley!) utilizzavano la stessa password sui diversi account social. E quella password era nota perché rubata a LinkedIn nel 2012.

L'insegnamento che si trae da questo episodio è molto chiaro e ci evidenzia una delle regole essenziali sul corretto uso delle password: **non utilizzare mai la stessa password in account diversi**, perché se non possiamo evitare che il nostro provider venga violato (non dipende da noi e anche siti molto famosi hanno subito attacchi), possiamo almeno impedire che tutti i nostri account vengano hackerati in un colpo solo a causa dell'utilizzo di una sola password.

Infatti, una volta in possesso di un archivio di credenziali rubate (se ne trovano tanti, in vendita nel Darkweb), gli hacker cominciano a testarle sui vari servizi in rete. L'operazione è proficua, ma molto lunga. Ora però è possibile velocizzare questo processo utilizzando Shard, un software che è stato sviluppato per consentire agli utenti di testare se una password che è utilizzata per un sito è impiegata anche per accedere ad altri servizi, tra cui Facebook, LinkedIn, Reddit, Twitter o Instagram. Il codice del tool Shard è disponibile su GitHub[91].

13.2 Le password sono importanti anche per i dispositivi IoT

Internet delle cose (dall'inglese IoT, "Internet of Things") è un termine riferito all'estensione di Internet al mondo degli oggetti. Oggi si usano, sempre di più, dispositivi IoT connessi in rete. Si ritiene che ce ne siano già oltre 6 miliardi nel mondo e questo numero è destinato ad aumentare molto rapidamente.

La loro protezione necessita delle stesse attenzioni richieste per i computer.

In particolare, sarà estremamente importante dotarli di password forti e sicure, condizione che in molti casi non si verifica: spesso i dispositivi IoT vengono immessi sul mercato con password standard (il classico "admin/admin" o cose del genere...), o addirittura talvolta non hanno neppure la password impostata. Significa che sono completamente esposti!

Troppo spesso chi li installa dimentica che si tratta di computer, quindi non si cura di cambiare la password d'accesso, così il dispositivo rimane vulnerabile, accessibile da chiunque, con tutti i cyber rischi che possiamo ben immaginare.

Se pensate che queste siano paranoie degli esperti della cybersecurity e siete convinti che "tanto questo non è un problema che mi riguarda", vi invito a visitare questo simpatico sito: https://www.insecam.org
Qui si possono vedere (letteralmente!) migliaia di webcam di tutto il mondo (è possibile fare anche una ricerca per area geografica) accessibili liberamente perché non adeguatamente protette.

Non basta? Esiste Shodan[92], che così si definisce nella sua homepage: "*Shodan is the world's first search engine for Internet-connected devices*".
In pratica il Google dell'IoT, un motore di ricerca che scandaglia il web alla ricerca dei dispositivi IoT connessi. E se non sono adeguatamente protetti...

[Torna al capitolo] 13.3 Come ci vengono rubate le password?

Per capire meglio come proteggerci, vediamo intanto quali sono le tecniche per scoprire le nostre password. Sono più d'una, talvolta veramente banali, e quasi sempre funzionano grazie agli errori degli utenti.

- **Ingegneria sociale**: ad esempio phishing e password sniffing; in pratica siamo noi che ci lasciamo ingannare dalle tecniche di social engineering e diamo le password a chi ce le chiede, per esempio attraverso messaggi, e-mail, siti fake ("falsi") che dissimulano un sito noto.
- **Indovinando le password:** utilizzando informazioni personali come nome, data di nascita, nomi dei figli o di animali domestici. A scoprire la password sarà magari il collega di lavoro o il vicino di casa, ma potrebbe essere anche un hacker lontano, quando superficialmente lasciamo le nostre informazioni personali sulla pagina pubblica di Facebook.
- **Attacco "brute force" ("a forza bruta")**: attraverso la prova automatica di un gran numero di password fino a quando viene trovata quella giusta. Esistono programmi appositi per fare questo, facilmente reperibili sul web, il più noto

dei quali è **John the Ripper**[93]. Si tratta di una tecnica onerosa, che richiede tempo e potenza di calcolo, ma che può raggiungere il risultato. Oggi esistono computer in grado di portare con grande potenza di calcolo un attacco brute force. "I computer più veloci sono in grado di calcolare e testare più di due miliardi di chiavi al secondo" (Claudia Eckart, direttore Fraunhofer Institute for Applied e Integrated Security). L'unica difesa da questo tipo di attacco è l'uso di una password forte e lunga, che aumenti il numero delle combinazioni possibili (come vedremo al par. 13.5 "Come si costruisce una password forte").

- **Intercettazione** di una password mentre viene trasmessa su una rete. È frequente la pessima abitudine di comunicare password via e-mail: ci sono addirittura siti che, non appena ci registriamo, ci inviano un "cortese" messaggio di benvenuto contenente username e password esposti "in chiaro"; peccato che l'e-mail – come già spiegato – non sia uno strumento sicuro... Qualora si verificasse un caso del genere, consiglio di cambiare – subito – la password, perché non più sicura.
- **"Shoulder surfing"**: osservando qualcuno alle spalle ("shoulder") mentre digita la password. Negli uffici, tra colleghi, succede anche questo...
- **Installando un keylogger** per intercettare le password digitate in un dispositivo. Ricordiamo che i keylogger sono programmi (trojan) che registrano tutto ciò che viene digitato sulla tastiera e trasmettono poi questi dati all'hacker che li hanno installati. Esistono anche keylogger hardware che richiedono accesso diretto al computer della vittima, ma che si installano con grande facilità: sono simili a chiavette USB e vanno semplicemente collegati al cavo di comunicazione tra la tastiera e il computer. Basta riprendersi il keylogger e leggere i dati memorizzati. Fin troppo facile!
- **Password memorizzate in modo non sicuro**, per esempio scritte a mano su un foglietto, o salvate su un file di word/excel (ovviamente denominato "Password", per essere sicuri di trovarlo!). Questo è uno degli errori più frequenti, definito anche *"idiocy attack"* con un nome che ci fa capire bene di cosa si tratta.
- **Compromettendo un database** di un sito contenente un gran numero di password utente, quindi utilizzando queste credenziali per attaccare altri sistemi dove gli utenti hanno riutilizzato le stesse password ("*credential stuffing*"). È per

esempio quello che è successo a LinkedIn e a Mark Zuckerberg nella storia che abbiamo raccontato in precedenza.

13.4 Evitare il "Social login"

È una buona regola evitare di registrarci a un sito usando il login con Google, Facebook, LinkedIn, Twitter e altri siti social che ci offrono il **Social login** [Vedi Figura 54]. Questo sistema è un esempio di SSO ("Single Sign-On"), cioè una singola password per tutto.

È ovviamente molto pratico, perché ci evita di dover inserire ogni volta le nostre credenziali, oltre a dover scegliere e ricordare nuove password.

Ma ha due importanti controindicazioni a causa delle quali lo sconsigliamo:

1. la prima, più importante, riguarda la sicurezza. Questi sistemi si basano su protocolli aperti come **OAuth 2.0** (sviluppato da Blaine Cook e Chris Messina dal 2006). La possibilità di collegare a un sito l'account Facebook, Google, ecc. (definiti anche "provider dell'identità") evita a tutti gli effetti il dover creare altre password, ma nel caso in cui l'account principale e/o il provider dell'identità siano compromessi, l'attaccante ottiene l'accesso immediato a tutti i siti (o alle applicazioni) collegati. In altre parole, viene rubata la chiave che apre tutte le porte... Inoltre, nel sistema OAuth2.0 è stata rilevata una vulnerabilità (probabilmente risolta, ma meglio non fidarsi): può capitare che l'applicazione esegua automaticamente l'accesso al profilo senza che i dati forniti coincidano con l'account utilizzato per l'autenticazione. Quindi questo metodo di autenticazione è da considerarsi complessivamente poco sicuro.
2. la seconda è che può raccogliere più informazioni riguardanti l'utente di quante siano effettivamente necessarie per il semplice accesso. Il protocollo OAuth 2.0 non garantisce confidenzialità né sulle richieste né sui contenuti.

13.5 Come si costruisce una password forte

Una password è caratterizzata da:

1. lunghezza, cioè il numero di caratteri: **consigliabile usare almeno 12 caratteri**

2. tipi di caratteri usati:

- numeri (0-9) = **10 tipi**
- lettere = **52 tipi** (26 minuscole + 26 maiuscole)
- caratteri speciali da tastiera, cioè quelli presenti sui tasti, per es.: # &%? ecc. = **33 tipi**

Quindi in totale abbiamo a disposizione 95 tipi di caratteri: è **consigliabile usarli tutti, per aumentare il numero delle combinazioni.**

Aumentando i tipi dei caratteri, il numero delle combinazioni cresce in modo addirittura esponenziale [Vedi Figura 55], ove alla colonna "tempo" abbiamo calcolato quanto impiegherebbe un attacco "brute force" realizzato con un computer in grado di provare un miliardo di chiavi al secondo:

Quindi: **usare tutti i caratteri disponibili (95) e usare una password di (almeno) 12 caratteri** per aumentare il numero di combinazioni e quindi la sicurezza dell'account.

In questo esempio risulta chiaro uno dei principi che stanno alla base della sicurezza informatica: rendere più difficile e oneroso il compito dell'attaccante.

In altre parole: se la password è banale, sarà agevole per l'attaccante scoprirla rapidamente. Ma se invece la password è costruita in modo corretto, il tempo per scoprirla diventerà troppo lungo e quindi non più conveniente.

13.5.1 Il decalogo per una password sicura

Riassumiamo dunque le buone regole per una password sicura:

- **sempre diversa:** non utilizzare mai la stessa password in account diversi ("non puoi evitare che il tuo provider venga violato, ma puoi evitare che tutti i tuoi account vengano hackerati in un colpo solo a causa dell'utilizzo di una sola password")
- **lunga**: almeno 12 caratteri (ma anche di più!)
- **mista**: utilizzare tutti i tipi disponibili: lettere maiuscole e minuscole, numeri e caratteri speciali
- **senza senso**: evitare nomi, parole o parti di parole che possono essere ritrovati automaticamente in un dizionario in qualsiasi lingua.

Da evitare:

- sequenze o caratteri ripetuti, come ad esempio 12345678, 222222, abcdefg, o lettere adiacenti sulla tastiera (per esempio: qwerty)
- parole scritte al contrario, errori comuni di ortografia e abbreviazioni
- modificazioni ovvie alla password, come sostituire "a" con "@", "e" con "&" o "3", "s" con "$", o come inserire un numero progressivo diverso dopo la medesima parola: sono trucchi banali, ben noti agli hacker
- informazioni personali o di familiari: nome, compleanno, numero di patente e di passaporto o informazioni analoghe.

13.5.2 Una password pratica non è mai una password sicura

Vediamo alcuni esempi di password e spieghiamo perché non sono poi così sicure (tranne l'ultima) [Vedi Figura 56].

Quindi l'unica password sicura è quella che non si può ricordare, come recita il titolo di un famoso articolo dell'esperto australiano Troy Hunt: "**The only secure password is the one you can't remember**"[94].

13.5.3 Non fidatevi dei "password meter"

Quando in un sito si imposta una password, compaiono spesso barre colorate rosso/giallo/verde (o semafori) che ci indicano se la password scelta è sufficientemente forte. Questi sistemi misurano il livello di sicurezza della password, ma sono spesso poco affidabili.

Potrebbe succedere che una password composta da nome, cognome e data di nascita possa avere un punteggio elevato (perché lunga), sebbene in quanto a sicurezza sia pessima; mentre una password con caratteri casuali, ma più breve, sarebbe considerata meno sicura!

Sconsiglio di fidarsi di tali strumenti: meglio far generare la password da un buon password manager... e impostarla ben lunga, tanto sarà il PM a doversela ricordare!

Un altro grave errore che si trova su molti siti è quello di imporre un formato ("pattern") obbligato per la password. Per esempio, la password deve essere di 8 caratteri (lunghezza fissa!) con una lettera maiuscola e un numero. È infatti ovvio

che è molto più facile indovinare una password di cui si può supporre a priori la lunghezza, piuttosto che individuare una password di lunghezza sconosciuta. Ma questa sciocca imposizione si trova ancora su molti siti, persino in quelli di alcune banche.

13.5.4 Non salvare mai le password nel browser

Se per ogni account la password deve essere diversa e se una password sicura è una password che non si può ricordare, come fare a gestire tante password? Si potrebbe ricorrere a una soluzione comoda e già pronta: salvare le password nel browser. Ma non è assolutamente una buona idea...

FAQ ▶ PERCHÉ NON È SICURO SALVARE LE PASSWORD NEL BROWSER?

Esiste una funzionalità – all'apparenza molto comoda – che ci viene offerta da tutti i browser: salvare le password al loro interno. Niente di più facile: quando facciamo il login a un sito, è il browser stesso che ci offre di salvare la password appena digitata, per non doverla riscrivere alla successiva occasione.

In realtà le password così salvate possono essere scoperte molto facilmente. Non facciamoci ingannare dal fatto che compaiono sotto forma di anonimi pallini: quei "pallini" sono solo una mascheratura della password (come se fosse una formattazione o un font di carattere), ma in realtà la password **non è stata crittografata**.

Quindi con una banale operazione di modifica della "formattazione", chiunque potrebbe far comparire al posto dei pallini la password scritta in chiaro.

13.6 Usare un password manager (PM)

Come abbiamo detto, per essere sicuri dobbiamo usare password sempre diverse e molto complesse.

Tutto chiaro, ma come fare a ricordarle? Oggi le password che ciascuno di noi deve gestire sono spesso molte decine, alcune delle quali assolutamente delicate: Internet Banking, account aziendali, e-mail, ID Apple o Google (collegati agli smartphones), servizi Cloud, siti di e-commerce come Amazon e servizi di pagamento come PayPal.

La soluzione che consiglio (e che consiglia anche Troy Hunt, nell'articolo sopra citato) è semplice e molto pratica: **usare un password manager** (PM)**.**

Cosa sono? Sono programmi e app che archiviano in modo sicuro e crittografato le credenziali (username e password) di accesso ai servizi web in una sorta di cassaforte ("*vault*") virtuale, rendendola disponibile all'utente quando ne ha bisogno.

I migliori PM sono "multipiattaforma", cioè sono disponibili per i sistemi Mac, Windows, IOS e Android. Questo permette – ma non è un obbligo – di sincronizzare attraverso il Cloud (p.es. Dropbox) le password su ogni dispositivo su cui i PM sono installati (computer, laptop o smartphone che sia).

I PM sono protetti da una **master password**, che serve per aprirli e che diventa perciò **l'unica password che occorre ricordare**.

13.6.1 I vantaggi dei password manager

Sono molti i vantaggi che offrono i migliori PM presenti sul mercato:

- C'è **una sola password**: è la master password per aprirli.
- Per ciascuna voce possiamo **memorizzare molti dati**: username, password, numeri di telefono, date di scadenza, ecc. Il PM ci propone differenti modelli (siti web, carte di credito, ecc.) tra cui scegliere quello più idoneo.
- Nei migliori PM, **i dati memorizzati vengono crittografati** con sistema di cifratura AES 256 bit, una tecnica crittografica utilizzata come standard dal governo USA e che la stessa NSA ritiene adatta per proteggere i documenti classificati "Top Secret".
- Hanno la capacità di **generare automaticamente password sicure e complesse**.
- Hanno un **sistema intelligente di riempimento automatico dei moduli nei siti web** (non occorre perciò fare "copia/incolla" delle password). Questa funzionalità (presente solo in alcuni PM) è eccezionalmente comoda: è sufficiente entrare nella pagina di login del sito, avere il PM sbloccato e questo automaticamente (ed istantaneamente!) riconoscerà il sito e inserirà le relative credenziali d'accesso. A questo punto non importa più avere una password lunga 10, 20 o 30 caratteri: se ne occuperà il PM.

13.6.2 Gli svantaggi dei password manager

I migliori PM sono sicuri e molto pratici nell'uso. Segnalo solo due possibili rischi:

1. **Scegliere un password manager non sicuro**: secondo l'opinione di alcuni, potrebbe essere pericoloso affidare le proprie password a un software creato da altri. Obiezione corretta: un hacker potrebbe confezionare e mettere in commercio un PM appositamente per rubarci le password. Per evitare questo rischio – che esiste – consiglio perciò di scegliere solo PM di aziende note e affidabili. Vedremo più avanti quali sono.
2. **Dimenticare la master password:** sui PM (tranne qualche eccezione, che non consiglio) non esiste il solito pulsante "Ho dimenticato la password" per recuperare la chiave d'accesso, proprio per ragioni di sicurezza. Quindi dimenticare la master password significa non avere più l'accesso al PM e perdere irrimediabilmente tutte le proprie password!

13.6.3 I password manager più consigliati

Per quanto spiegato sopra, sarà bene affidarsi a prodotti di aziende serie e di sicura reputazione.
Elenco qui i migliori e più noti password manager attualmente sul mercato:

LastPass[95]: uno dei più conosciuti e utilizzati (soprattutto in ambito aziendale), è disponibile per Windows, Mac, Linux, IOS, Android e ha l'estensione per tutti i maggiori browser desktop e mobile. Offre setup molto granulari e ha anche il riempimento automatico ("form filling"). Presente sia la versione gratuita sia quella in abbonamento mensile (a partire da 2 $/mese).

1Password[96]: è il principale concorrente di LastPass e, a parere di chi scrive, il miglior PM sul mercato, soprattutto per il mondo Apple. Sviluppato dalla canadese AgileBits, è nato infatti per sistemi Mac (nel 2006) e poi per IOS; solo successivamente è stato reso disponibile anche per Windows e Android. Ha tutte le migliori funzionalità richieste per un PM, ottimamente sviluppate e perfettamente integrate con i principali browser, ed è dotato del riempimento automatico. È disponibile con sottoscrizione in abbonamento (a 3,99 €/mese, o 34,99 € per un anno) oppure con acquisto della licenza "standalone". Ha un ottimo servizio clienti attraverso chat (solo in inglese).

Dashlane[97]: è disponibile per Windows, Mac, iOS e Android ed è un prodotto semplice da utilizzare. Ha il riempimento automatico. Offre sia la versione gratuita sia quella in abbonamento mensile (a partire da 3,33 $/mese).

Kaspersky Password Manager[98]: anche questo disponibile per tutti I sistemi operativi, al costo di 14,95 €/anno in abbonamento.

Keeper[99]: prodotto piuttosto noto e valido, anche se non ha il riempimento automatico, è proposto in abbonamento mensile (a partire da 2,50 €/mese).

KeePass[100]: l'unico dell'elenco che è totalmente gratuito, perché si tratta di un progetto open source. Nato in ambiente Windows, esiste ora anche la versione per Mac e Linux, oltre che per iOS ed Android. L'interfaccia grafica è piuttosto datata, ma la qualità è nel complesso buona. Non ha però la comoda funzionalità del riempimento automatico.

13.7 Cambiare periodicamente le password (o forse no...?)

Esiste il principio, universalmente accettato, secondo cui le password vanno cambiate periodicamente (ogni 3-6 mesi). Questo in molti casi è addirittura un obbligo (password aziendali, Internet banking, ecc.).

La regola nacque nel 2003, quando fu emessa una guida, approvata anche dall'Istituto Nazionale degli Standard e delle Tecnologie (NIST) americano, dedicata proprio al corretto uso delle password. Essendo state pubblicate dal NIST, ente molto autorevole, queste linee guida sono state accettate in tutto il mondo.

Ma ormai il dogma è caduto: nel 2017, l'autore della guida del 2003, Bill Burr, ha "chiesto scusa" agli utenti perché "l'obbligo di cambio frequente non serve a garantire la sicurezza delle password". Al contrario, secondo Burr, se l'utilizzatore viene obbligato a cambiare la password frequentemente, finirà per sceglierla semplice e ripetitiva.

È stato dimostrato infatti che quanto più spesso si chiede a qualcuno di cambiare la propria password, tanto più deboli sono quelle che vengono scelte (magari

sostituendo un carattere alla fine).

Oggi le linee guida suggeriscono di non modificare frequentemente le password: il primo ad aver abbracciato questa impostazione è stato il Centro Nazionale di Sicurezza informatica della Gran Bretagna (NCSC) che ha pubblicato nel 2016 la propria guida: "Password Guidance: Simplifying Your Approach"[101].

Anche perché le password, quando rubate, vengono sfruttate ("exploited") immediatamente.

Quindi: scegliamo la password una volta sola, ma che sia ben robusta!

13.8 Non usare le domande di (in)sicurezza

Come abbiamo visto, non è solo l'utente a sbagliare, ma spesso anche chi ci fornisce il servizio opera in modo non sicuro. Un'altra pratica discutibile è l'uso delle "famigerate" domande di sicurezza.

Le conosciamo e le usiamo tutti: molti siti ci obbligano a impostare le "domande di sicurezza per il recupero della password" qualora ce la dimenticassimo. Ma le domande che i siti spesso ci propongono sono di questo genere (esempi reali, tratti da siti rinomati che non voglio citare):

- *Qual era il cognome da nubile di tua madre?*
- *Qual era il nome della tua scuola elementare?*
- *Il nome del tuo primo animale?*
- *La tua squadra del cuore?*

Le domande semplici non sono mai sicure (le risposte in genere sono molto facili) e chi ci conosce bene potrebbe facilmente sapere la risposta. Oppure potrebbe bastare controllare l'account Facebook o Twitter di una persona – dove sono riportate molte informazioni personali – e scoprire la risposta alla domanda di sicurezza. Secondo Google in circa 10 tentativi è possibile risalire alla gran parte delle risposte alle domande di sicurezza.

In alternativa potremmo usare domande difficili o risposte senza senso? Forse, ma poi le risposte saranno facilmente dimenticate!

Un caso molto famoso, noto come "The Fappening", è avvenuto nel 2014 (in realtà ce n'è stato più di uno, ma tutti simili): grazie alle domande di sicurezza banali sono stati violati gli account Apple iCloud di alcune attrici americane (Jennifer Lawrence, Miley Cyrus, Kate Upton, Kirsten Dunst e altre ancora). Le loro foto (alcune non proprio vestite...) sono finite nel web. Il responsabile Ryan Collins è stato poi condannato a 18 mesi di carcere[102].

Nel settembre 2016 il caso si è ripetuto (con la medesima tecnica) per la giornalista di Sky Diletta Leotta e per Pippa Middleton (a cui sono state chieste 50 mila sterline per le 3.000 foto private sottratte in iCloud).

Come non essere obbligati a usare le domande di (in)sicurezza? Utilizzando al loro posto l'autenticazione a due fattori.

13.9 L'autenticazione a due fattori

Definita anche **2FA** ("2 Factor Authentication") **o MFA** ("Multi-Factor Authentication"), è oggi il sistema di protezione più sicuro che possiamo usare. Anzi che DOBBIAMO usare: se crediamo che con una password ritenuta "abbastanza forte" si possa stare tranquilli, stiamo sbagliando. Quella password "sicura" potrebbe essere rubata o scoperta, per esempio a causa di un data breach al sito, come è successo con Linkedin, Yahoo! e molti altri. Quindi è importante avere una seconda linea di difesa, se la prima viene superata.

Per autenticarsi a sistemi digitali (computer, Internet banking o altro) ci sono tre diversi metodi:

- **"una cosa che sai"**, per esempio una password o il PIN
- **"una cosa che hai"**, come uno smartphone o un token di sicurezza [Vedi Figura 57] (quelle piccole "chiavette" che ci davano le banche e che generavano un codice a 6 cifre)
- **"una cosa che sei"**, come l'impronta digitale, il timbro vocale, l'iride, o altre caratteristiche biometriche.

Si parla di 2FA se si usano due fattori e di 3FA se ne vengono richiesti tre (molto meno usata) [Vedi Figura 58].

Come funziona?

La MFA utilizza **almeno due dei tre fattori** sopra elencati: dopo aver digitato la password (primo fattore) del proprio account, sarà richiesto di inserire un secondo fattore, che nella maggior parte dei casi è un PIN o un codice, da ottenere grazie allo smartphone (sotto forma di SMS o tramite un'apposita applicazione) o tramite un token fisico.

A differenza della password, questo secondo codice è di fatto inattaccabile, perché generato in maniera pseudocasuale secondo un algoritmo e con una durata molto limitata nel tempo (solitamente 30 secondi). Si chiama anche, per questo motivo, OTP: **"one time password"**.

Talvolta il secondo fattore è di tipo biometrico. Ne abbiamo un esempio nelle applicazioni per smartphone delle banche: per aprire l'app e anche per eseguire operazioni dispositive (p.es. fare un bonifico), ci viene richiesta la seconda autenticazione con l'impronta digitale o con il riconoscimento facciale.

13.9.1 Come ottenere il secondo fattore di autenticazione

Esistono quattro possibili modalità:

1. con un **token hardware** [Vedi Figura 59]: sistema molto sicuro ma poco diffuso. A ogni account (che ne supporti la funzionalità) viene collegato un dispositivo fisico d'accesso (simile a una chiavetta USB), realizzato secondo lo standard FIDO U2F Security Key, uno standard di autenticazione open source sviluppato inizialmente da Google e da Yubico (in figura una U2F Security Key by Yubico). Non è certamente il sistema più pratico, né il più economico: oltre ad avere un costo (non meno di 10 € per la chiavetta), oggi solo i browser Chrome, Firefox e Opera lo supportano. Inoltre richiede il collegamento diretto al computer per l'autenticazione: nel caso dei PC l'interazione è tramite porta USB. Ma nel caso degli smartphone la situazione diventa più complessa: i token per l'autenticazione a due fattori sono dotati solitamente di tag NFC ("Near Field Communication") e si collegano velocemente ai dispositivi

Android, mentre non è altrettanto semplice (almeno per il momento) con gli iPhone, perché Apple limita NFC solo ad alcuni usi (per esempio i pagamenti con Apple Pay).

2. **Attraverso un sms che ci viene inviato**: è una soluzione molto diffusa, ma è anche la meno sicura, a causa della ormai nota vulnerabilità del protocollo Signalling System No 7[103] (SS7). Inoltre esiste un rischio ancora peggiore: si potrebbe incorrere nella truffa nota come "SIM swap fraud" (di cui abbiamo parlato al par. 6.3.4 "La 'SIM Swap Fraud'"). E infine, da non sottovalutare: questo sistema ci obbliga a fornire il nostro numero di cellulare a un social network o a un sito web: questo potrebbe non essere gradito in termini di privacy.
3. Utilizzando **applicazioni dedicate o un token hardware con un display che genera un codice** a 6 cifre da inserire nel browser (come quelli che di solito vengono dati dalle banche) [Vedi Figura 60]: quando il sito rende disponibile questa opzione (non è sempre così, talvolta esiste solo l'opzione con SMS), consiglio di sceglierla, perché è il metodo più pratico, non richiede la copertura telefonica ed è molto sicuro. Le applicazioni più note – tutte gratuite – che si possono utilizzare sono Authy, Google Authenticator, Microsoft Authenticator. La stessa 1Password, che abbiamo prima presentato tra i password manager, implementa questo servizio. Il sistema tramite app non è ancora molto diffuso, ma negli ultimi anni stanno aumentando i siti che lo supportano.
4. Via **notifica push**: l'autenticazione a due fattori viene data attraverso una notifica che arriva da un'applicazione collegata al servizio in uso, ma installata su un altro dispositivo. Questo sistema si sta diffondendo nell'Internet banking: le banche stanno abbandonando i token hardware e utilizzano in alternativa le loro app installate sugli smarthphone. È una modalità molto sicura e anche semplice: dopo l'immissione di password e nome utente, la persona riceverà una notifica push sullo smartphone che gli chiederà se vuole autorizzare l'accesso attraverso l'applicazione della stessa banca. Spesso questa autorizzazione viene data mediante una pratica e veloce autenticazione biometrica: impronta digitale, viso o altro.

13.9.2 Come attivare l'autenticazione a due fattori

La modalità di attivazione è più o meno sempre la stessa: dopo essersi registrati al sito, si accede alla pagina delle "Impostazioni di Sicurezza" (il nome può anche essere leggermente diverso, ma si tratta sempre della sezione dove andiamo, per esempio, per modificare la password).

Si sceglie di attivare la 2FA, dopodiché il sito ci guiderà nella procedura e ci chiederà come vogliamo ricevere il codice: il metodo più diffuso in tutti i siti è attraverso un SMS, quindi dovremo indicare uno smartphone "affidabile" al quale il codice verrà inviato.

Consiglio di registrare sempre **due** o più numeri di telefono, per maggior sicurezza. Poi, a ogni successivo invio, ci verrà chiesto di scegliere su quale dispositivo vogliamo ricevere il codice.

Alcuni siti permettono di scegliere, in alternativa al codice via SMS, l'uso delle succitate applicazioni in grado di generare il codice temporaneo (OTP). Come detto, se disponibile, è la scelta da preferire ed è anche molto semplice: l'abbinamento viene fatto attraverso la lettura di un QRcode che compare sullo schermo del computer e che dovremo inquadrare con la camera dello smartphone. In questo modo l'applicazione si sincronizzerà con il sito.

Ciascuna di queste applicazioni permette di salvare al suo interno le OTP per tutti i siti nei quali abilitiamo la 2FA.

Nella fase di attivazione dell'autenticazione a due fattori, in genere (ma ogni sito potrebbe avere comportamenti leggermente differenti) ci verrà data anche una **chiave di recupero**, molto complessa, da conservare a parte. Di regola per la 2FA si usano Password + Codice OTP, mentre la chiave di recupero è la "soluzione di emergenza" da utilizzare solo in caso di password dimenticata o dispositivo smarrito o rubato.

Ai successivi login, oltre a username e password, dovremo inserire il codice OTP a 6 cifre visualizzato dall'applicazione [Vedi Figura 61] e che ogni 30 secondi verrà rigenerato.

Esiste – quasi in tutti i siti – una comoda opzione che ci permetterà di non dover più inserire nei login successivi il codice OTP: questa opzione si chiama in genere:

“considera questo dispositivo attendibile” (o qualcosa di simile) e va attivata una tantum.

In pratica, poiché l’autenticazione a due fattori è finalizzata a evitare accessi da computer o dispositivi diversi dai nostri, potremo fare in modo che il sito riconosca che stiamo facendo il login dal nostro “abituale” dispositivo e non ci richieda più il secondo fattore di autenticazione.

13.9.3 Quali servizi offrono l’autenticazione a due fattori?

A eccezione dei servizi di Internet banking, che ce la impongono, in tutti gli altri siti non siamo obbligati a usare l’autenticazione a due fattori. È un’opzione facoltativa, ma che consiglio caldamente, almeno per i servizi più importanti come, per esempio, Amazon, Apple ID (iCloud), Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, PayPal, Twitter, Yahoo!, Wordpress.

Ce ne sono anche molti altri che la offrono, si può consultare l’elenco completo (con visualizzazione delle opzioni disponibili per ciascun sito) su questo utile link: https://twofactorauth.org

13.9.4 Qual è il futuro dell’autenticazione a due fattori?

Secondo un recente rapporto di Juniper Research[104], il numero di utenti di smartphone che faranno uso di sistemi di autenticazione biometrica (impronta, viso, voce, iride, ecc.) crescerà di oltre il 250% nei prossimi 5 anni.

Nel 2018 la stanno usando 429 milioni di persone, che diventeranno 1,5 miliardi nel 2023. Questo eleverà la sicurezza dei pagamenti mobili. Secondo l’autore del report James Moar:

> La battaglia principale ora sarà convincere gli utenti, in particolare quelli in Europa e Nord America, che questi metodi sono sicuri almeno quanto i tradizionali sistemi di sicurezza basati su hardware.

Sicuri ma soprattutto molto semplici da usare.

13.10 Un ultimo utile consiglio: “Have I been pwned?”

L’esperto australiano di cybersecurity Troy Hunt ha creato un utile servizio che possiamo consultare gratuitamente per sapere se le nostre credenziali sono finite

in qualche "data breach".

Nel sito https://haveibeenpwned.com (che si potrebbe tradurre con: "Sono stato violato?") [Vedi Figura 62] ha classificato tutti i data breach noti degli ultimi anni, creando un archivio con oltre 5 miliardi di account violati.

È sufficiente inserire il proprio username e cliccare sul pulsante "**pwned?**" per sapere se il nostro account è stato coinvolto in qualche incidente informatico. Se così fosse, la schermata diventa rossa e compare la scritta "**Oh no — pwned!**". E vengono elencati i "**Breaches you were pwned in**", gli incidenti nei quali il nostro account è finito. Con il consiglio, ovvio, di cambiare subito la password dell'account violato!

Il sito è sicuro e ormai molto noto, tant'è che viene utilizzato anche dal browser Google Chrome, attraverso un'apposita estensione (chiamata "PassProtect"), la quale, ogni volta che inseriamo una password nel browser, controlla sul database di Haveibeenpwned se la password risulta essere stata hackerata.

E se lo è, ci dà l'informazione *"The password isn't safe"*, con l'invito a cambiarla.

---

[89] *2017 Data Breach Investigations Report* (10th Edition), Verizon 2017.

[90] https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf

[91] https://github.com/philwantsfish/shard

[92] https://www.shodan.io

[93] http://www.openwall.com/john/

[94] https://www.troyhunt.com/only-secure-password-is-one-you-cant/

[95] https://lastpass.com/it/

[96] https://1password.com

[97] https://www.dashlane.com/it

[98] http://www.kaspersky.com/password-manager

[99] https://keepersecurity.com/it_IT/

[100] http://keepass.info/

[101] https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

[102] https://www.esquire.com/lifestyle/news/a50101/fappening-hacker-sentenced/

[103] https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls

[104] https://www.juniperresearch.com/press/press-releases/future-smartphone-payments-to-rely-on-software-sec?utm_source=pressgroup_mobile_merchant_transactions_in_emerging_markets_drive_financial_inclusion_more_than_doubling_to_3.8bn_annually_in_2023&utm_campaign=mobile_payment_security_18_pr2&utm_medium=email

14

La Cybersecurity in pratica

14.1 Il tramonto degli antivirus

Abbiamo visto al capitolo dedicato ai ransomware come i tradizionali software antivirus non siano più sufficienti a garantire una difesa totale, soprattutto per il fenomeno del polimorfismo, che riesce a superare i sistemi di controllo "signature based" (basati sulle firme).

Quindi gli antivirus non servono più? Assolutamente no: è importante averli e ancora di più è essenziale mantenere sempre aggiornata la "definizione dei virus". Ma dobbiamo essere consapevoli che **gli antivirus, pur necessari, non sono più sufficienti a garantirci una protezione completa.**

Per questo sono nati nuovi programmi di sicurezza che superano il problema del controllo basato sulle firme e che operano mediante l'analisi comportamentale.

14.2 I sistemi di protezione avanzata più efficaci: User Behavior Analytics (UBA)

"Se miagola come un gatto, fa le fusa come un gatto e caccia i topi come un gatto, allora... probabilmente è un gatto". Questa semplice frase ci spiega la teoria secondo la quale è possibile identificare un soggetto attraverso i suoi comportamenti, per induzione e data la tipicità dei comportamenti stessi.

I **sistemi di analisi comportamentale degli utenti** (**User Behavior Analytics**) si fondano proprio su questo principio.

Alla base c'è la distinzione tra tutto ciò che sembra normale attività dell'utente e quello che sembra un comportamento anomalo. Questa analisi viene fatta attraverso algoritmi di "machine learning" che monitorano il comportamento degli utenti, raccolgono dati e da questi dati creano modelli comportamentali per capire qual è un "comportamento normale". Durante l'implementazione,

necessitano perciò di un tempo di apprendimento iniziale, per capire il comportamento tipico dell'utente.

In questo modo sono in grado di determinare, per esempio, se un account è stato compromesso e se il traffico generato da questo account è lecito oppure è "sospetto".

È quindi possibile rilevare il comportamento di un utente malintenzionato o quello di utente compromesso, ricordando ancora che "l'anello debole è rappresentato sempre dal fattore umano" e che molto spesso nelle aziende il pericolo arriva dall'interno (ne abbiamo parlato appunto nel par. 4.4 "Il pericolo arriva soprattutto dall'interno").

Vediamo ora un esempio. Consideriamo un utente che per la sua mansione in azienda utilizza il computer in un modo tipico e definito: usa alcuni applicativi, accede abitualmente a determinate cartelle e produce un traffico dati "tipico" e in genere verso indirizzi IP con certe caratteristiche.

Il sistema UBA avrà classificato questo comportamento come "standard". Ma se un giorno lo stesso utente usa altri programmi, oppure entra in cartelle nelle quali non avrebbe motivo di entrare (magari modificando o copiando file), o anche si collega a indirizzi IP anomali e sospetti, il sistema rileverà che "questo utente si sta comportando in maniera anomala" e invierà un allarme all'amministratore di sistema, che avrà le informazioni utili per prendere le decisioni più opportune.

L'intervento umano è quindi sempre necessario, anche per evitare i cosiddetti "falsi positivi", così come per fissare le regole che stabiliscono che cosa va considerato comportamento lecito. Queste regole, definite inizialmente, dovranno essere aggiornate sia dagli algoritmi di "apprendimento automatico" del sistema, sia dall'amministratore, in modo da tenere in considerazione i nuovi tipi di attacchi.

Gli UBA possono avere anche un'ulteriore capacità di rilevamento: poiché si è constatato che gli attacchi (soprattutto i ransomware) hanno comportamenti tipici (scrivere su determinate cartelle di sistema, collegarsi con IP particolari per scaricare malware, ecc.), sono in grado di rilevare questi comportamenti, riconoscere l'attacco e bloccarlo. In pratica gli UBA non prevengono l'attacco, ma

lo bloccano non appena si verifica. In questi casi sono anche in grado di eseguire il "**roll back**" del sistema che sta subendo l'attacco. Per fare questo creano degli snapshot ("fotografie" in un determinato istante dello stato del sistema). In caso di attacco, è possibile ritornare allo stato precedente registrato dall'istantanea.
Gli User Behavior Analytics rappresentano oggi una delle soluzioni più avanzate di protezione e tutti i maggiori vendor di sicurezza li offrono.

14.3 L'importanza del backup

Il **backup** in informatica indica l'operazione di salvataggio su un qualunque supporto dei dati archiviati in un computer (o altro dispositivo), per prevenire la perdita in caso di eventi accidentali, intenzionali o attacchi da parte di malware.
Alcuni dati significativi (e preoccupanti):

- il 30% delle persone non fa mai il backup
- 113 smartphone sono persi o rubati ogni minuto
- 1 computer su 10 è infettato da malware ogni mese.

Proprio per questo è stata istituita la **Giornata mondiale del backup**, il World Backup Day[105] [Vedi Figura 63], nata per far comprendere l'importanza di fare con regolarità il salvataggio dei dati. Si celebra dal 2011 il 31 marzo di ogni anno, giorno scelto perché precede il primo d'aprile. Lo slogan è infatti "Non farti fare un pesce d'aprile!".

Il backup andrebbe fatto ogni giorno, perché in tanti casi rappresenta l'unica soluzione per recuperare i dati dopo un incidente informatico; e un incidente che ci compromette i dati può sempre accadere, anche se crediamo di aver fatto tutto quanto necessario per proteggerli.

14.3.1 Il Disaster Recovery Plan

Il backup è quindi una misura che fa parte del **Disaster Recovery Plan**, il piano che ogni azienda dovrebbe aver predisposto preventivamente per essere pronta ad affrontare qualsiasi tipo di incidente informatico. Alla base di tutto ci deve essere un'analisi, che parte da queste domande:

- quanto sono importanti i miei dati?
- quanti dati posso permettermi di perdere senza creare un danno alla mia azienda?
- quanto tempo posso perdere per il ripristino dei miei dati, prima di subire danni?

Da queste domande derivano:
- il **Recovery Point Objective (RPO)**: rappresenta il massimo tempo entro il quale deve essere fatto il backup di un dato. Ci indica la misura della quantità di dati che siamo disposti a perdere a causa di incidente. Dal RPO discende la scelta della frequenza temporale dei backup.
- Il **Recovery Time Objective (RTO)**: è il tempo entro il quale l'azienda deve essere in grado di ripristinare la sua operatività. In pratica il tempo massimo che si ritiene tollerabile per un downtime (blocco dell'operatività).

Fatta questa analisi – preventiva – saremo in grado di stabilire:
1. ogni quanto tempo fare il backup (un'ora, un giorno, una settimana)
2. quali dati sottoporre al backup.

14.3.2 La 3-2-1 Backup Strategy

Una regola fondamentale di sicurezza ci indica che un solo backup non è sufficiente: potremmo scoprire, al momento del ripristino, che l'unica copia di backup è corrotta, quindi inutilizzabile. Questo è un rischio che nessuna azienda può permettersi di correre. Per questo si applica la regola nota come "3-2-1 Backup Strategy":

- 3 copie di ogni dato che si vuole conservare
- 2 copie "on-site" ma su storage differenti (HD, NAS, Cloud) [Vedi Figura 64]
- 1 copia "off-site" in sito remoto.

14.4 I sistemi di archiviazione avanzati: i NAS

I **NAS ("Network Attached Storage")** rientrano tra le soluzioni più efficienti per il salvataggio di dati e la loro conservazione, nonché per la loro condivisione

all'interno della rete. L'acronimo è infatti traducibile in "deposito connesso alla rete".

I NAS funzionano come molteplici dischi esterni che, invece di essere connessi al computer tramite cavo USB, condividono i dati sulla rete LAN permettendo di fatto l'accesso a tutti i computer che condividono la medesima rete.

Di norma sono dotati di una porta RJ-45 (la classica porta standard Ethernet) – e talvolta più di una per gestire la ridondanza –, una o più porte USB per la condivisione sulla rete di stampanti o chiavette USB, un processore, memoria RAM e un sistema operativo di tipo "embedded" (ovvero destinato all'uso su hardware proprietario) e molteplici dischi utili per il salvataggio dei dati e la loro ridondanza.

È quindi importante comprendere che il NAS non è un semplice "insieme di hard disk", ma piuttosto un vero e proprio computer che gestisce in modo intelligente due o più hard disk.

Il punto focale di molti NAS è infatti la possibilità di salvare i dati non su un solo disco (come avverrebbe con un comune disco fisso esterno), quanto piuttosto secondo una logica detta RAID, che permette la distribuzione, copia o partizione dei dati su più dischi.

14.4.1 Il RAID

Il RAID (originariamente detto "Redundant Array of Inexpensive Disks" o insieme ridondante di dischi poco costosi, poi corretto, visto il costo delle memorie di massa, in "Redundant Array of Indipendent Disks", ovvero insieme ridondante di dischi indipendenti) è **una logica di archiviazione** alla base del salvataggio efficiente e previdente dei dati.

Alla base della logica del RAID vi è la coeva esistenza di molteplici dischi sui quali i dati sono salvati in maniera orizzontale. Il diverso approccio al salvataggio, nonché il numero minimo di dischi necessari, è alla base della differenziazione delle varie tipologie di RAID.

Prima di esaminare le diverse versioni di RAID, è necessario introdurre un po' di terminologia tecnica:

- **Ridondanza**: replicazione, concetto alla base della logica di backup. I dati ridondati sono dati salvati su più destinazioni diverse contemporaneamente,

così in caso di rottura di uno dei dischi si ha sempre una copia aggiornata.
- **Hot swap**: possibilità di cambiare un disco rotto al volo ("a caldo"), senza spegnere il NAS/server e senza interrompere le funzionalità di alcun sistema.
- **Concorrenza**: possibilità di eseguire due o più operazioni contemporanee. Esempio: l'accesso concorrente a due dischi in lettura significa che è possibile leggere due file diversi su due dischi diversi ma afferenti allo stesso sistema, contemporaneamente.

Vediamo ora la classificazione RAID:

RAID 0: non è propriamente ridondante perché utilizza (minimo) due dischi che sono visti dal sistema come un disco unico; il salvataggio dei dati avviene a scelta alternativamente solo su uno dei dischi alla volta, quindi la capacità totale sarà la somma della capacità dei dischi, mentre la tolleranza alla rottura è pari a 0, perché tra i dischi del RAID 0 non esistono copie dello stesso dato.
Anche l'hot swap non è permesso.

RAID 1: detto anche "mirroring", ovvero "specchiamento", prevede l'utilizzo di un numero pari di dischi (generalmente due), di cui uno è copia esatta dell'altro, come dimensione e come contenuto. In questo caso abbiamo la ridonzanza.
In caso di rottura di uno dei dischi, l'altro garantisce l'accesso ai dati contenendo di fatto tutti i file del disco rotto. Il RAID 1 non garantisce però il recupero dei dati in caso di cancellazione, in quanto il dato sarebbe istantaneamente cancellato anche dal disco "specchio". L'hot swap è permesso.

RAID 2: non viene più utilizzato.

RAID 3: è un sistema in cui ogni file è diviso byte per byte tra più dischi. Questo permette una ricerca molto veloce e parallela tra più dischi, di tutti i frammenti di file grandi un byte l'uno. In caso di rottura di un disco si perderebbero unicamente i frammenti di un documento e non il file nella sua interezza. Al fine di ricostruire e recuperare il documento viene aggiunto un disco detto "disco di parità", nel quale, per lo stesso file, è salvato il risultato di una operazione matematica tra i frammenti nei dischi precedenti. Questo permette, in caso di

mancanza di un frammento dovuto alla rottura di un disco, di ricostruirlo avendo gli altri frammenti sui dischi precedenti e il risultato sul disco di parità. Questo principio di disco di parità viene adottato da tutti gli altri sistemi RAID. Il RAID 3 però non è più usato in quanto la frammentazione del file byte per byte non permette per motivi di performances le ricerche simultanee.

RAID 4: il RAID 4 suddivide i files a blocchi mantenendo però il concetto di disco di parità. Il vantaggio di scrivere solo blocchi di files (e non byte per byte) è dividere un file in gruppi minori di dimensioni quindi maggiori, riducendo il problema del RAID 3 dell'accesso concorrente. Assumiamo per esempio che in un sistema di 3 dischi RAID 4 (più uno di parità, per un totale di 4 dischi), un file sia sufficientemente piccolo da essere scritto su un blocco nel primo disco. All'atto della lettura, gli altri due dischi rimangono disponibili per operazioni di ricerca concorrenti.

RAID 5: identico al RAID 4, perde però il disco a parte "di parità", il cui contenuto viene salvato sui dischi stessi. Il grande problema dei RAID precedenti (oltre che degradare le performances a causa di letture e scritture costanti su un disco separato) era il rischio di rottura del disco di parità (che è unico). In quel caso sarebbe stato impossibile ricostruire i dati in caso di ulteriori incidenti.

RAID 6: come il RAID 5, ma introduce il concetto di doppia parità, per massimizzare la ridondanza e la capacità di ricostruzione dei dati in caso di errore. Infatti il calcolo della parità viene replicato su due dischi in contemporanea, così che la rottura di uno non impedisca la ricostruzione dei files.

È quindi evidente come la tecnologia RAID, alla base delle modalità di salvataggio dei dati sui NAS, sia fondamentale per garantire la "business continuity", in caso sia di danneggiamento dei dati, che di rottura dei dischi.
È però importante sottolineare come il NAS non sia un sistema da solo sufficiente alla gestione del backup. Infatti in caso di infezione (per esempio un ransomware) anche i dati nel NAS, se questo è connesso in rete, sarebbero compromessi.
Quindi anche per i NAS è valida la politica del backup "3-2-1" illustrata nel capitolo precedente.

Il NAS stesso – se utilizzato per i backup e non come mero disco di rete – deve essere inaccessibile ai client in rete. Solo l'utente amministratore del backup dovrà avere i privilegi di lettura/scrittura.

Un altro vantaggio dell'utilizzo dei NAS come dispositivi di storage riguarda le funzionalità messe a disposizione dal sistema operativo del NAS stesso. Autenticazione, granularità dei permessi, creazione di cartelle pubbliche o private, messaggi di allerta via mail in caso di accesso non autorizzato, crittografia del disco, sono solo alcune delle funzionalità di sicurezza avanzate non replicabili con altri sistemi di salvataggio dei dati.
Inoltre svariati produttori (come Qnap, Synology) forniscono un negozio virtuale di software (generalmente gratuiti) compatibili coi NAS di loro produzione, che permettono di evolvere il NAS da semplice dispositivo di archiviazione a strumento multimediale o, per gli utenti più smaliziati, a strumento di sviluppo.

[Torna al capitolo] 14.5 POLP: il principio del Minimo Privilegio

Nel lontano 1975 Jerome H. Saltzer, dell'Università della Virginia, enunciava il **"Principle of Least Privilege"**[106] (POLP).
Si tratta di un principio fondamentale per la sicurezza informatica, valido allora, ma ancor di più oggi che può essere sintetizzato come: "Ogni programma ed ogni utente del sistema dovrebbero operare utilizzando il più basso livello di privilegi necessari a portare a termine il proprio compito".
In altre parole:

- **Limitare i privilegi degli utenti**: ciascun utente dovrebbe avere accesso solo ai dati e alle cartelle che realmente gli servono.
- **Limitare il numero e l'utilizzo di account privilegiati**: gli account "amministratore" dovrebbero essere concessi esclusivamente agli amministratori di sistema, mentre a tutti gli altri dovrebbero essere assegnati account da semplice utente, con privilegi ridotti.
- **Evitare di esporre credenziali privilegiate su sistemi meno privilegiati e potenzialmente compromessi**: chi accede ai server del sistema dovrebbe farlo

utilizzando computer che siano diversi da quelli che utilizza per accedere, per esempio, alla rete o ai social (che rischiano di essere compromessi).

Questa regola è di grande importanza perché – non dimentichiamolo mai – un eventuale attaccante acquisirà i privilegi dell'utente che ha attaccato: se questo utente ha privilegi o accessi limitati, anche l'attaccante sarà limitato e meno invasivo.

Viceversa, se viene violato un account amministratore, l'attaccante avrà "pieni poteri" e riuscirà a fare molti più danni.

14.6 Mantenere sempre aggiornati i sistemi

Le vulnerabilità considerate più temibili sono quelle definite "Vulnerabilità 0-day" (v. par. [8.1 Vulnerabilità, Exploit, Patch, Hacker: un po' di nomenclatura preliminare]), perché non sono ancora note e non è stato ancora distribuito un aggiornamento di sicurezza (patch).

In realtà, come riporta Gartner in un suo studio, **il 90% degli attacchi che hanno successo vengono portati contro vulnerabilità note**, per le quali sono già disponibili aggiornamenti di sicurezza, ma che non sono stati scaricati da chi subisce l'attacco.

Paradossalmente **la finestra temporale di maggior rischio**, quella in cui avvengono molti sfruttamenti delle falle nei sistemi, **è quella subito dopo la pubblicazione di una patch**.

Perché? Fino a che la vulnerabilità era 0-day, probabilmente nessuno la conosceva e quindi nessuno aveva avuto la possibilità di sfruttarla. Nel momento in cui la patch viene rilasciata, diventa di dominio pubblico. Analizzandola, gli hackers possono capire come sfruttare la vulnerabilità e, con tecniche di "reverse engineering", sono in grado di costruire un Exploit in grado di attaccare i sistemi che non sono stati ancora aggiornati.

Quindi per la sicurezza **è estremamente importante mantenere sempre i sistemi aggiornati**. Questo principio è valido sia per il sistema operativo che per i software applicati e vale allo stesso modo anche per i dispositivi mobili, dove

vanno aggiornate anche le applicazioni, come abbiamo spiegato nel par. [10.4 I dispositivi non aggiornati sono più vulnerabili].

14.7 Le verifiche periodiche di sicurezza: Vulnerability Assessment e Penetration Test

Per individuare meglio le vulnerabilità di un sistema, può essere molto utile eseguire un **Vulnerability Assessment** (VA): si tratta di un'analisi di sicurezza che ha l'obiettivo di identificare tutte le vulnerabilità potenziali dei sistemi e delle applicazioni installate. Il risultato è una lista di vulnerabilità, ordinate in base alla gravità e al livello di rischio assegnato all'asset soggetto ad analisi.

Il Vulnerability Assessment esegue un'analisi dei rischi secondo una valutazione di probabilità e impatto (come spiegato nel par. 4.5.1 "L'analisi del rischio informatico") e permette quindi di definire i piani di mitigazione per ridurre o eliminare il rischio derivato da un possibile sfruttamento delle vulnerabilità.

Il **Penetration test** (detto anche "pentest") è un processo operativo che simula l'attacco da parte di un utente malevolo, usando gli stessi strumenti che userebbe un hacker.

Si tratta quindi un attacco reale, con violazione delle difese, mappatura dei vettori d'attacco, sfruttamento delle vulnerabilità e utilizzo di exploit. In altre parole, un pentest dimostra come un attaccante malintenzionato potrebbe eludere le difese della nostra organizzazione e sfruttare le vulnerabilità per accedere ai dati o prendere il controllo del sistema.

Un Penetration test può aiutare a capire se il sistema è protetto o se presenta delle vulnerabilità, individuando in questo caso quali difese il test ha perforato.

A realizzarlo sono in genere hacker, o più correttamente degli hacker speciali detti "**ethical hacker**", che utilizzano programmi appositi per fare una scansione delle vulnerabilità. Si tratta di "scanner automatici", quali, a titolo di esempio, Burp Suite, SQLmap e Raccoon.

Oltre a questi strumenti, serve poi anche l'abilità dell'hacker nell'individuare le falle del sistema per penetrarle.

Un Penetration test viene classificato in base al livello di conoscenza e al livello di

accesso concesso all'attaccante all'inizio del compito [Vedi Figura 65]

- **black box**: si presuppone che chi esegue il pentest non abbia alcuna conoscenza dei sistemi da analizzare. La modalità black box è la più neutra: determina se il sistema ha vulnerabilità o no. Alcuni problemi risultano però più difficili da individuare con questo metodo e il test rischia quindi di essere meno completo perché il rischio è che l'attaccante non riesca a violare il perimetro.
- **gray box**: se in un pentest di tipo black box, l'attaccante vede il sistema dal punto di vista di un estraneo, nel gray box ha i livelli di accesso e conoscenza di un utente, con maggiori privilegi. Si può così fare un'analisi più efficiente della sicurezza di una rete e di un sistema rispetto a una modalità black-box. Quindi i pentesters possono concentrare i loro sforzi sulle parti di maggior rischio, piuttosto che dover spendere tempo a determinare queste informazioni per conto proprio.
- **white box**: l'attaccante ha una conoscenza dettagliata dei sistemi (infrastruttura, account, indirizzi IP); questa modalità è usata per esempio nel mondo bancario dove l'hacker potrebbe essere un utente registrato, con un account cliente. I pentest white box riescono a fornire una valutazione più completa delle vulnerabilità interne ed esterne, ma potrebbero dare risultati meno realistici, poiché operano in base a conoscenze non disponibili agli hacker.

Quale metodo scegliere?

Lo scopo dei pentest è identificare le vulnerabilità che verrebbero sfruttate da un utente malintenzionato. La forma ideale sarebbe la black box, in quanto la maggior parte degli attaccanti non ha conoscenza del funzionamento interno del sistema bersaglio prima di lanciare il proprio attacco.

Tuttavia, l'hacker ha in genere più tempo da dedicare al processo rispetto a chi compie il pentest, quindi gli altri due tipi sono stati sviluppati proprio per ridurre il tempo di esecuzione.

La soluzione intermedia gray box, fornendo informazioni limitate sul sistema di destinazione, simula il livello di conoscenza che un hacker riesce a ottenere con

un accesso prolungato a un sistema; rappresenta quindi una soluzione di compromesso che potrebbe dare al pentest una maggiore efficacia.
Il pentest deve essere svolto a fronte di un contratto commerciale/tecnico stipulato tra l'azienda cliente e chi eseguirà il test. Il contratto – da non trascurare – ha lo scopo di stabilire in modo chiaro le "regole d'ingaggio" e in particolare:

- Il pentest non dovrà arrecare danni o disservizi all'azienda: è la simulazione di un attacco, non un attacco a scopo malevolo!
- L'esecutore deve impegnarsi a garantire la riservatezza dei dati che andrà probabilmente a scoprire. Questa condizione è essenziale soprattutto ora, in vigenza del GDPR.

14.8 Le polizze assicurative per il cyber rischio

La consapevolezza del rischio informatico sta crescendo: per i risk manager italiani l'incidente cyber è al terzo posto nella classifica delle minacce più temute. In particolare, preoccupano l'interruzione delle attività, la violazione e il furto di informazioni riservate e/o sensibili.

Per questo si stanno diffondendo le polizze assicurative a copertura del rischio cibernetico.

Secondo i dati pubblicati dall'ANIA (Associazione Nazionale fra le Imprese Assicuratrici) nel 2017, la diffusione di coperture specifiche per le imprese italiane è ancora molto limitata: solo il 5% delle aziende ha stipulato una polizza di questo tipo e si tratta soprattutto di grandi aziende.

È anche molto limitata l'offerta commerciale di questi prodotti e le polizze "tradizionali" spesso non considerano o escludono specifiche coperture legate al cyber rischio.

Una polizza cyber è di solito strutturata in moduli che possono essere attivati anche separatamente e che prevedono:

- il risarcimento per responsabilità civile verso terzi
- l'indennizzo delle spese sostenute per la gestione dell'emergenza, per il recupero e il ripristino dei dati

- l'indennizzo (sotto forma di diaria) delle perdite che derivano dall'interruzione totale o parziale dell'attività aziendale
- l'indennizzo dei costi relativi alle spese necessarie per la tutela dell'immagine e della reputazione
- l'indennizzo per la violazione della proprietà intellettuale
- l'indennizzo di importi illegalmente sottratti tramite trasferimento elettronico conseguenti ad accesso o utilizzo non autorizzato ai conti.

Tra le coperture che queste polizze prevedono ne manca una, ma la più importante: il recupero dei dati se sono andati distrutti.

Se un'azienda perde un capannone a causa di un incendio, potrà farlo ricostruire grazie all'indennizzo assicurativo. Ma se la stessa azienda perde i suoi dati e non ha un backup per recuperarli, **nessuna assicurazione glieli potrà ridare. Quei dati sono persi per sempre!**

Per questo, in conclusione di questo capitolo, è necessaria una considerazione: l'assicurazione contro il cyber rischio rappresenta un'ulteriore misura di sicurezza, che un'impresa lungimirante potrà considerare. Ma questo non deve farci dimenticare che **la prima e più importante misura di sicurezza è la prevenzione del rischio**.

In realtà, se un'assicurazione stipula una polizza del genere, avrà tutto l'interesse che l'incidente informatico non si verifichi e spingerà l'azienda cliente, magari con incentivi di riduzione del premio, affinché adotti politiche di sicurezza più attente. Quindi anche le polizze a copertura dei rischi informatici aiutano a migliorare la sicurezza.

---

[105] http://www.worldbackupday.com/it/

[106] http://www.cs.virginia.edu/~evans/cs551/saltzer/

Conclusioni

"Il fattore umano è veramente l'anello più debole della sicurezza". Questa frase è stata scritta dal famoso hacker Kevin Mitnick, detto il "Condor", nel suo libro *The Art of Deception* (L'arte dell'inganno). Ci possiamo credere, perché questo personaggio ha costruito la sua carriera sulla debolezza del fattore umano.

È infatti ormai assodato che oltre il 90% dei cyber attacchi sono causati da un errore umano, quindi l'affidabilità di un sistema informatico meticolosamente protetto può andare in frantumi di fronte a un click errato di un utente.

Pertanto, una delle prime cose da mettere in atto è **sviluppare una cultura e una consapevolezza in azienda**: è inutile installare delle misure di sicurezza importanti e costose, se poi le persone continuano a fare click su qualunque cosa ricevano per e-mail.

La sicurezza informatica come "Gioco di squadra"

Una sicurezza informatica ben costruita è costituita da molti componenti, ciascuno in grado di dare il suo contributo. Nessuno di questi componenti è sufficiente da solo a garantirci la sicurezza, ma tutti sono necessari.

Vediamo quindi, in conclusione, quali sono gli elementi da considerare per proteggere se stessi e la propria azienda.

Riassumiamo quanto esposto in precedenza, cercando di farne una sintesi che rappresenta un

Decalogo (doppio...) della Sicurezza

1. Usare programmi antivirus e mantenerli sempre aggiornati.
2. Installare Firewall perimetrali per limitare gli accessi agli URL non sicuri.
3. Non crediamo a qualsiasi cosa ci appare in internet: spesso l'apparenza inganna.
4. Teniamo sempre presente una regola fondamentale del web: "se è gratis,

probabilmente TU sei il prezzo".

5. Non aprire mai gli allegati di e-mail di dubbia provenienza. Usiamo la "regola dei cinque secondi": fermiamoci anche solo cinque secondi per capire se quell'e-mail ha qualcosa di sospetto. Facciamoci qualche domanda…
6. Fare attenzione anche alle e-mail provenienti da indirizzi noti.
7. Installare servizi antispam efficaci ed evoluti, in grado di proteggerci dallo spoofing.
8. Diffidare delle chiavette USB: se non siamo certi della loro provenienza, evitiamo di inserirle nel nostro computer.
9. Implementare soluzioni User Behavior Analytics (analisi comportamentale).
10. Applicare il Principio del minimo privilegio (POLP) con una gestione differenziata dei privilegi d'accesso.
11. Mantenere i sistemi sempre aggiornati (anche gli smartphone!). Scaricare le patch di sicurezza.
11. Proteggere gli smartphone con password di blocco.
12. Controllare che il sito sia in HTTPS prima di inserire dati riservati.
13. Impostare password forti e sempre diverse.
14. Non trascrivere le password su foglietti o files.
16. Non memorizzare le password nel browser.
17. Utilizzare un password manager.
18. Non usare le "domande di sicurezza".
19. Usare l'autenticazione a due fattori.
20. Fare il backup dei propri dati, in almeno due differenti destinazioni (locale e off-site). Ancora meglio: impostare una policy di backup commisurata alle esigenze dell'azienda.

E, per ultima, la regola probabilmente più importante e che può fare la differenza:

Non trascurare il fattore UMANO: fare FORMAZIONE per creare la consapevolezza dei rischi.

Nell'ambito della
SICUREZZA
la PARANOIA
è una VIRTÙ

Matteo G. P. Flora
(Fondatore di The Fool,
esperto in reputazione e tutela
della proprietà intellettuale)

• • •

Solo i
PARANOICI
SOPRAVVIVONO

Andrew Grove
(co-fondatore di Intel
e mentore di Steve Jobs)

Glossario

(fonte: Rapporto CLUSIT 2018 e altro)

Account hijacking Compromissione di un account ottenuta ad esempio mediante phishing.

Account take-over Acquisizione illecita di un account al fine di impersonificare la vittima (ad esempio di effettuare transazioni finanziarie sui suoi conti).

Adware Tipo di malware che visualizza pubblicità solitamente senza il consenso dell'utente. Può includere funzionalità spyware.

AES (Advanced Encryption Standard) Algoritmo per la cifratura dei dati a chiave simmetrica, che ha sostituito il precedente DES (Data Encryption Standard). Utilizza chiavi di cifratura a 128, 192 o 256 bit. Conosciuto anche come Rijndael (dal nome dei due crittografi belgi, Joan Daemen e Vincent Rijmen che l'hanno creato nel 1998), oggi è adottato dal Governo USA come standard per i documenti riservati. Per i documenti classificati "Top secret" viene utilizzato con chiave a 256 bit (AES 256).

AgID Agenzia per l'Italia Digitale. È l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. Ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese. https://www.agid.gov.it

AISP (Account Information Service Provider) Prestatori di servizi informativi relativi a saldi o movimenti dei conti aperti ai clienti che detengono uno o più conti di pagamento online presso uno o più istituti di credito.

Analytics-As-A-Service Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.

API (Application Programming Interface) Librerie software di un linguaggio di programmazione, ossia un insieme di procedure (routine, protocolli, funzioni) che rende possibile l'interazione tra due programmi per computer.

APT (Advanced Persistent Treath) Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: un accurato studio preventivo del bersaglio che spesso continua anche durante l'attacco; l'impiego di tool e malware sofisticati, la lunga durata o la persistenza nel tempo (l'attaccante cerca di rimanere inosservato per continuare a perpetrare quanto più possibile l'effetto).

Attacco Pivot back Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.

Backdoor La "porta sul retro". Soluzione tecnica che consente di mantenere aperto l'accesso a un

sistema superando i normali meccanismi di protezione. Entrare in un sistema in genere richiede tempo e molti passaggi, per questo gli hacker non ripetono ogni volta tutti i passaggi ma utilizzano le backdoor, ovvero piccoli programmi che permettono loro di potersi collegare in modo diretto al sistema violato. La backdoor può essere creata appositamente dallo stesso sviluppatore del software, per avere una "porta nascosta" (ben dissimulata nel programma), che gli permetta ulteriori accessi.

Black list o Block list Liste di indirizzi IP mantenute aggiornate e rese disponibili da una serie di server consultabili da chiunque, in cui vengono elencati gli indirizzi IP ritenuti fonte di spam. Le blacklist sono un sistema per combattere lo spam e sono utilizzate da molti software antispam. Le e-mail inviate dal sito verranno rifiutate dai principali servizi di posta dotati di sistemi antispam correttamente configurati. Se il mittente viene classificato come potenziale spammer l'e-mail viene bloccata. Si finisce in blacklist anche qualora si venga identificati da Google come "siti compromessi" con la conseguente segnalazione nei risultati del motore di ricerca. Un sito in blacklist avrà la sua operatività estremamente ridotta (se non completamente bloccata) e a quel punto si dovranno attivare azioni di "recupero" attraverso il provider o il servizio di hosting.

Blind signature Firma elettronica cieca utilizzata nell'ambito dell'e-voting. La preferenza espressa dall'elettore viene cifrata, poi un ufficiale elettorale autentica il voto tramite firma elettronica e infine si ha il deposito nell'urna.

Booter-stresser Strumenti a pagamento che consentono di scatenare attacchi DDoS.

Botnet Insieme di dispositivi compromessi da malware e connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco, ad esempio di tipo DDoS.

Buffer overflow Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.

Business continuity Soluzioni di natura tecnica e organizzativa predisposte per garantire la continuità dell'erogazione di un servizio.

BYOD (Bring Your Own Device) In un'organizzazione, l'impiego di dispositivi digitali personali per finalità aziendali da parte dei dipendenti. Tali dispositivi hanno un uso promiscuo (aziendale/personale) che in genere viene regolamentato da policy interne all'organizzazione.

Captatore informatico Software (detto anche "spyware") che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni. L'uso nel corso di indagini su alcuni specifici crimini è specificatamente regolamentato dal Codice Penale. L'utilizzo di spyware, se non autorizzato dalla magistratura, costituisce un reato.

CDN (Content Delivery Network) Sistemi di computer collegati in rete messi a disposizione dia un'azienda per distribuire contenuti in internet nel modo più veloce ed efficiente possibile. Per ottimizzate il servizio di consegna, il CDN sceglie il nodo ottimale, cioè quello che può soddisfare la richiesta nel minor tempo possibile: in genere è quello più vicino alla locazione del richiedente, oppure quello con un minor carico di lavoro. In pratica i CDN sono "i corrieri di internet". I più importanti nel mondo sono Akamai, Cloudflare e Amazon.

C&C (Command & Control) Centri di comando e controllo, ossia quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) da parte dell'hacker che gestisce la botnet.

CEO Fraud Tipi di attacco phishing mirati verso figure aziendali di alto profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, ecc.

CERT (Computer Emergency Response Team) Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce. Fra i principali obiettivi di un CERT: fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini; incrementare la consapevolezza e la cultura della sicurezza; cooperare con istituzioni analoghe, nazionali e internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione;facilitare la risposta a incidenti informatici su larga scala; fornire supporto nel processo di soluzione di crisi cibernetica.

Cifratura omomorfa Sistema di cifratura che consente di sommare due numeri cifrati o compiere altre operazioni algebriche senza decifrarli. Tecnica utilizzata nell'ambito dell'e-voting.

CISP (Card-based Payment Instrument Issuing Service Provider) Prestatori di servizi di pagamento che possono emettere carte di debito a valere su conti di pagamento detenuti dai clienti presso istituti di credito diversi.

CLUSIT Associazione Italiana per la Sicurezza Informatica, costituita a Milano il 4 luglio 2000. È un'associazione senza fini di lucro, che ha lo scopo di promuovere e diffondere la cultura e la consapevolezza della sicurezza informatica, promuovere iniziative per la formazione e la sensibilizzazione, fornire supporto alle imprese in materia di sicurezza informatica, intraprendere iniziative nei confronti di aziende e autorità competenti, con lo scopo di coordinare, sia sul piano nazionale che internazionale, l'evoluzione delle tecniche e delle norme di sicurezza. Redige ogni anno il "Rapporto CLUSIT" sulla sicurezza ICT in Italia. https://clusit.it

CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) Unità specializzata, interna al Servizio di Polizia Postale e delle Comunicazioni, dedicata alla prevenzione e repressione dei crimini informatici diretti ai danni delle infrastrutture critiche nazionali.

Crittografia "end-to-end" Sistema di comunicazione cifrata in cui solo il mittente e il destinatario possono leggere i messaggi (letteralmente "da un estremo all'altro"). Serve a impedire gli attacchi "man in the middle" (MITM), che puntano a rubare dati e informazioni personali "intercettando" le comunicazioni tra due utenti. Utilizza la crittografia asimmetrica (detta "a chiave pubblica"), basata sulla generazione di una coppia di chiavi, una "privata" e una "pubblica" che sono differenti. Ogni utente utilizza una chiave pubblica e una chiave privata legate tra loro in maniera indissolubile. Il doppio paio di chiavi crittografiche è necessario per cifrare e decifrare i messaggi in partenza e in arrivo. La chiave privata è destinata a rimanere sul dispositivo del mittente e del destinatario per decrittare i messaggi in arrivo; la chiave pubblica, invece, viene condivisa con l'interlocutore e utilizzata per crittografare i messaggi in uscita. Grazie a questa tecnica, creata nel 1976 da Whitfield Diffie e Martin E. Hellman, un matematico e un ingegnere della Stanford University, le comunicazioni, pur viaggiando attraverso canali "scoperti" e potenzialmente

intercettabili, sono leggibili solo dal dispositivo che ospita la chiave privata legata alla chiave pubblica utilizzata nel processo di crittografia.

Cryptojacking Attacco informatico in cui un hacker prende il controllo del computer attaccato e ne utilizza la potenza di elaborazione per fare mining di criptovalute a suo vantaggio. Dal momento che per generare criptomonete è necessario disporre di computer molto potenti, gli hacker sfruttano hardware e processori di computer di altre persone, che diventano in questo modo miner inconsapevoli. Il cryptojacking passa facilmente inosservato: il computer attaccato non subisce danni o perdite di dati, ma solo un rallentamento delle prestazioni.

Cryptolocker Malware (della categoria ransomware) che cripta i file presenti nel dispositivo infettato. L'attaccante chiede alla vittima un riscatto per renderli nuovamente intellegibili. Essendo stato uno dei primi (2013) e tra i più famosi, spesso si parla di "Cryptolocker" per definire in generale un ransomware.

CVE (Common Vulnerabilities and Exposures) Letteralmente "vulnerabilità ed esposizioni comuni". Sono le vulnerabilità note, che vengono catalogate con una sintassi *CVE – anno – numero.* A mantenere aggiornata questa classificazione è la MITRE Corporation.

Cyber attacco (o attacco informatico) Un qualunque tipo di attacco che colpisce sistemi informativi, infrastrutture, reti di calcolatori e/o dispositivi elettronici personali tramite armi informatiche (malware) che utilizzano in genere vulnerabilità dei sistemi attaccati. L'attacco è finalizzato al furto, all'alterazione o alla distruzione di dati presenti nell'obiettivo violato, oppure allo spionaggio, attraverso l'installazione di programmi cosiddetti spyware, o addirittura al blocco delle infrastrutture di intere nazioni. In quest'ultimo caso si parla di "cyber warfare" (guerre cibernetiche) o cyberterrorismo a seconda del contesto. Gli attacchi informatici utilizzano molte tecniche diverse, a seconda dell'obiettivo e della finalità dell'attacco.

Cyber espionage Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.

Cybersquatting Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.

Cyber resilience Capacità di un'organizzazione di prevenire un attacco o di resistere a un attacco ripristinando successivamente la normale operatività.

Cybersecurity Gruppo di attività e competenze multidisciplinari, complesse e sofisticate, anche non informatiche, che hanno lo scopo di proteggere tutti quegli asset materiali e immateriali che possono essere aggrediti tramite il "cyberspazio", ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale. Molte di queste competenze sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale".

Data breach Violazione dei dati personali: è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non

autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (GDPR, art.4 comma 12).

Deep web L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing, ecc.). Un piccolo sottoinsieme del Deep web è costituito dal **Dark web**.

Defacement Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.

DES (Data Encryption Standard) Algoritmo per la cifratura dei dati a chiave simmetrica, oggi superato dal più aggiornato e sicuro AES.

DNS (Domain Name System) L'insieme gerarchico di dispositivi e il protocollo utilizzati per associare un indirizzo IP a un nome di dominio tramite un database distribuito.

DNS Open Resolver Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo DDoS amplificati.

DDoS (Distributed Denial of Service) Attacchi DoS distribuiti, cioè basati sull'uso di una rete (botnet) di apparati, composta da un gran numero di sistemi compromessi e infetti, volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti, attraverso la saturazione delle risorse e il sovraccarico delle connessioni di rete dei sistemi server.

DDoS-for-hire Servizio DDoS da noleggiare.

DGA (Domain Generation Algorithms) Algoritmo utilizzato da alcuni malware per la generazione di migliaia di nomi di dominio, alcuni dei quali utilizzati dai server C&C.

DNS Cache Poisoning Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni: l'indirizzo che comparirà nella barra url di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.

DoS (Denial of Service) Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti); volumetrici, tesi a generare un volume di traffico maggiore della banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di C&C si parla di **DDoS** (Distribuited Denial of Service).

Drive-by exploit kit Attacco particolarmente insidioso che si realizza inducendo l'utente a navigare su pagine web che nascondono gli exploit kit per versioni vulnerabili di Java o dei plug-in del browser. Questo tipo di attacchi è in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.

DRDoS (Destribuited Reflection Denial of Service) Tipologia di *DDoS* che sfrutta lo spoofing dell'indirizzo IP di una vittima per inviare piccole richieste a un host vulnerabile inducendolo a indirizzare le risposte alla vittima dell'attacco. Permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del protocollo NTP.

DRP (Disaster Recovery Plan) Misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi aziendali, a fronte di gravi emergenze.

Eavesdropping Letteralmente "origliare (una conversazione)". L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni. Nell'ambito VoIP è un attacco del tutto simile al classico "man in the middle".

EIDAS Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (che abroga la direttiva 1999/93/CE) finalizzato a garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari.

ENISA (European Network and Information Security Agency) Agenzia UE, con sede in Grecia, creata nel 2004 per la sicurezza delle informazioni e delle reti. Tra i suoi compiti principali vi è il supporto alla Commissione Europea, agli Stati membri, alle istituzioni europee ad alle aziende in materia di "sicurezza cibernetica europea".

Escalation Privilege Escalation attraverso la quale un attaccante, una volta entrato nel sistema informatico, acquista i privilegi di un utente normale, che non sono sufficienti per compiere attività illecite, e quindi, attraverso spostamenti all'interno del sistema attaccato, cerca di arrivare a ottenere privilegi di amministratore o superutente.

Exploit Dal verbo *to exploit*, "sfruttare (una falla)". Codice con cui è possibile sfruttare una vulnerabilità di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le vulnerabilità note, sia i relativi exploit.

Exploit kit Applicazioni, utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le vulnerabilità di un dispositivo (di norma browser e applicazioni richiamate da un browser).

Firewall Letteralmente "muro tagliafuoco". Una difesa perimetrale per monitorare e filtrare il traffico di rete in entrata e in uscita attraverso i computer di un'azienda. Può essere un software oppure un dispositivo hardware con un software dedicato (si parla in questo caso di "appliance"). Viene usato per applicare filtri di protezione, secondo regole ("policy") definite dall'amministratore del sistema. Il filtraggio del traffico di rete viene configurato in base agli indirizzi di provenienza e di destinazione. In pratica è un filtro che si interpone tra la WAN (Wide Area Network), cioè la rete esterna, e la LAN (Local Area Network).

Fix Codice realizzato per risolvere errori o vulnerabilità nei software.

Furto d'identità Crimine perpetrato spacciandosi per un'altra persona e finalizzato a ottenere

indebitamente denaro o vantaggi, o a screditare la vittima. In quest'ultimo caso può rappresentare anche una forma di cyberbullismo (esercitato soprattutto attraverso i social media). Vittima del furto d'identità può risultare anche un'azienda con ricadute economiche, ma soprattutto reputazionali e legali.

Hacktivism Azioni che comprendono attacchi informatici, effettuate per finalità politiche o sociali.

Header Intestazione: in informatica e nella trasmissione di un pacchetto dati, indica appunto l'intestazione, quella parte di un pacchetto che contiene informazioni di controllo necessarie al funzionamento della trasmissione.

HyperText Transfer Protocol (https) Protocollo utilizzato su internet per la comunicazione sicura attraverso una rete di computer. Integra il protocollo standard HTTP con un meccanismo di crittografia di tipo Transport Layer Security (SSL/TLS). Quindi i pacchetti dati viaggiano all'interno di una connessione crittografata da TLS e non possono essere intercettati attraverso attacchi del tipo "man in the middle" (MITM). I siti web che utilizzano il protocollo HTTPS sono dotati di un certificato preinstallato che ne attesta la proprietà. I certificati vengono rilasciati da Certificate Authority (CA). Se il sito è dotato di certificato HTTPS, compare un pulsante a forma di lucchetto accanto all'indirizzo del sito. Cliccando sul lucchetto, si potrà vedere il certificato e da quale CA è stato rilasciato.

ICS (Industrial Control System) Acronimo che raggruppa i sistemi di controllo di supervisione e acquisizione dei dati SCADA (Supervisory Control and Data Acquisition), i sistemi di controllo distribuiti DCS (Distributed Control Systems) e i controllori a logica programmabile PLC (Programmable Logic Controller), impiegati usualmente negli impianti industriali.

IDS (Intrusion detection system) Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.

IMEI (International Mobile Equipment Identity) Codice univoco che identifica un terminale mobile.

IMSI (International Mobile Subscriber Identity) Codice univoco internazionale che combina SIM, nazione e operatore telefonico.

Infostealer Malware finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.

Intrusion software Spyware (definizione della Commissione Europea nell'ambito della regolamentazione dell'esportazione di prodotti dual use).
Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini.

IoC (Indicator of Compromise) Indicatori di Compromissione: sono indicatori impiegati per la rilevazione di una minaccia nota e generalmente riconducibili a indirizzi IP delle infrastrutture di Comando e Controllo (C&C), ad hash (MD5, SHA1, ecc.) e ai moduli del malware (librerie,

dropper, ecc.).

iot (Internet of Things) Internet delle cose: è un termine riferito all'estensione di Internet al mondo degli oggetti. Fu introdotto da Kevin Ashton, cofondatore e direttore esecutivo di Auto-ID Center. I campi di impiego sono molti: dalle applicazioni industriali (processi produttivi) alla logistica e all'infomobilità, fino all'efficienza energetica, all'assistenza remota, alla tutela ambientale e alla domotica.

IPS (Intrusion Prevention System) Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.

Istant phishing Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.

Jailbreak Si riferisce in genere agli iPhone ed è il processo di rimozione delle limitazioni di sicurezza imposte da Apple sul sistema operativo iOS. "Jailbreaking" significa ottenere pieno accesso al sistema operativo e alle sue funzionalità. Implica anche la violazione del modello di sicurezza, consentendo a tutte le app, incluse quelle malevole, l'accesso ai dati inseriti nelle altre applicazioni. Il jailbreak del dispositivo ne riduce drasticamente la sicurezza.

Keylogger Malware o dispositivi hardware in grado di registrare quello che la vittima digita sulla tastiera comunicando tali informazioni all'attaccante.

MAC (Media Access Control) address o indirizzo mac È un codice di 48 bit (6 byte, cioè 6 ottetti separati da un trattino) assegnato in modo univoco a ogni scheda di rete ethernet o wireless prodotta al mondo. Rappresenta un identificativo univoco, in realtà è modificabile a livello software (in modo non permanente).

Malvertising Tecniche che utilizzano la pubblicità on line come veicolo di diffusione di malware.

Malware Definizione generica di applicazioni finalizzate ad arrecare danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili...).

Man in the browser Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.

Man in the middle (mitm) In italiano "uomo nel mezzo", indica un attacco informatico in cui qualcuno riesce a porsi "nel mezzo" della comunicazione tra due parti che credono di comunicare direttamente tra di loro. In questo modo è in grado di intercettare la comunicazione ed anche di modificarla. Un esempio di MITM è un attaccante che si intromette all'interno di un access point WI-FI non criptato e ruba ("sniffa") i pacchetti dei dati trasmessi. Per evitare l'attacco MITM si utilizza la crittografia "end-to-end".

MFU (Malicious File Upload) Attacco a un web server basato sul caricamento remoto di malware o più semplicemente di file di grandi dimensioni.

Mining Lo strumento per la convalida delle transazioni nella rete di una criptovaluta. In cambio della potenza di elaborazione utilizzata, il miner ottiene come ricompensa una parte (blocco) della stessa criptovaluta. Negli ultimi anni, la complessità degli algoritmi di generazione delle criptovalute è cresciuta a tal punto che il valore della valuta ottenuta ("minata") spesso non giustifica la spesa energetica per ottenerlo.

Mules Soggetti che consentono di "convertire" attività illegali in denaro (cash out), ad esempio attraverso attività di riciclaggio.

NTP (Network Time Protocol) Protocollo che consente la sincronizzazione degli orologi dei dispositivi connessi ad una rete.

OTP (One Time Password) Password utilizzabili per una sola volta, di norma entro un tempo limitato (30 ÷ 60 secondi).

Payload Letteralmente "carico utile". Nell'ambito della sicurezza informatica è la parte di un malware che arreca danni.

Pharming Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.

Phishing Neologismo dato dall'omofonia con "fishing" (letteralmente "pescare"), per indicare un tipo di attacco che mira a indurre la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi a un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di rivelare informazioni personali come username e password, numeri di carta di credito, dati bancari, ecc.

Phone hacking Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.

PISP (Payment Initiation Service Provider) Prestatori di servizi di disposizione di ordini che trasmettono un ordine di pagamento emesso da un cliente che detiene un conto online presso un istituto di credito a favore di un conto di un beneficiario o operatore commerciale (e-merchant).

PLC (Programmable Logic Controller) Hardware che esegue un programma per gestire un processo industriale: sono simili a computer, ma più semplici e con funzioni finalizzate al controllo di una macchina industriale. E sono programmabili via computer.

PSD2 (Payment Services Directive, versione 2) Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/ UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE che stabilisce le regole in base alle quali gli Stati membri distinguono le varie categorie di prestatori di servizi di pagamento. L'Italia ha recepito la Direttiva PSD2 con il decreto legislativo 15 dicembre 2017, n. 218, pubblicato nella Gazzetta Ufficiale n. 10 del 13 gennaio 2018.

QTSP (Qualified Trust Service Provider) Prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati. La qualifica è assegnata dall'organismo di vigilanza.

Ransomware Malware che cripta i file presenti sul computer della vittima richiedendo il pagamento di un riscatto per averne la decriptazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Oltre ai citati "cryptolocker", esistono anche (con minor diffusione) i "locker-ransomware" che bloccano l'accesso al dispositivo (in genere colpiscono gli smartphone).

RAT (Remote Administration Tool) Anche: Remote Access Trojan Letteralmente "strumenti di amministrazione remota" che permettono all'amministratore del sistema o all'utente di accedere da remoto alla macchina e di eseguire operazioni sulla stessa. Vengono usati anche dal cybercrime come trojan ad accesso remoto, per avere il controllo del computer violato. Sono composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, e un file client, usato dall'attaccante per inviare istruzioni che il server esegue. Utilizzati anche negli attacchi APT.

RDP (Remote Desktop Protocol) Protocollo proprietario sviluppato da Microsoft per la comunicazione remota fra computer (in particolare per le comunicazioni tra il Terminal Server e il client Terminal Server). Utilizza di default la porta TCP/UDP 3389.

Rootkit Malware che consente il controllo occulto di un dispositivo nascondendo la presenza propria e di altri malware.

Sandbox Letteralmente "il recinto della sabbia per i giochi dei bambini". In informatica identifica un ambiente di test, di prova, isolato dal sistema principale. Viene usato per lo sviluppo e il test delle applicazioni e per eseguire operazioni potenzialmente "pericolose" per l'integrità del sistema.

SCADA (Supervisory Control and Data Acquisition) Tipologia dei sistemi di controllo industriale. Si tratta di sistemi informatici distribuiti per il monitoraggio e il controllo elettronico centralizzato di infrastrutture cd. cyber-fisiche, tra loro anche geograficamente lontane, tipicamente utilizzati in ambito industriale e per infrastrutture critiche.

Side-channel attacks Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.

SIEM (Security information & Event Management) Software che unisce le capacità di "Security Information Management" (SIM) a di "Security Event Management" (SEM). Aggrega quindi i dati corrispondenti agli eventi prodotti da dispositivi di sicurezza (Firewall, IDS, IPS, ecc.), dalle infrastrutture di rete, da sistemi e applicazioni. Correla gli eventi in maniera finalizzata al monitoraggio della sicurezza.

SOC (Security Operations Center) Centro per la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.

Social engineering Ingegneria sociale, cioè l'insieme delle tecniche di attacco basate sulla manipolazione psicologica del target, per indurlo a compiere determinate azioni o a rivelare informazioni sensibili (ad esempio, credenziali di accesso a sistemi informatici). "Fregare il prossimo con la psicologia" (Paolo Attivissimo).

Social threats Versione VoIP del furto d'identità, finalizzata a impersonare un utente e perpetrare

azioni malevole con lo scopo di arrecare danni, ad esempio il furto di informazioni aziendali riservate.

Spam Lo spam, da cui "spamming" (fare spam o spammare), è l'invio di messaggi ripetuti e indesiderati (generalmente a scopo commerciale), da cui anche la denominazione di "posta spazzatura" ("junk mail"). Il termine "spam" viene dal nome di un cibo in scatola considerato poco appetitoso e dal sapore piatto, ben poco attraente se – come i messaggi indesiderati – viene servito sempre, a pranzo e cena.

Spear phishing Letteralmente "phishing con la fiocina". È un tipo di phishing mirato verso soggetti specifici, mediante l'invio di e-mail formulate con cura, dopo aver studiato la vittima.

Spoofing Tecnica di attacco utilizzata per falsificare diverse informazioni, come ad esempio l'identità di un host all'interno di una rete o il mittente di un messaggio. Una volta che un hacker riesce a impersonare qualcun altro all'interno di una rete, gli è possibile intercettare dati riservati, diffondere informazioni false e tendenziose o effettuare qualsiasi tipo di attacco. Questa tecnica risulta particolarmente efficace in combinazione con tecniche di social engineering per ottenere l'accesso a informazioni "riservate" e credenziali degli utenti. Social media scammers o phishers usano questa tecnica ad esempio per convincere un utente a connettersi a un server malevolo intercettando così le sue credenziali.

Spyware Malware che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante. Quando gli spyware vengono utilizzati sui dispositivi mobili per intercettazione e spionaggio, si parla di "captatori informatici", impiegati anche dalle polizie per le intercettazioni telefoniche.

SQL (Structured Query Language) Linguaggio standardizzato per database basati sul modello relazionale (RDBMS) progettato per creare e modificare schemi di database.

SQL injection Tecnica mirata a colpire applicazioni web che si appoggiano su database programmati con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in input e l'inserimento di codice malevolo all'interno delle query. Tali attacchi consentono di accedere alle funzioni di amministrazione del sistema oltre che di sottrarre o alterare i dati.

SSH (Secure Shell) Protocollo cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.

SSL (Secure Sockets Layer) Letteralmente "Livello di socket sicuro". È stato il primo protocollo crittografico che ha permesso una comunicazione sicura dalla sorgente al destinatario ("end-to-end") sulle reti TCP/IP (qual è, per esempio, Internet). Serve a garantire autenticità, integrità e confidenzialità dei dati trasmessi. Diverse versioni del protocollo SSL (ora TLS) sono ampiamente utilizzate in applicazioni come i browser, l'e-mail, la messaggistica istantanea e il VoIP. Un esempio di applicazione di SSL/TLS è nel protocollo HTTPS. La comunicazione fra sistemi può riguardare un server o client (ad es. un sito web di e-commerce e un browser) o due server. In questo modo è possibile impedire la lettura e l'intercettazione di qualsiasi dato trasferito fra i due

sistemi in comunicazione. Serve a prevenire l'attacco MITM ("Man in the Middle").

TCP (Transmission Control Protocol) Protocollo di rete per il trasporto dei pacchetti dei dati. È uno dei protocolli fondamentali che hanno permesso lo sviluppo della rete, poiché Internet esegue la trasmissione dei dati a pacchetti.

TLS (Transport Layer Security) Protocollo per la comunicazione sicura su reti TCP/IP. È una versione aggiornata e più sicura di SSL (Secure Sockets Layer). Diverse versioni del protocollo sono ampiamente utilizzate in applicazioni come i browser, l'e-mail, la messaggistica istantanea e il VoIP. Un esempio di applicazione di SSL/TLS è nel protocollo HTTPS. Gmail di Google (per esempio) utilizza TLS per impostazione predefinita.

TOR Rete di dispositivi che consente l'uso dei servizi internet in modalità anonima (www.torproject.org).

Trojan horse Malware che si installa in modo occulto su un dispositivo presentandosi come un file legittimo (ad esempio con estensione .doc o .pdf): Il file in realtà cela un programma che consente l'accesso non autorizzato al sistema da parte dell'attaccante. Il trojan può avere diverse funzioni: dal furto di dati all'assunzione del controllo o al danneggiamento del sistema target. Particolare categoria sono i cd. Banking Trojan, programmati per acquisire le credenziali di accesso degli account dei siti di banca on-line al fine di effettuare illeciti trasferimenti di fondi verso conti bancari controllati da gruppi di cyber criminali.

UDP (User Datagram Protocol) È uno dei principali protocolli di trasporto di Internet. È un protocollo di livello di trasporto a pacchetto, che, a differenza di TCP, non prevede l'interazione di ritorno tra sorgente e destinatario (per esempio per verificare se il destinatario è raggiungibile).

UPNP (Universal Plug and Play) Protocollo di rete che consente la connessione e condivisione automatica di dispositivi a una rete.

VoIP (Voice over ip) Voce tramite protocollo Internet: è una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o una qualsiasi altra rete dedicata che utilizzi il protocollo IP (ad esempio la propria rete LAN aziendale) invece di utilizzare la rete telefonica tradizionale (PSTN). Il VOIP offre molti vantaggi: la riduzione dei costi soprattutto sulle chiamate a lunga distanza (internazionali e intercontinentali) e la possibilità per persone dislocate su sedi diverse di lavorare insieme come fossero nello stesso ufficio con risparmio di tempo e di costi. Inoltre un numero telefonico su rete digitale resta attivo indipendentemente dalla sua localizzazione, in quanto si riferisce all'indirizzo IP cui è collegato, a differenza di un numero telefonico su una rete analogica che è legato a una precisa posizione geografica ed è attivo solo ad un preciso indirizzo fisico. D'altra parte, a differenza della rete telefonica tradizionale, richiede la presenza di una copertura internet e quindi non funziona in assenza di corrente elettrica che alimenti il router; inoltre si potrebbero avere ritardi nella trasmissione qualora la banda non sia sufficientemente ampia.

VPN (Virtual Private Network) Una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso,

come ad esempio la rete Internet. La connessione VPN crea un tunnel "virtuale" (protetto e sicuro) che viaggia attraverso la rete pubblica come fosse un cavo fisico. In questo modo la comunicazione end-to-end tra utenti rimane a livello logico confinata all'interno della rete privata stessa. Si utilizza VPN quando serve una connessione di rete sicura da remoto: in questo modo si possono utilizzare le risorse di rete aziendali (cartelle, sistemi informatici gestionali, posta elettronica) senza rischi. L'accesso alla VPN deve essere protetto da un processo di autenticazione forte.

VBR (Volume Boot Record) Piccola porzione di disco allocata all'inizio di ciascuna partizione e che contiene un codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.

Vulnerabilità Debolezza intrinseca di un asset (ad esempio un'applicazione software o un protocollo di rete) che può essere sfruttata da una minaccia per arrecare un danno.

Vulnerabilità 0-day Una vulnerabilità sconosciuta o nota solo a pochi, ancora sconosciuta agli sviluppatori del software, che quindi hanno avuto "zero giorni" per ripararla e per distribuire una patch. Gli attacchi zero-day sono considerati una minaccia molto grave, in quanto sfruttano falle di sicurezza per le quali non è ancora disponibile nessuna soluzione (patch).

Watering hole Letteralmente "l'abbeveratoio". Particolare tipologia di attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target (individuato sulla base di attività di osservazione e profilazione della vittima). Tale strategia si rivela particolarmente utile laddove non sia possibile diffondere il malware tramite spear phishing.

Web injects Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.

Whaling Variante di phishing in cui si cerca di far abboccare un grande pesce (*whale*, "balena"). Consiste nel cercare di ingannare un alto dirigente o comunque una figura di elevato profilo aziendale, oppure un suo collaboratore, per indurlo con l'inganno a fornire informazioni riservate o addirittura a spostare somme in favore dell'attaccante.

XSS (Cross Site Scripting) Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.

Zero-day attach Attacco compiuto sfruttando vulnerabilità non ancora note/risolte.

Bibliografia

Libri

Walter Isaacson, *The Innovators*, Simon & Schuster, New York 2014; trad. it. *Gli Innovatori*, Mondadori, Milano 2013.

Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Penguin, London 2007; trad. it. *Il cigno nero. Come l'improbabile governa la nostra vita*, Il Saggiatore, Milano 2013.

Carola Frediani, *Guerre di rete*, Laterza, Roma-Bari 2017.

Riccardo Meggiato, *Cyberwar. Lo sapevi che un computer può uccidere?*, Hoepli, Milano 2016.

Ioannis Tsiouras, *Risk Management – La norma ISO 31000:2018. La metodologia per applicare efficacemente il risk management in tutti i contesti*, Youcanprint, Lecce 2014.

Francesco Amato, Giorgio Sbaraglia, *GDPR kit di sopravvivenza*, GoWare, Firenze 2018.

Rapporti e articoli

Gianfranco Tonello, "Ransomware 2017 Italy", TG Soft C.R.A.M., 2017.

Raoul Chiesa "La minaccia cyber: il futuro del cyber (il 'Cyberfuturo'?)".

"Rapporto Clusit 2016 sulla sicurezza ICT in Italia", CLUSIT, Milano 2016.

"Rapporto Clusit 2017 sulla sicurezza ICT in Italia", CLUSIT, Milano 2017.

"Rapporto Clusit 2018 sulla sicurezza ICT in Italia", CLUSIT, Milano 2018.

"2015 Italian Cybersecurity Report", CIS-La Sapienza, Roma 2014.

"2016 Italian Cybersecurity Report", CIS-La Sapienza, Roma 2016.

"The Top Ten Phishing Emails That Hook Us", Sophos, June 2018.

"SophosLabs 2018 Malware Forecast", Sophos, 2018.

"W32.Stuxnet Dossier Version 1.3 (November 2010)", Symantec, Cupertino (CA) 2010.

"W32.Stuxnet Dossier Version 1.4 (February 2011)", Symantec, Cupertino (CA) 2011.

"2017 Data Breach Investigations Report (10th Edition)", Verizon, New York 2017.

"2018 Data Breach Investigations Report (11th Edition)", Verizon, New York 2018.

"For Your Eyes Only? Ranking 11 technology companies on encryption and human rights", Amnesty International, London 2016.

Adam Alessandrini, "RANSOMWARE Hostage Rescue Manual", KnowBe4, Clearwater (FL) 2016.

"Analysis of the Cyber Attack on the Ukrainian Power Grid", E-ISAC, Washington DC 2016.

McAfee Labs, “Report sulle minacce (Aprile 2017)”, Intel Security, 2017.

Federal Bureau of Investigation et al., “Protecting Your Networks from Ransomware”, 2016.

“Cisco 2017 Annual Cyber Security Report”, CISCO, San Jose (CA) 2017.

“Framework for Improving Critical Infrastructure Cybersecurity Version 1.1”, NIST (National Institute of Standards and Technology), 2018.

“Sicurezza cibernetica: il contributo della Banca d’Italia e dell’Ivass”, a cura del Gruppo di coordinamento sulla sicurezza cibernetica (GCSC), Banca d’Italia e Ivass, 2018.

Ringraziamenti

Questo libro rappresenta la sintesi di un percorso professionale che è stato possibile anche grazie al supporto ed ai consigli di alcune persone che qui desidero ringraziare di cuore:

Cristina Vernizzi per avermi chiesto di scrivere questo libro, e per averlo poi così ben editato

Mario Mancini per avermi fatto scrivere questo libro

Uberto Vittorio Favero per il contributo tecnico, da vero “nerd”

Giovanni Principato per la consulenza legale

Alessandro Gigliotti per avermi dato l’opportunità di fare il mio primo corso

Marco Tupponi, l’amico di sempre, per il supporto e la carica che mi ha dato

Lia Benvenuti per i preziosi consigli

Alberto Rossi per aver creduto in me.

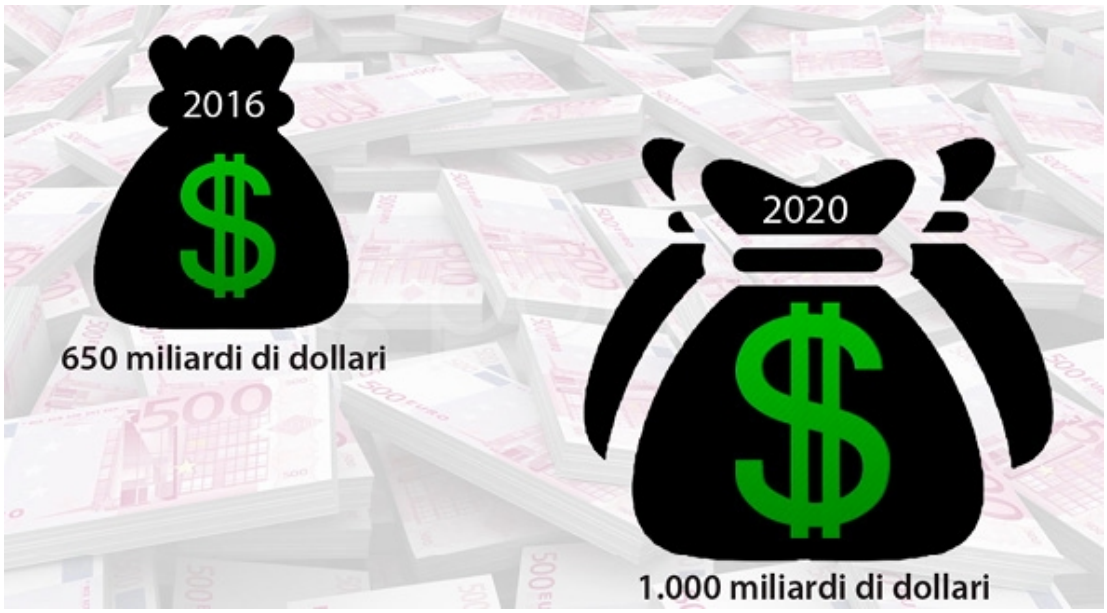
Un ringraziamento particolare a Federmanager Bologna-Ravenna.

E infine a Paola, che ha pazientemente corretto tutte le bozze.

Grafici, tabelle e illustrazioni

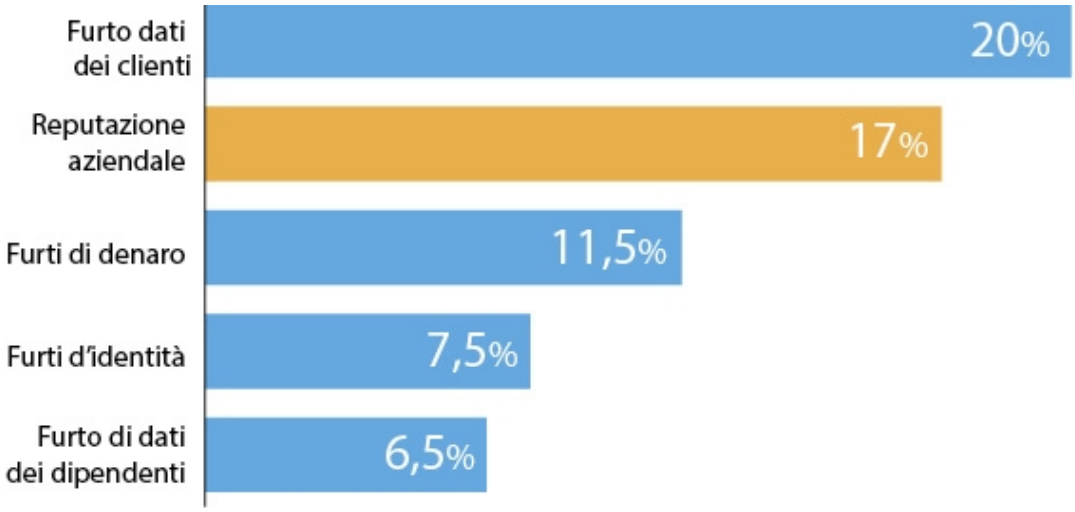
Un graffito dell'artista brasiliano Eduardo Kobra nel quartiere di Wynwood a Miami.

[Torna al capitolo] Figura 1 – Il peso del cybercrime sull'economia mondiale: 2016 e previsioni 2020 (fonte: IDC)



[Torna al capitolo] Figura 2 – Rapporto Clusit

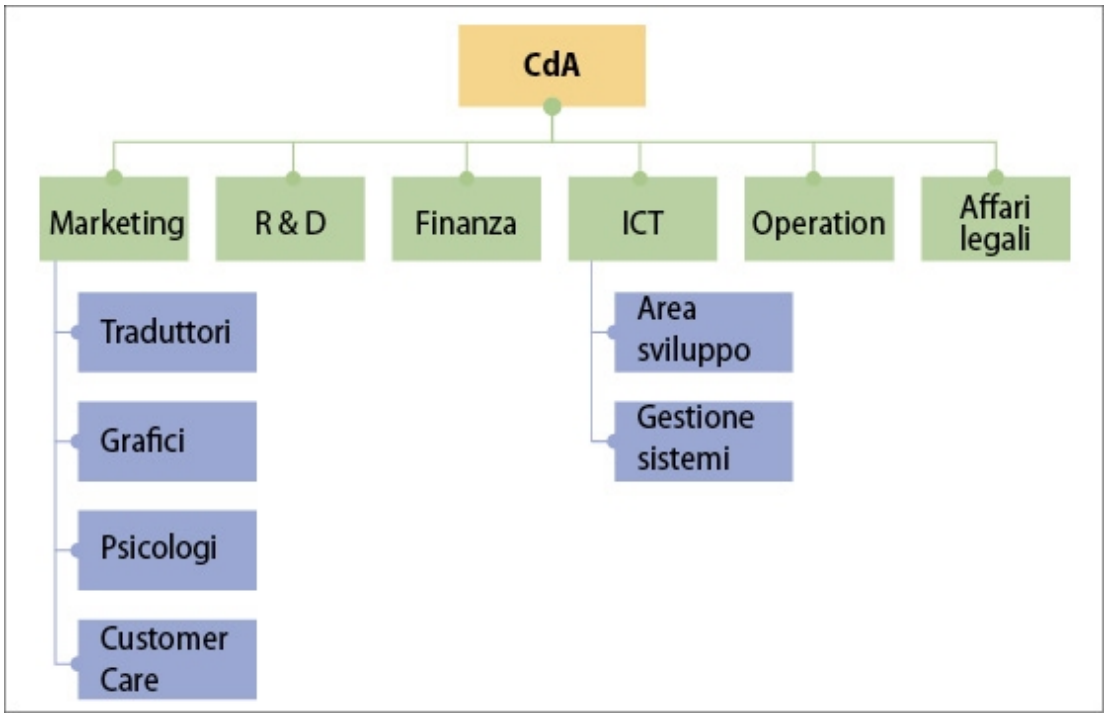
[Torna al capitolo] Figura 3 – I rischi più temuti dalla aziende in relazione al cybercrime (fonte: Rapporto Italia 2017 di Eurispes)



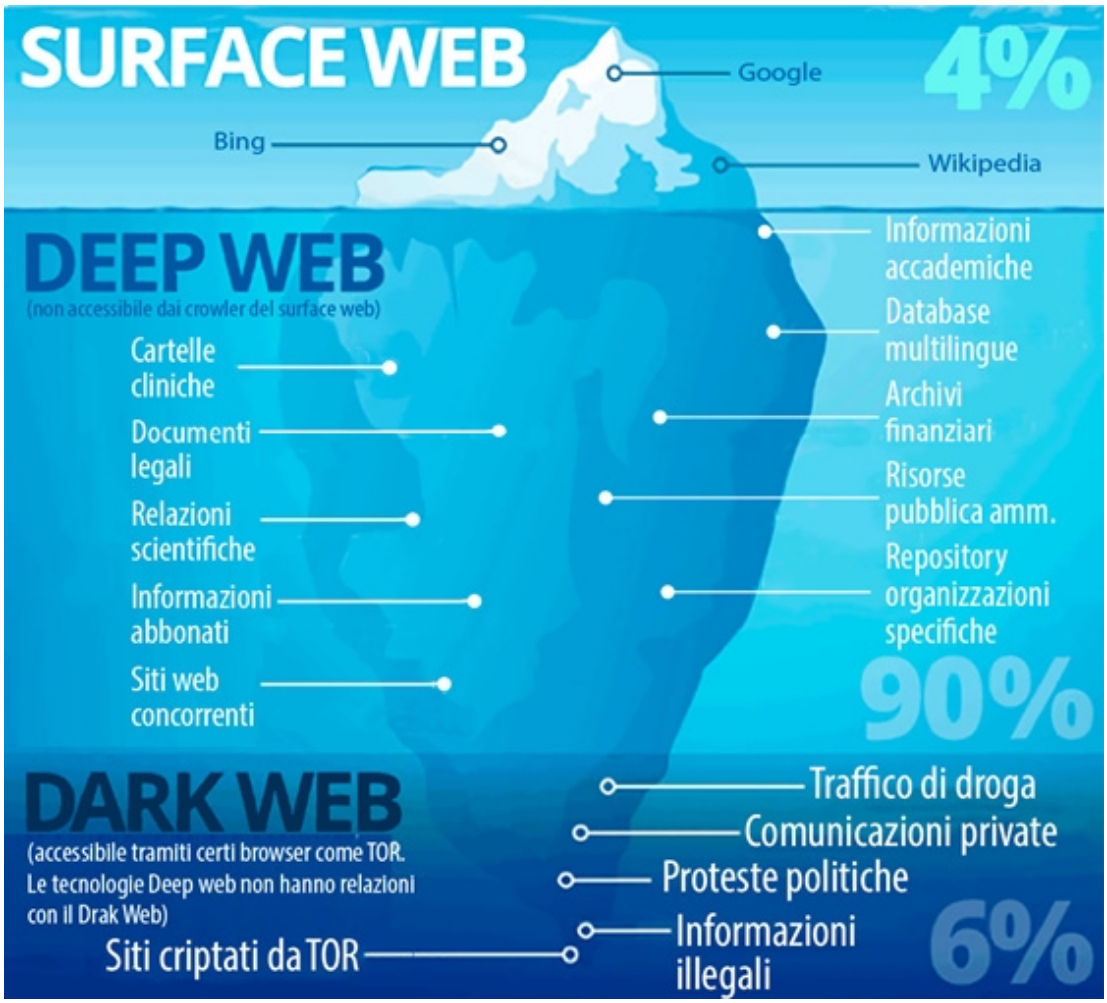
[Torna al capitolo] Figura 4 – L'ECSM

[Torna al capitolo] Figura 5 – C'era una volta...

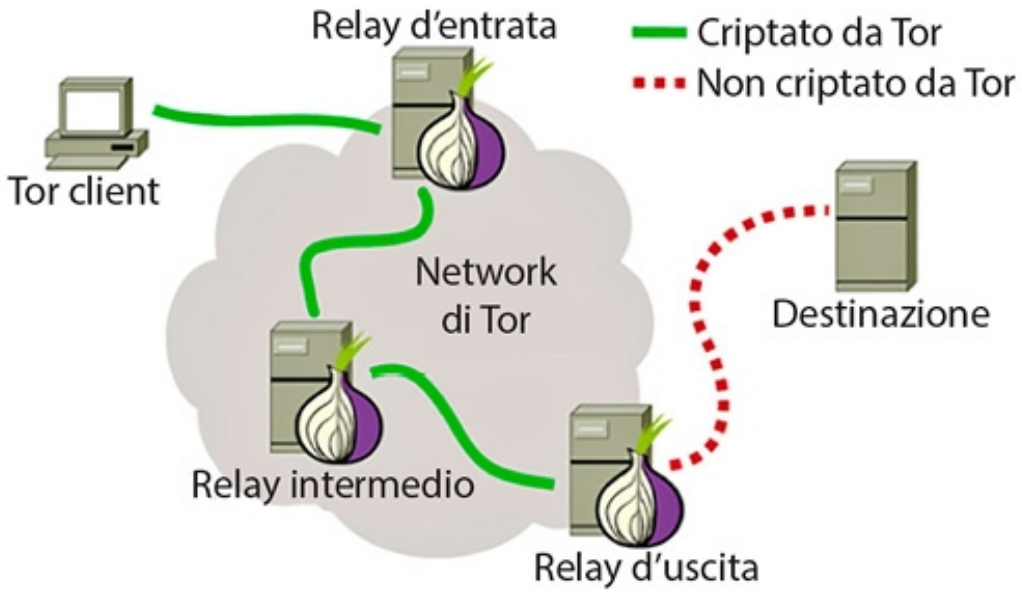
[Torna al capitolo] Figura 6 – Il modello organizzativo della cybercrime S.p.A.



[Torna al capitolo] Figura 7 – Gli strati del web



[Torna al capitolo] Figura 8 – Come funziona TOR



[Torna al capitolo] Figura 9 – Il messaggio di richiesta di riscatto di WannaCry

[Torna al capitolo] Figura 10 — Yahoo: nel 2013, mezzo milione di account rubati

[Torna al capitolo] Figura 11 – Chi sono i “bad guys”?

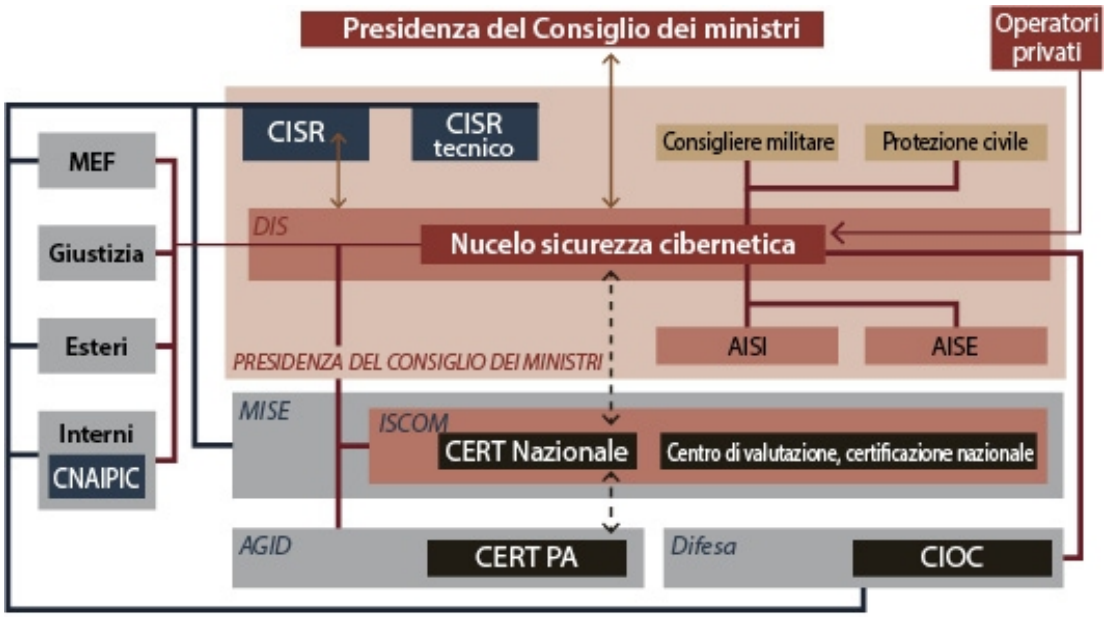
[Torna al capitolo] Figura 12 – Il comportamento delle persone mette a rischio l'azienda

[Torna al capitolo] Figura 13 – Salvaguardia dei dati da cyber rischi

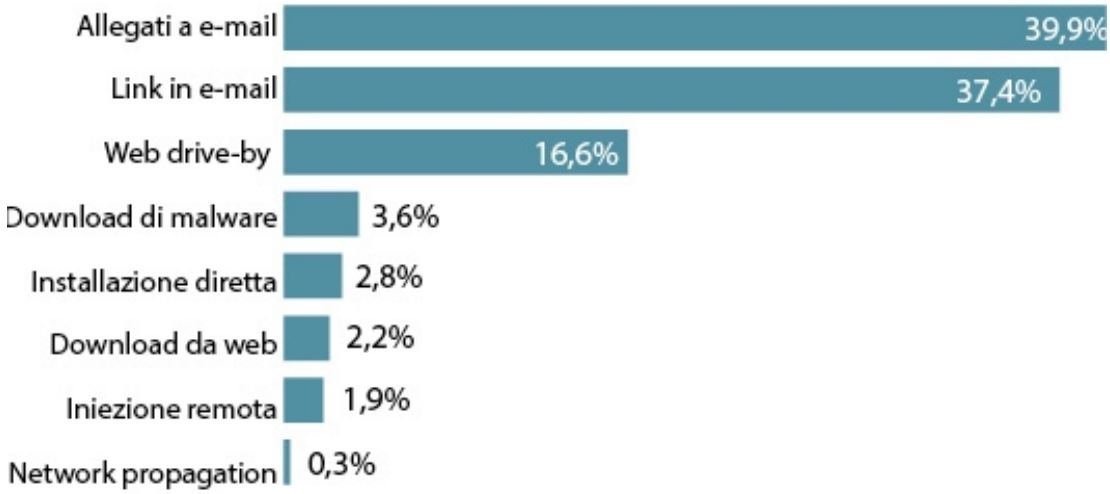
[Torna al capitolo] Figura 14 – La matrice per l'analisi del rischio

		Impatto				
		1 Insignificante	2 Minore	3 Moderato	4 Maggiore	5 Catastrofico
Probabilità	5 Quasi certo	5 Rischio Medio	10 Rischio Medio	15 Rischio Alto	20 Rischio Alto	25 Rischio Alto
	4 Probabile	4 Rischio Medio	8 Rischio Medio	12 Rischio Medio	16 Rischio Alto	20 Rischio Alto
	3 Possibile	3 Rischio Basso	6 Rischio Medio	9 Rischio Medio	12 Rischio Medio	15 Rischio Alto
	2 Remoto	2 Rischio Basso	4 Rischio Basso	6 Rischio Medio	8 Rischio Medio	10 Rischio Medio
	1 Improbabile	1 Rischio Basso	2 Rischio Basso	3 Rischio Basso	4 Rischio Medio	5 Rischio Medio

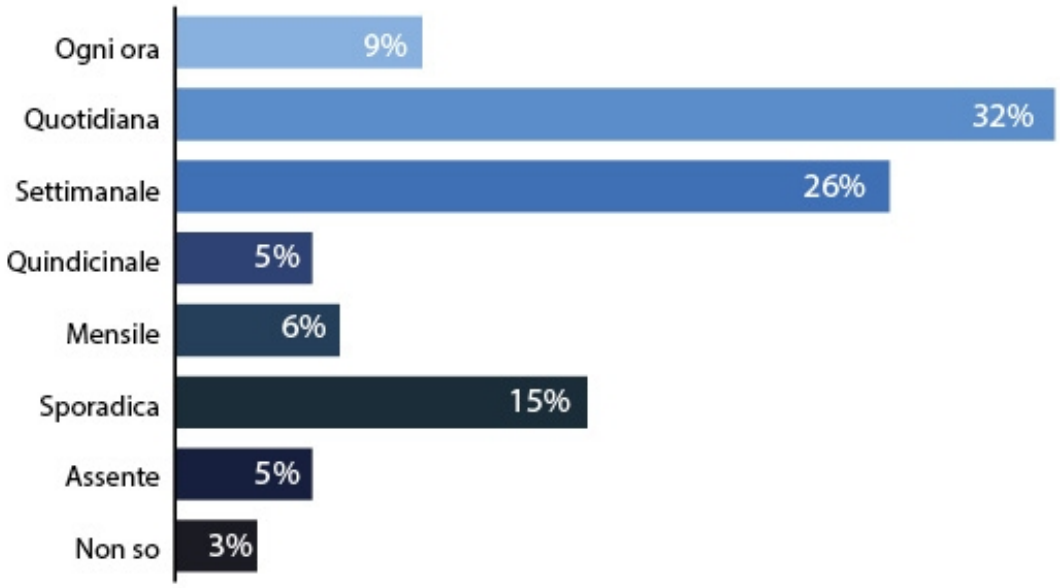
[Torna al capitolo] Figura 15 – Architettura nazionale per la cybersecurity del DPCM Gentiloni



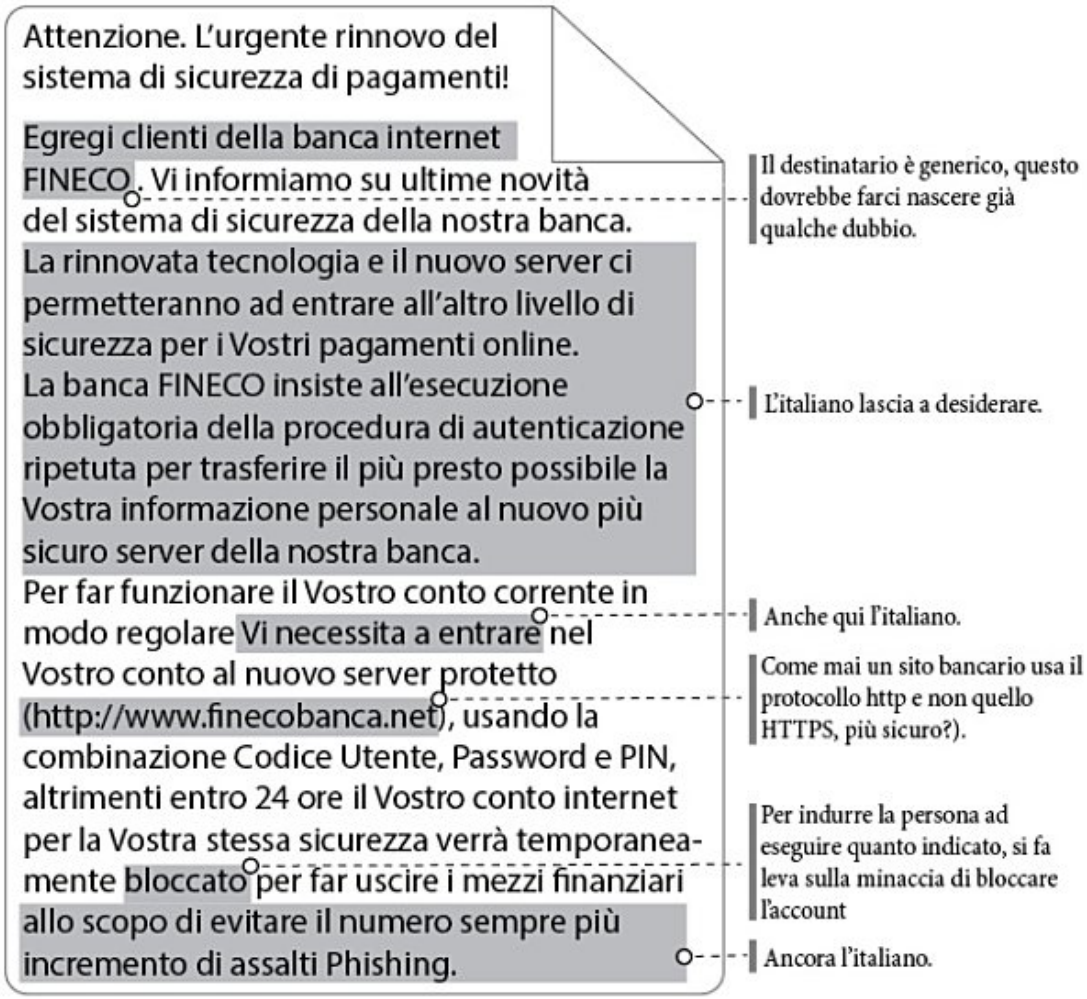
[Torna al capitolo] Figura 16 – I vettori dell'installazione di malware



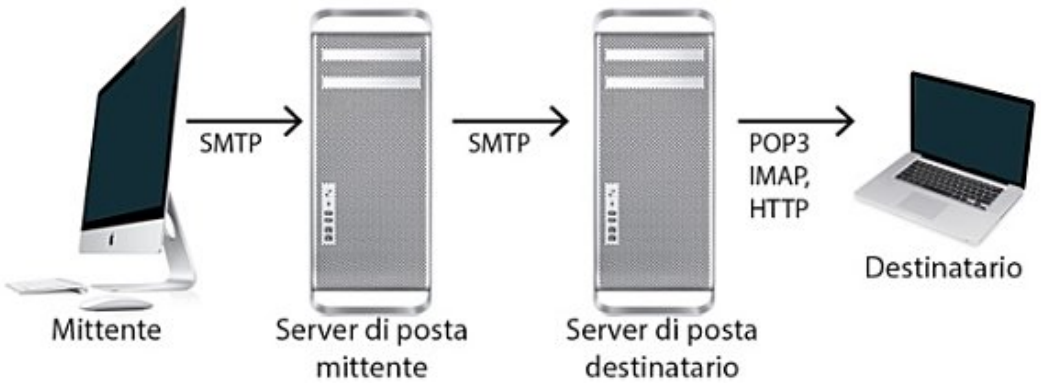
[Torna al capitolo] Figura 17 – Frequenza degli attacchi di phishing



[Torna al capitolo] Figura 18 – La e-mail di phishing del sedicente nuovo sito Fineco



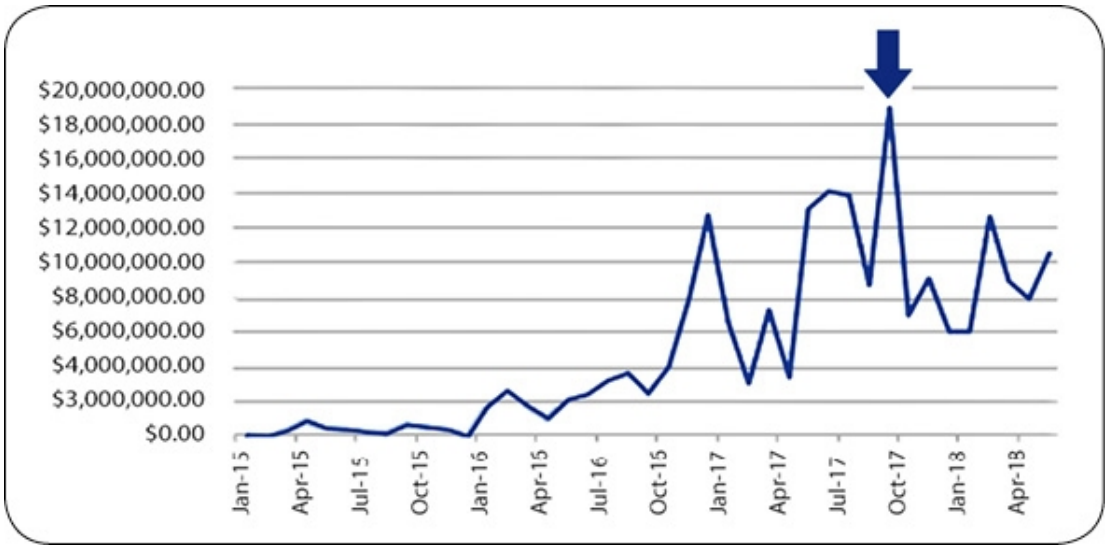
[Torna al capitolo] Figura 19 – Come funziona la posta elettronica



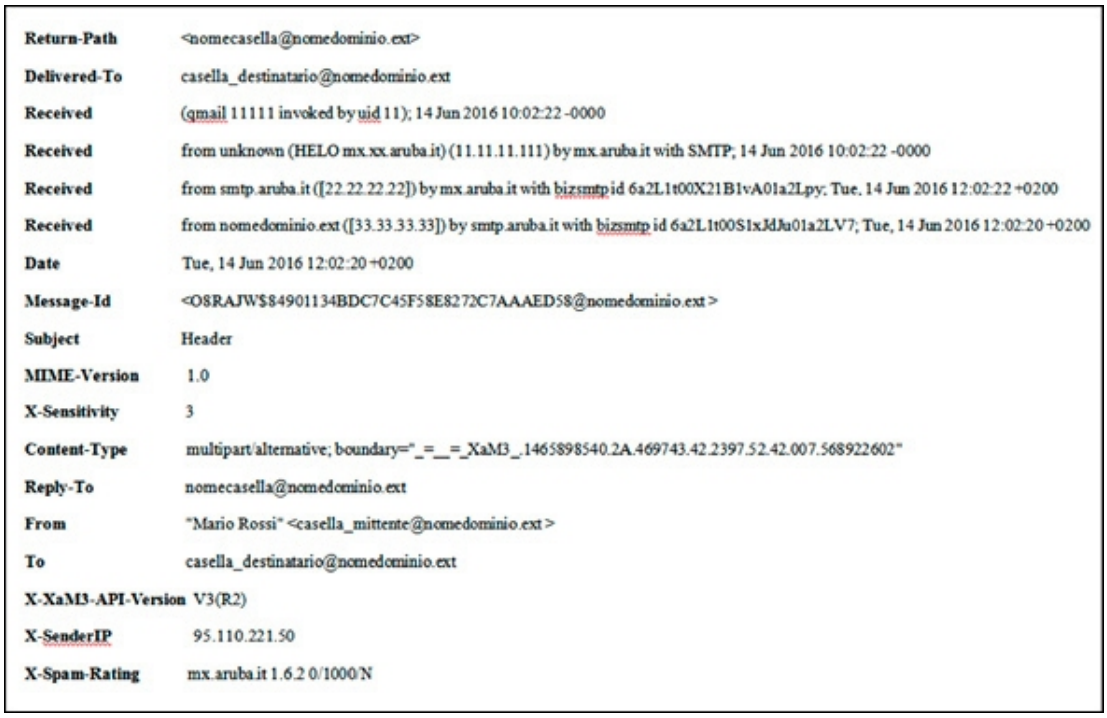
[Torna al capitolo] Figura 20 – La notizia sulla stampa

[Torna al capitolo] Figura 21 – L'ammonimento dell'FBI sui danni delle truffe BEC

[Torna al capitolo] Figura 22 – Le perdite dovute a truffe BEC nel settore immobiliare (Fonte: FBI, Rapporto Business E-mail Compromise Jul 12, 2018



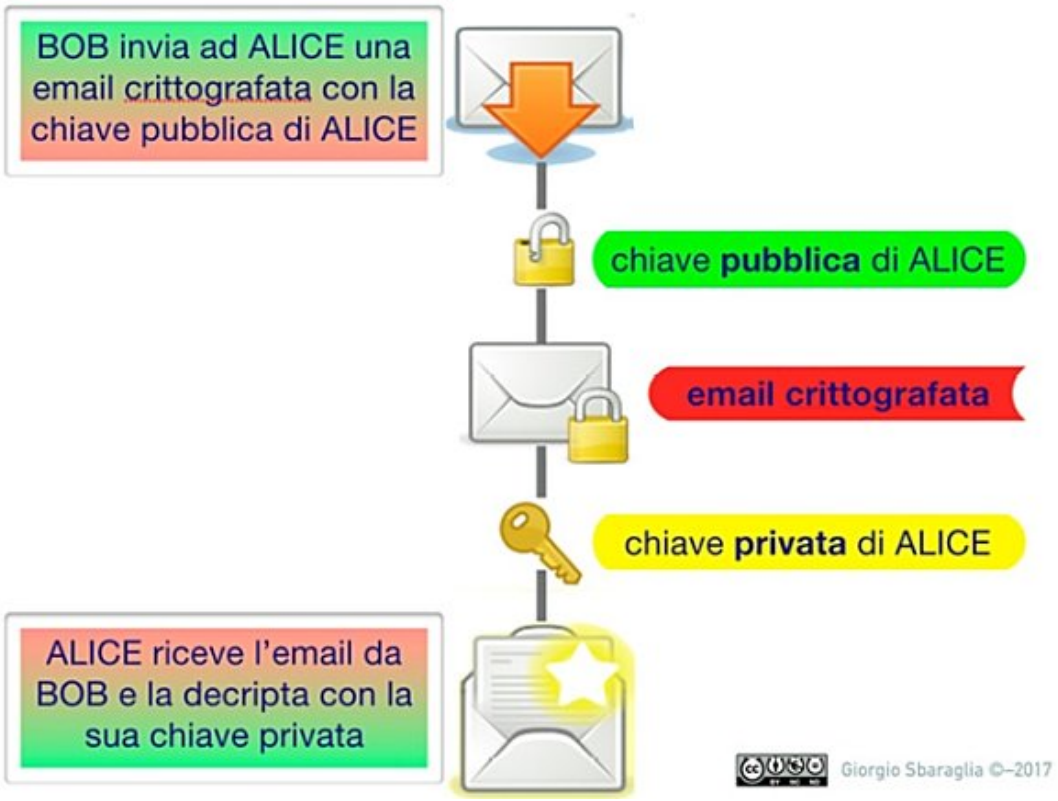
[Torna al capitolo] Figura 23 – Esempio di header di un'e-mail



Return-Path	<nomecasella@nomedominio.ext>
Delivered-To	casella_destinatario@nomedominio.ext
Received	(qmail 11111 invoked by uid 11); 14 Jun 2016 10:02:22 -0000
Received	from unknown (HELO mx.xx.aruba.it) (11.11.11.111) by mx.aruba.it with SMTP; 14 Jun 2016 10:02:22 -0000
Received	from smtp.aruba.it ([22.22.22.22]) by mx.aruba.it with bizsmtp id 6a2L1t00X21B1vA01a2Lpy; Tue, 14 Jun 2016 12:02:22 +0200
Received	from nomedominio.ext ([33.33.33.33]) by smtp.aruba.it with bizsmtp id 6a2L1t00S1xJdJa01a2LV7; Tue, 14 Jun 2016 12:02:20 +0200
Date	Tue, 14 Jun 2016 12:02:20 +0200
Message-Id	<O8RAJW$84901134BDC7C45F58E8272C7AAAED58@nomedominio.ext >
Subject	Header
MIME-Version	1.0
X-Sensitivity	3
Content-Type	multipart/alternative; boundary="_=__=_XaM3_.1465898540.2A.469743.42.2397.52.42.007.568922602"
Reply-To	nomecasella@nomedominio.ext
From	"Mario Rossi" <casella_mittente@nomedominio.ext >
To	casella_destinatario@nomedominio.ext
X-XaM3-API-Version	V3(R2)
X-SenderIP	95.110.221.50
X-Spam-Rating	mx.aruba.it 1.6.2 0/1000/N

[Torna al capitolo] Figura 24 – Edward Snowden con Glenn Greenwald a Hong-Kong

[Torna al capitolo] Figura 25 – Funzionamento del PGP

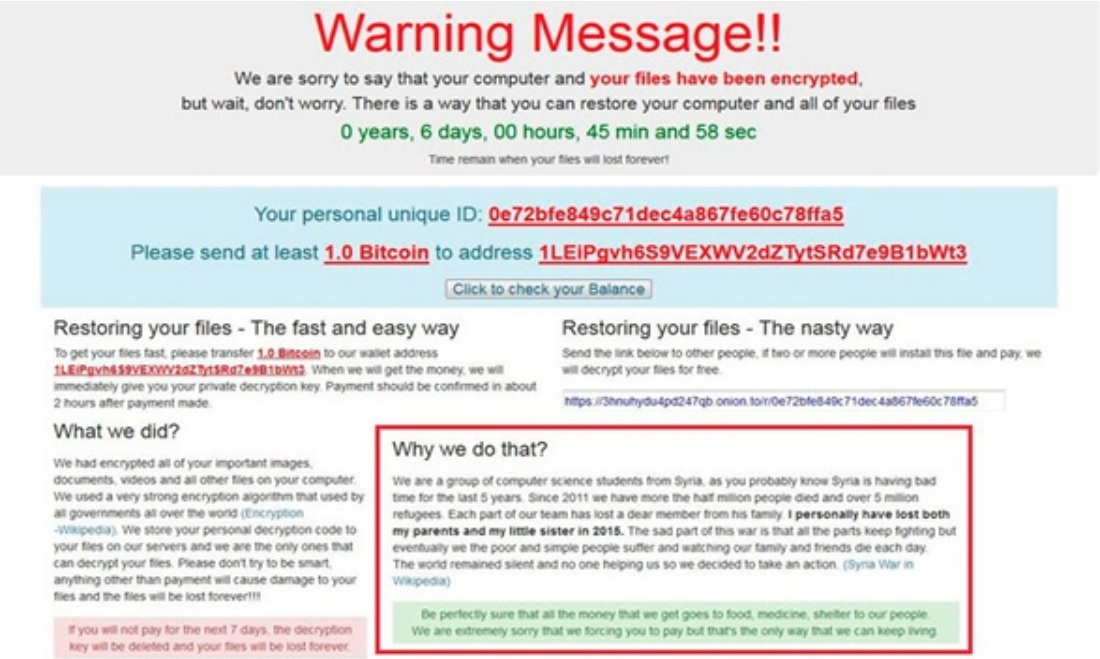


[Torna al capitolo] Figura 26 – Il primo ransomware

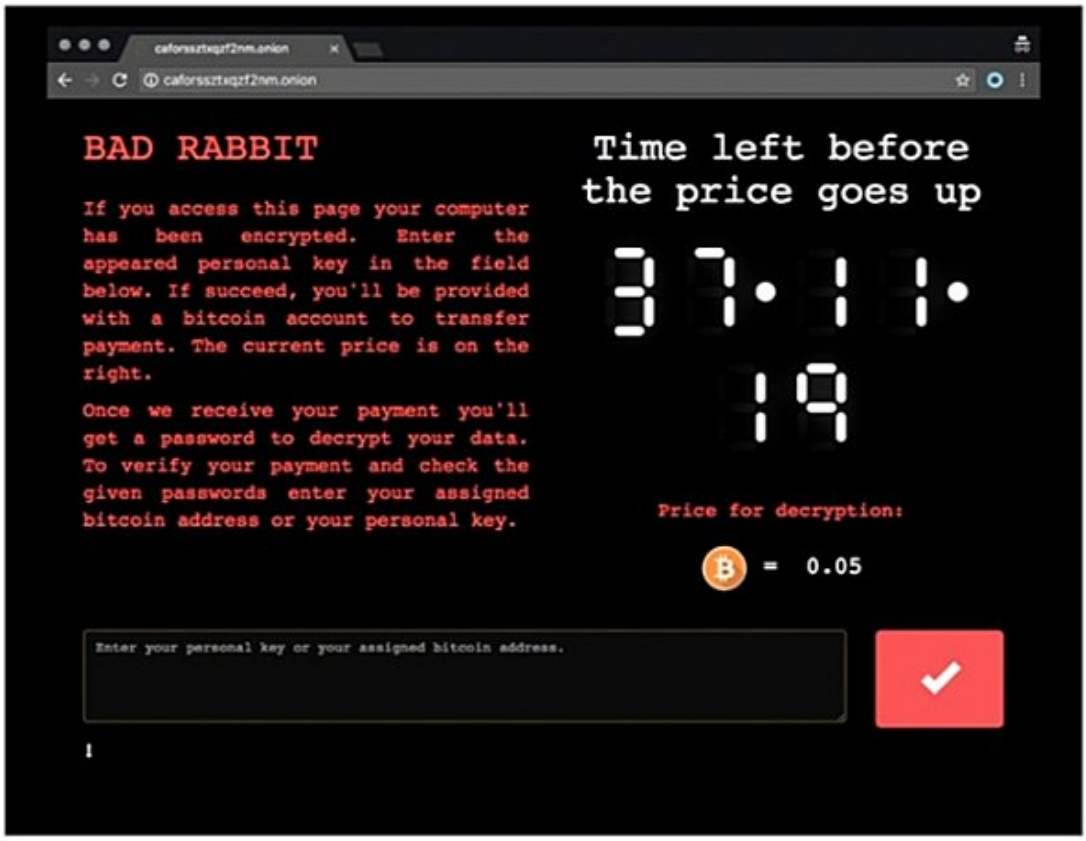
[Torna al capitolo] Figura 27 – Il messaggio del famoso Lockscreen Ransonware che visualizzava una finta schermata della Guardia di Finanza

[Torna al capitolo] Figura 28 – Ecco Petya!

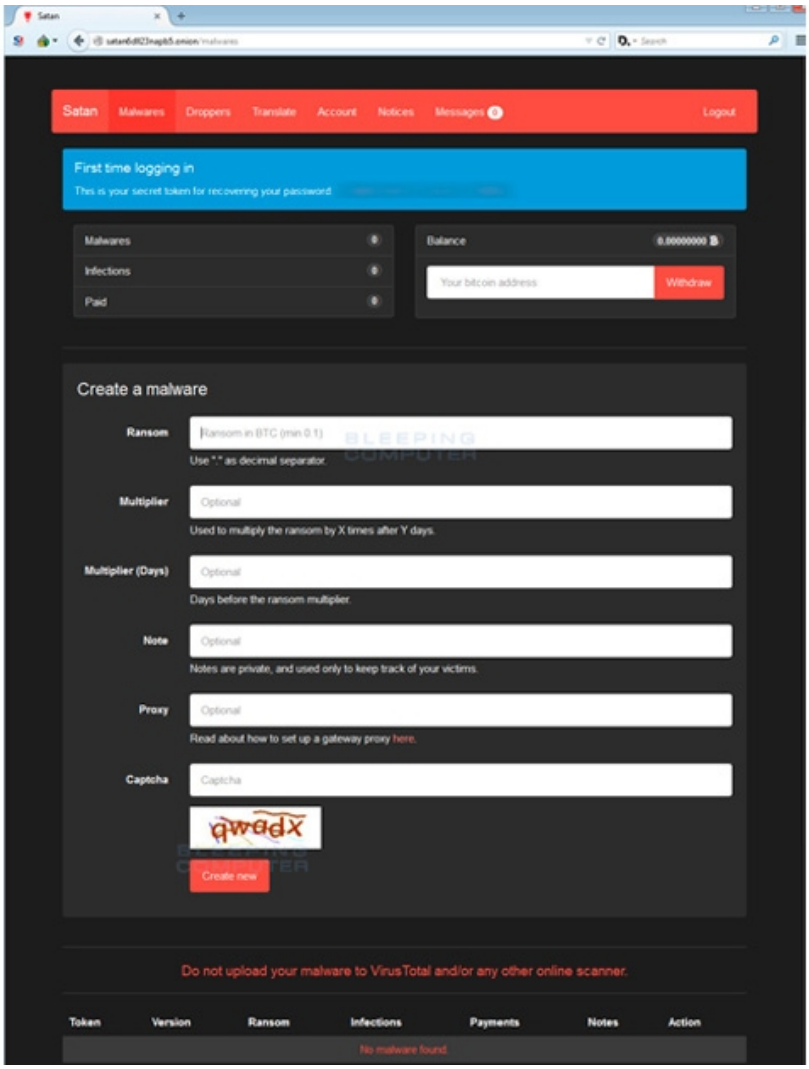
[Torna al capitolo] Figura 29 – Ecco Popcorn!



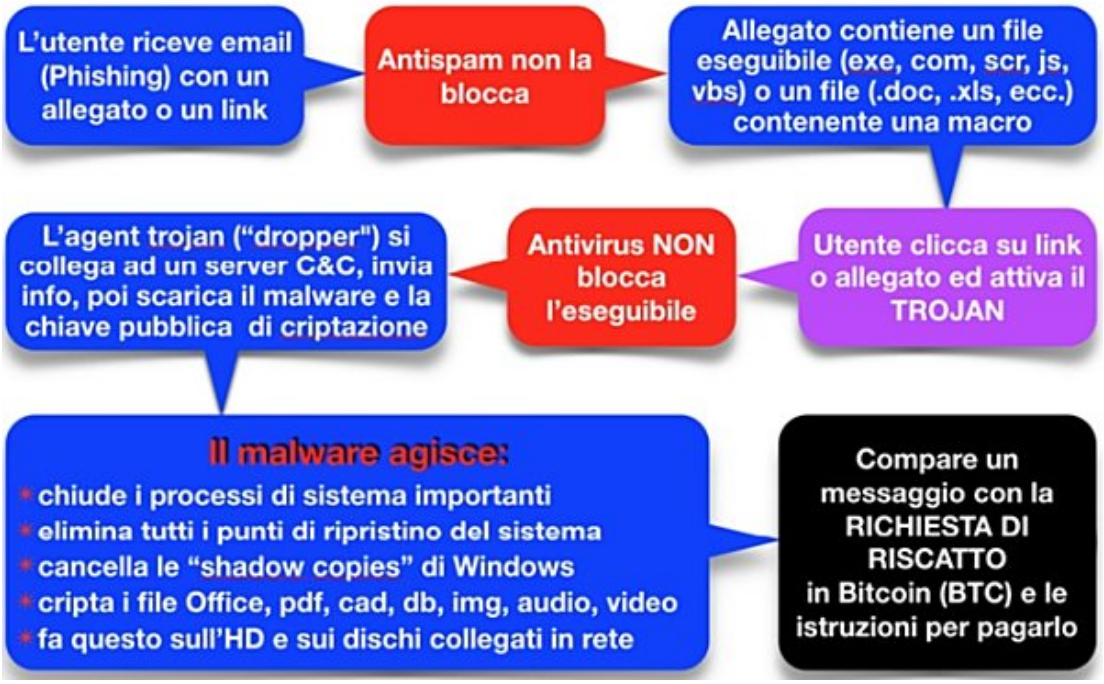
[Torna al capitolo] Figura 30 – Ecco Bad Rabbit!



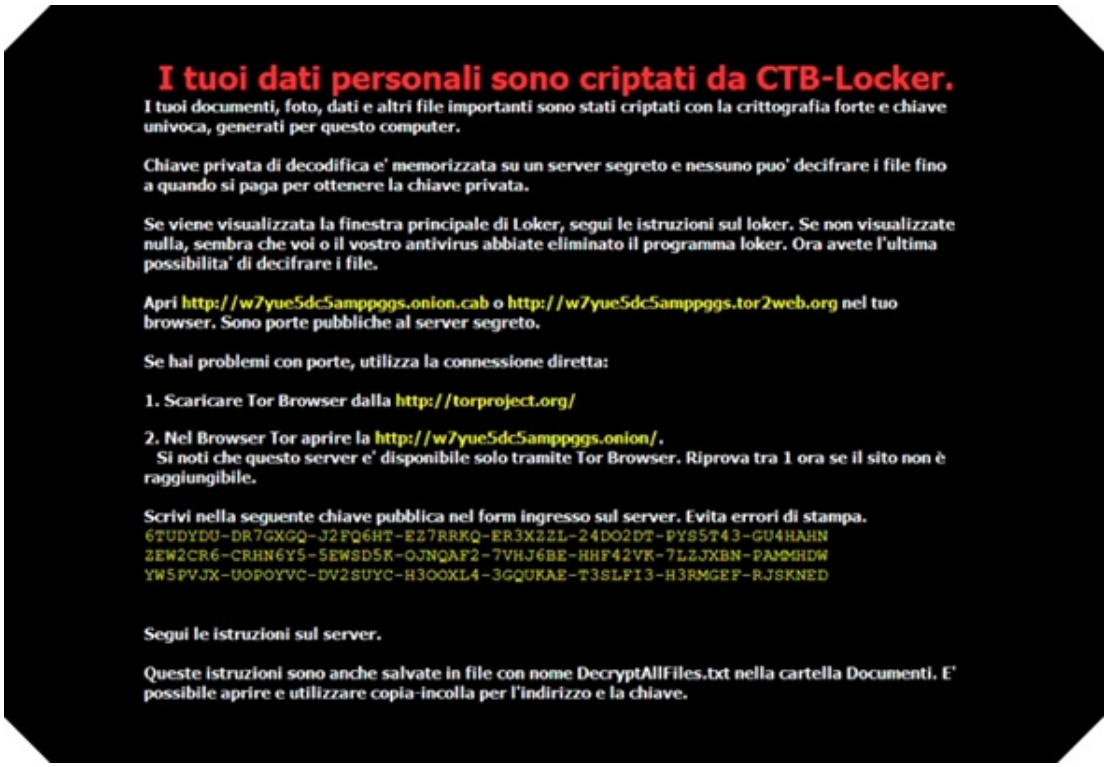
[Torna al capitolo] Figura 31 – La consolle di configurazione di Satan



[Torna al capitolo] Figura 32 – Modalità di attacco di un ransonware

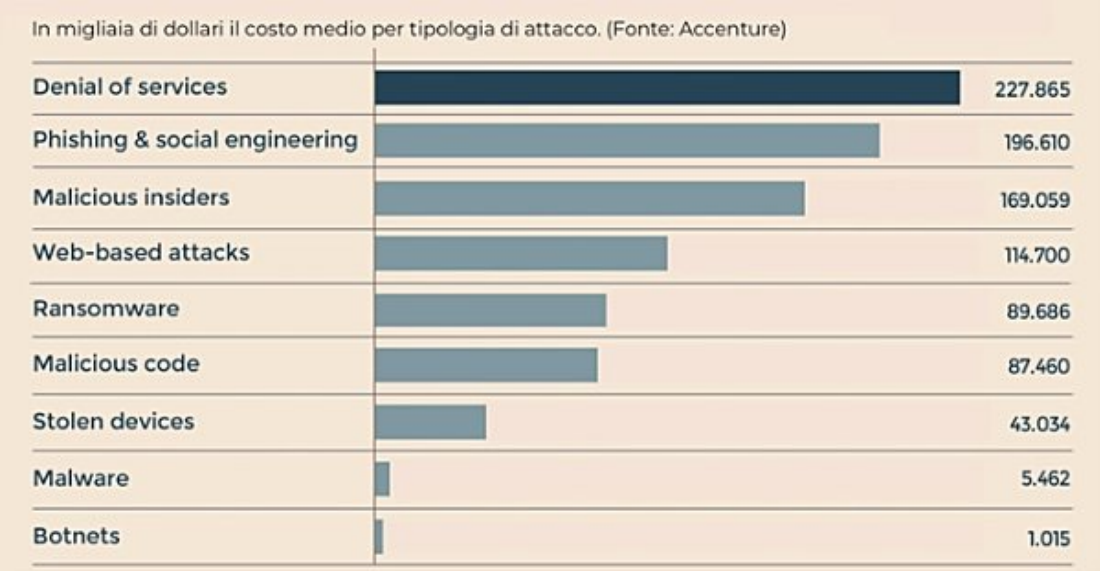


[Torna al capitolo] Figura 33 – Esempio di una richiesta di riscatto

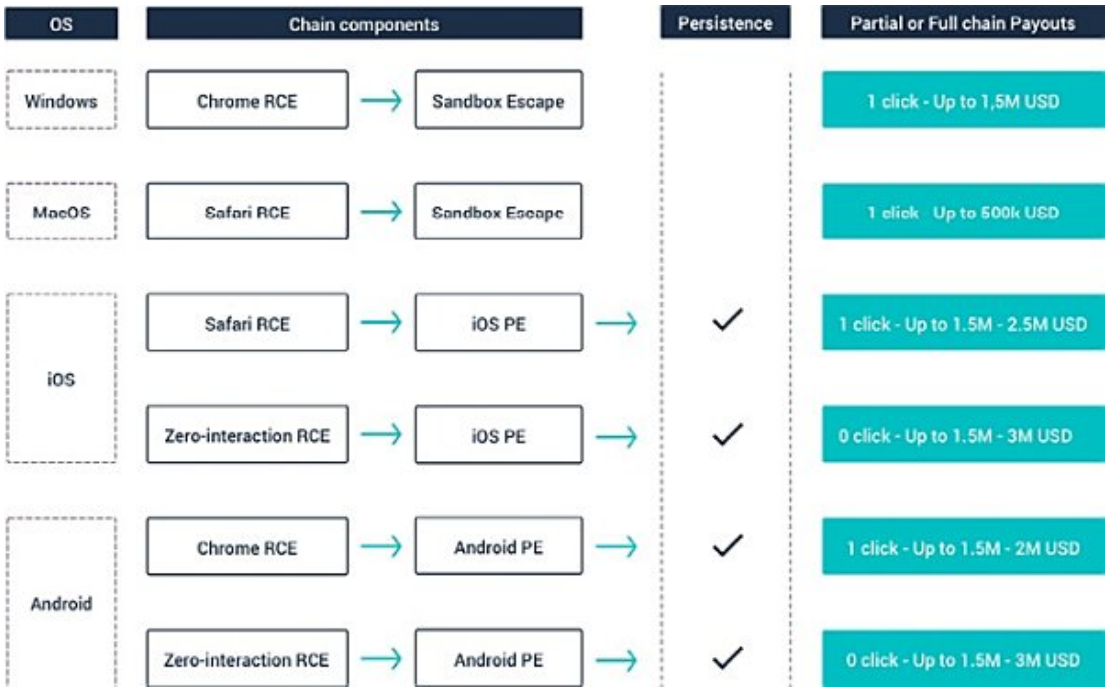


[Torna al capitolo] Figura 34 – La ricerca di un decryptor

[Torna al capitolo] Figura 35 – Quanto costano gli attacchi informatici (Fonte: Ponenon)

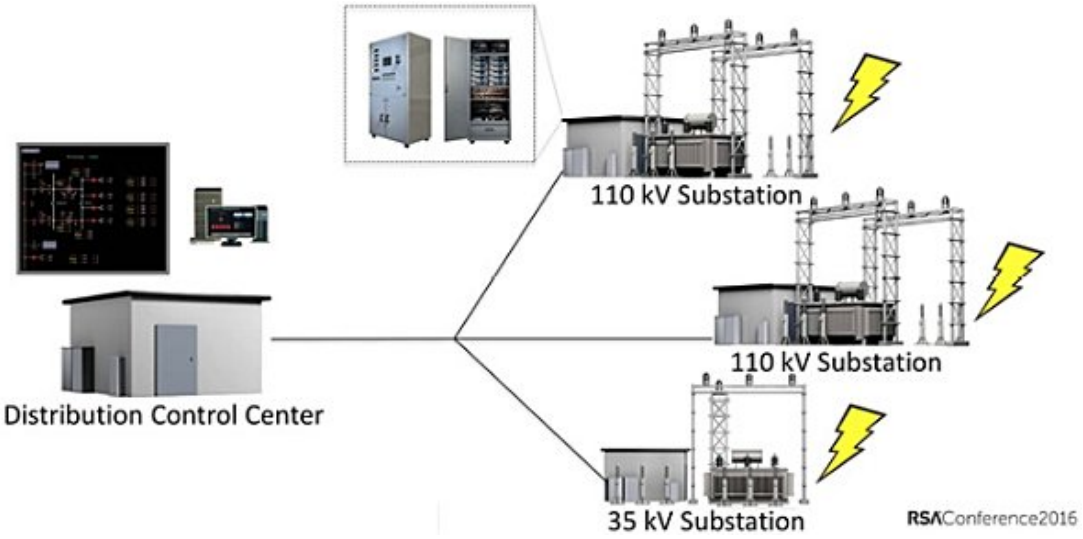


[Torna al capitolo] Figura 36 – Il “Bug Bounty Program” di Crowdfense (aprile 2018)



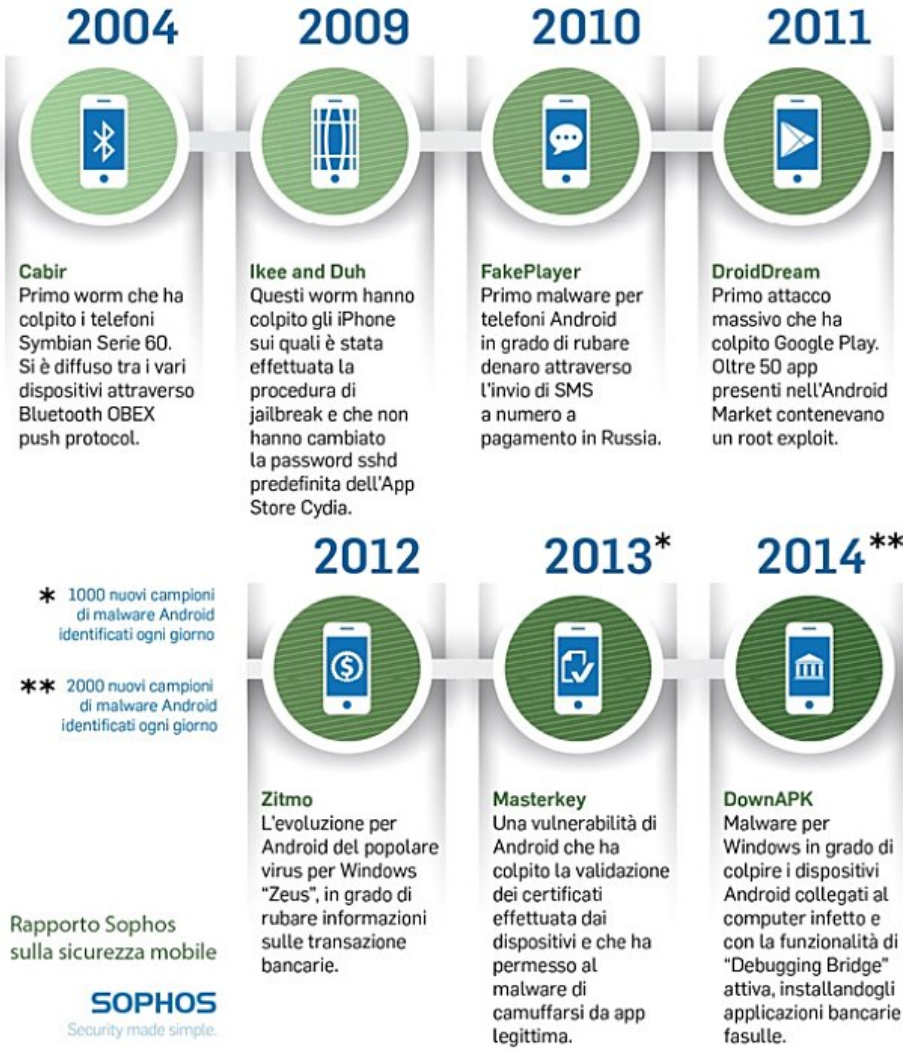
[Torna al capitolo] Figura 37 – Il presidente iraniano di allora, Mahmud Ahmadinejad, all'interno della centrale nucleare di Natanz

[Torna al capitolo] Figura 38 – L'attacco all' Ukrainian Kyivoblenergo

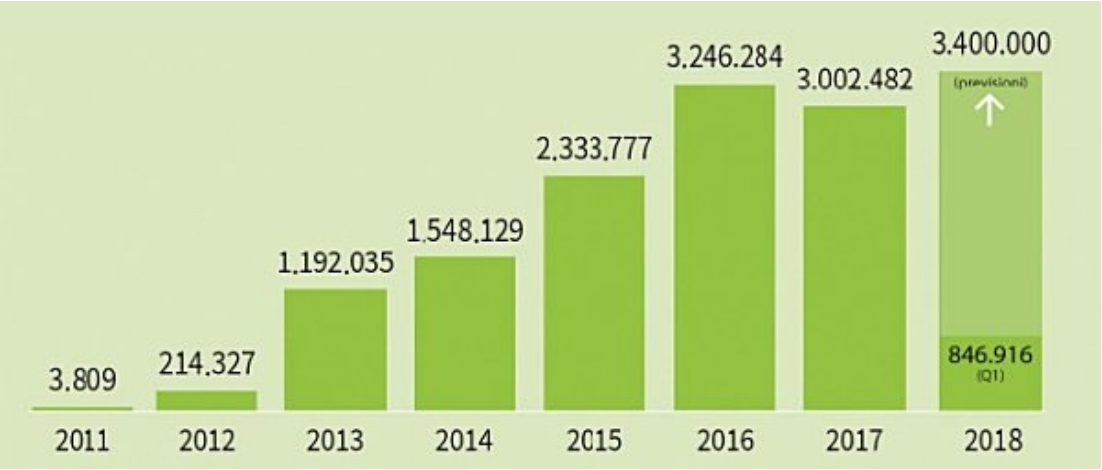


[Torna al capitolo] Figura 39 – Traffico Internet mobile/fisso nel mondo dal 2009 al 2016

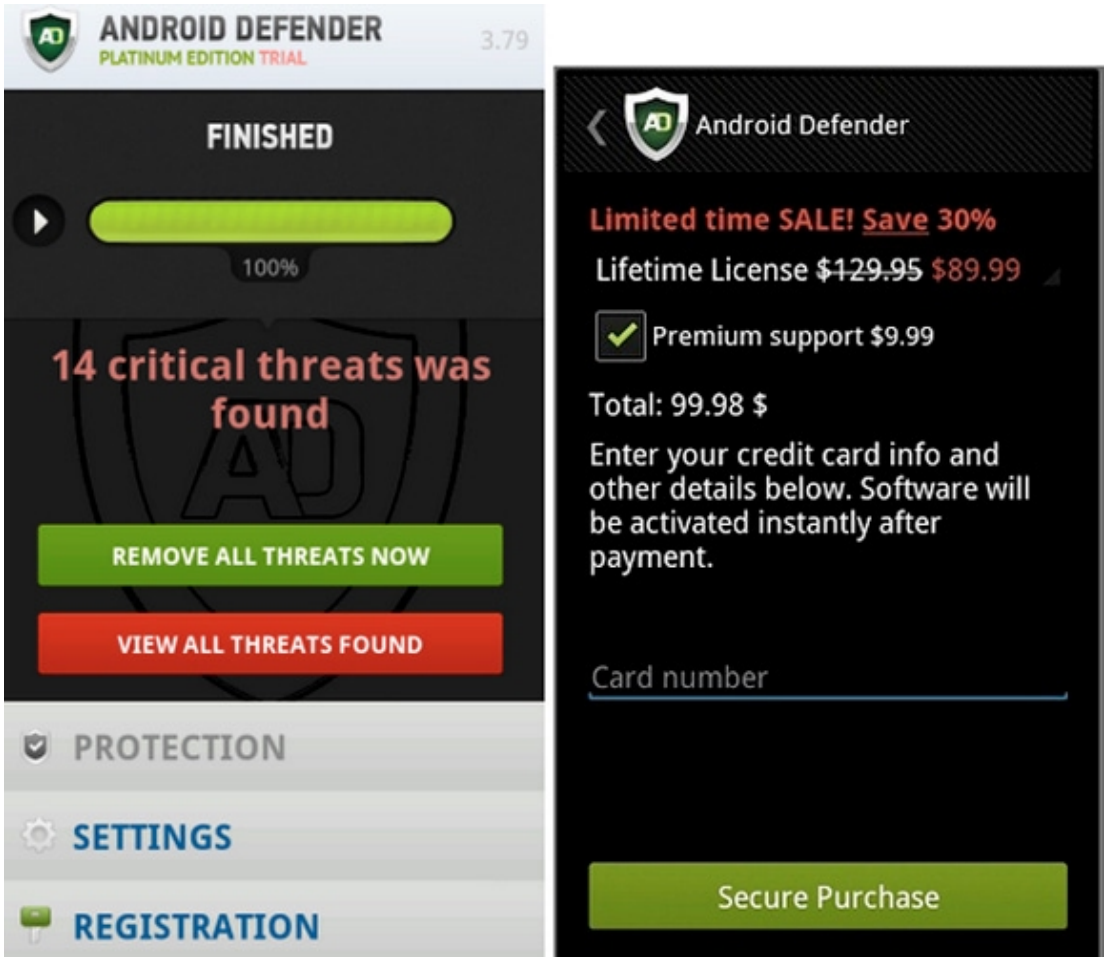
[Torna al capitolo] Figura 40 – Principali vettori di malware nel mobile (fonte: Rapporto Sophos sulla sicurezza mobile)



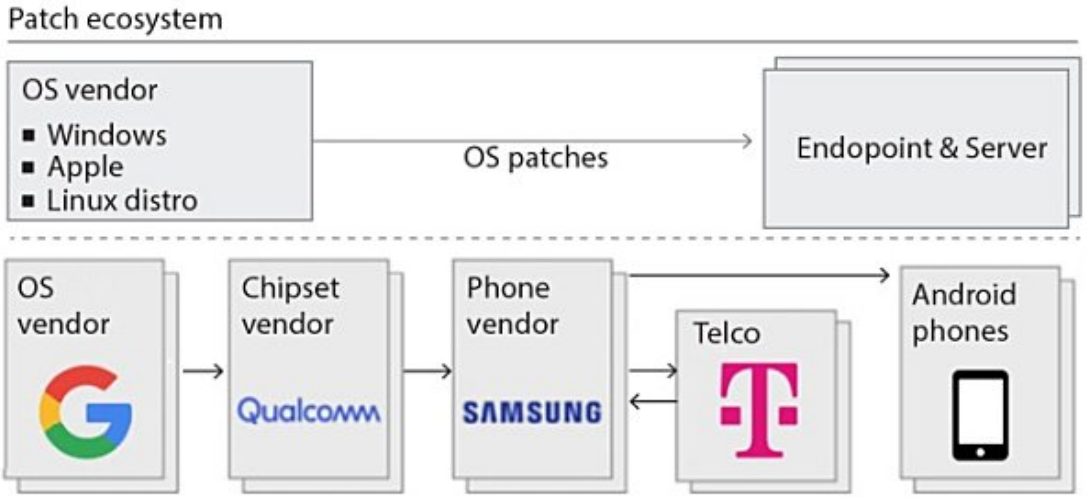
[Torna al capitolo] Figura 41 – Nuovi malware per Android ogni anno (fonte: GDATA Security Labs)



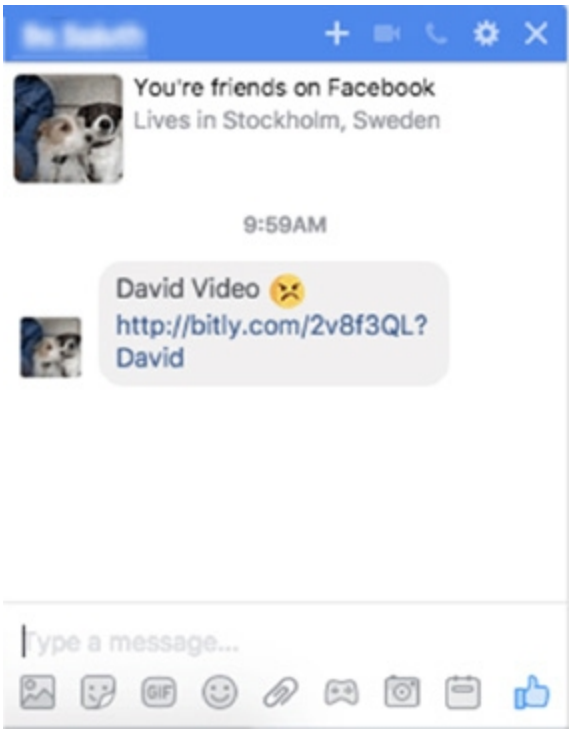
[Torna al capitolo] Figura 42 – L'app Android Defender



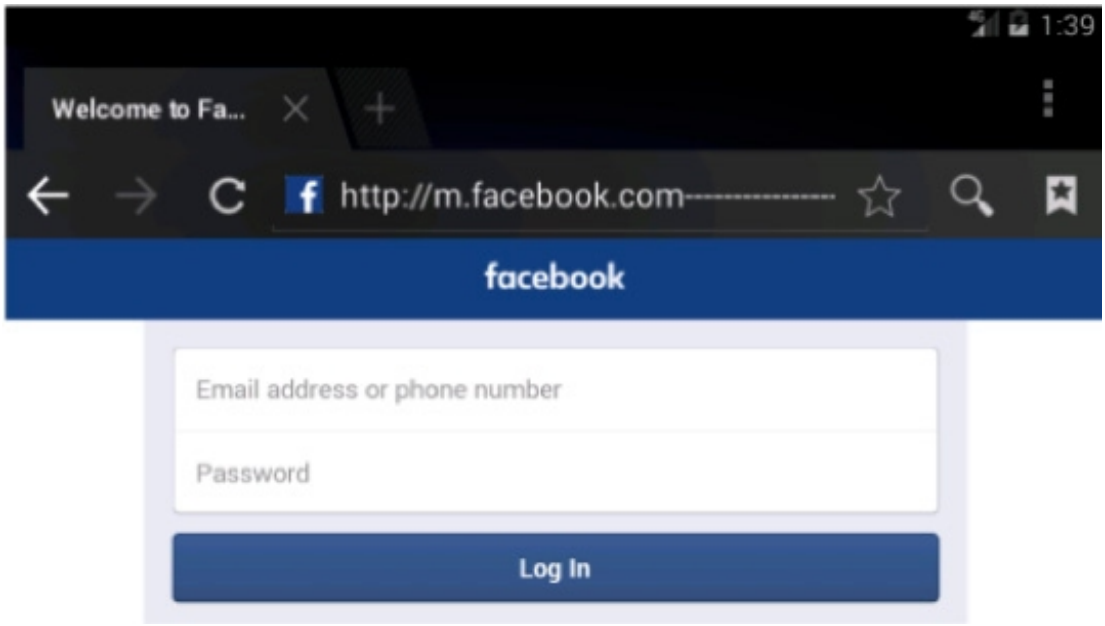
[Torna al capitolo] Figura 43 – L'aggiornamento del sistema operativo di uno smartphone Android



[Torna al capitolo] Figura 44 – Phishing su Messenger



[Torna al capitolo] Figura 45 – Schermata di accesso al sito “fake” di Facebook



[Torna al capitolo] Figura 46 – Attenzione ai buoni sconti su WhatsApp!

[Torna al capitolo] Figura 47 – Ahmed Mansoor e l'SMS da lui ricevuto nell'agosto 2016

Ahmed Mansoor
iPhone 6 iOS 9.3.3
(Agosto 2016)
"New secrets about torture of Emirates in state prisons"

[Torna al capitolo] Figura 48 – Classifica della privacy dei messaggi (Fonte: Amnesty International, “For your eyes only”)

	Servizi di Instant messaging	Risposta alla richiesta di informazioni	Punteggio su 100
1	Facebook Messenger, WhatsApp	Sì	73
2	Apple iMessage, FaceTime	Sì	67
3	Telegram Messenger	Sì	67
4	Google Allo, Duo, Hangouts	No	53
5	Line	Sì	47
6	Viber	Sì	47
7	KakaoTalk	Sì	40
8	Microsoft Skype	Sì	40
9	Snapchat	Sì	26
10	Blackberry Messenger	No	20
11	Tencent QQ, WeChat	No	0

[Torna al capitolo] Figura 49 – Caratteristiche di sicurezza dei servizi di Instant messaging

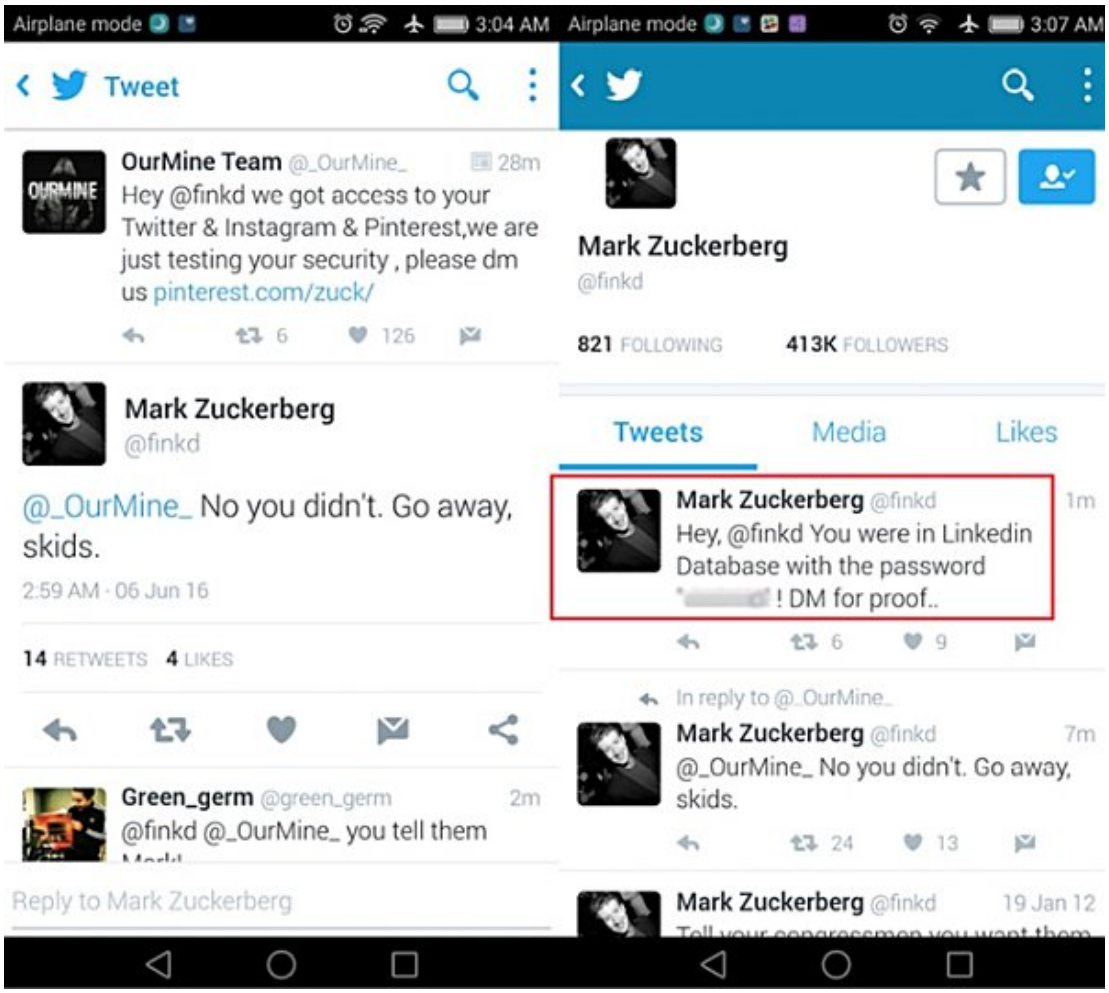
	Crittografia end-to-end	Crittografia: provider non può accedere	È verificata identità interlocutore?	Sicurezza in caso di furto chiavi	Il codice è accessibile per analisi?	C'è stata un'audit indipendente?
BBM (BlackBerry)	✅	⛔	⛔	⛔	⛔	⛔
Facebook Messenger	✅	⛔	⛔	⛔	⛔	✅
iMessage (Apple)	✅	✅	⛔	✅	⛔	✅
Signal (Open Whisper)	✅	✅	✅	✅	✅	✅
Skype (Microsoft)	✅	⛔	⛔	⛔	⛔	⛔
SnapChat	✅	⛔	⛔	⛔	⛔	✅
Telegram	✅	⛔	⛔	⛔	✅	✅
Viber	✅	⛔	⛔	⛔	⛔	✅
WhatsApp	✅	✅	✅	✅	⛔	✅

[Torna al capitolo] Figura 50 — Pineapple Nano

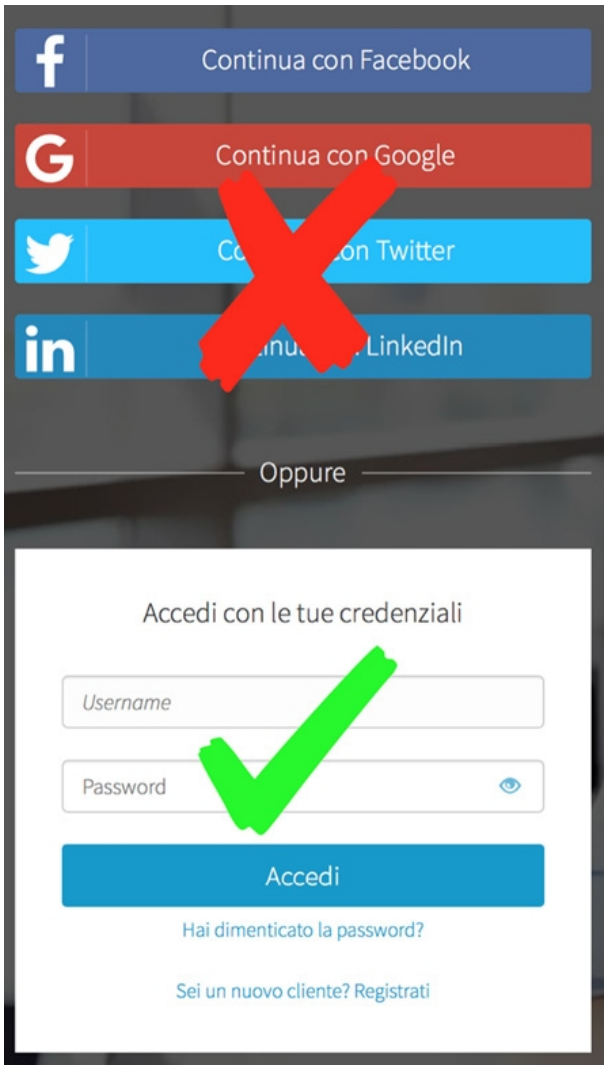
[Torna al capitolo] Figura 51 – Come Pineapple inganna i nostri dispositivi nella connessione alla rete Wi-Fi

[Torna al capitolo] Figura 52 – Schema di un attacco

[Torna al capitolo] Figura 53 – OurMine viola il profilo Twitter di Mark Zuckerberg



[Torna al capitolo] Figura 54 – Occhio alle modalità di accesso a un sito: evitiamo il social login



[Torna al capitolo] Figura 55 — Numerodi combinazioni e tempo necessario in un attacco “brute force” per password di 8 o 12 caratteri

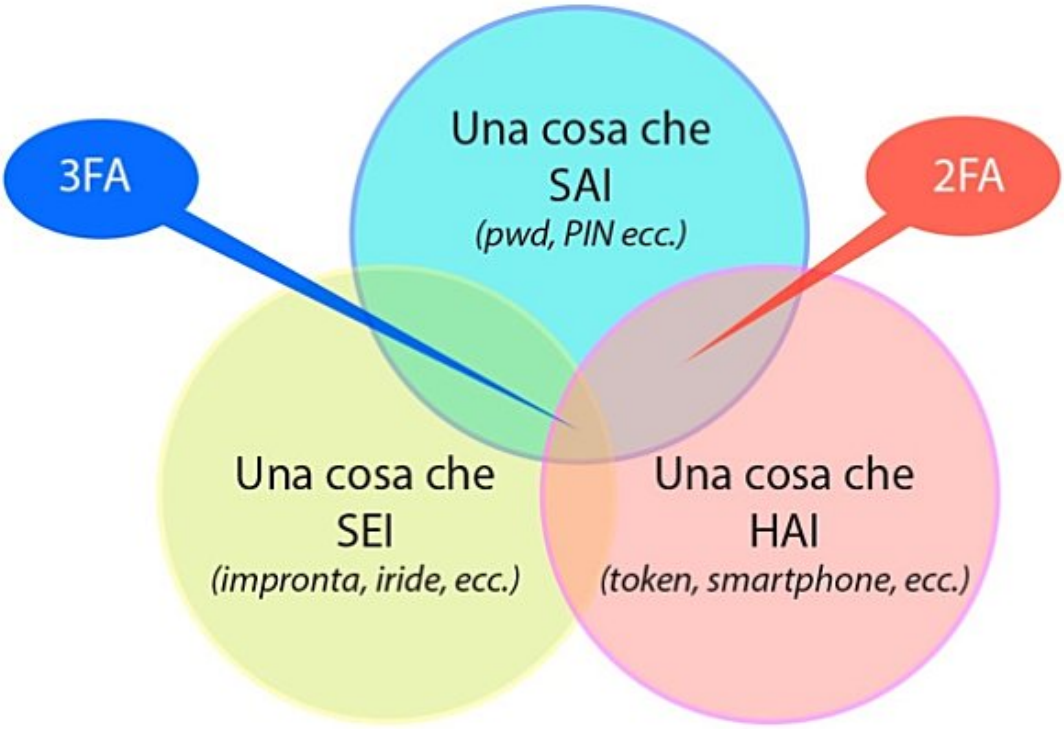
Password di 8 caratteri	Combinazioni	Tempo
Solo numeri (10^8)	1,0E + 08	< 1 sec.
Lettere + numeri (62^8)	2,2E + 14	2,5 giorni
Lett. + num. + car. spec. (95^8)	6,6E + 15	1.576 giorni
Password di 12 caratteri	**Combinazioni**	**Tempo**
Solo numeri (10^{12})	1E + 12	16 minuti
Lettere + numeri (62^{12})	3,2E + 21	1.023 secoli
Lett . + num.+ car. spec. (95^{12})	5,4E + 23	17 milioni anni

[Torna al capitolo] Figura 56 – Esempi di password e valutazione della loro sicurezza

Password	Sicura?	Perché
987654321	NO	sequenza numerica
precipitevolissimevolmente	NO	parola a dizionario
01101952	NO	data di nascita
password	NO	parola a dizionario, per di più ovvia e usatissima!
1q2 w3e4r	NO	sequenza su tastiera (a zig-zag su due righe)
T3L3VI510N3	NO	modificazione della parola TELEVISIONE
rtuoiry55TyUo77#	SÌ	combinazione casuale

[Torna al capitolo] Figura 57 – Un token per generare codici a 6 cifre

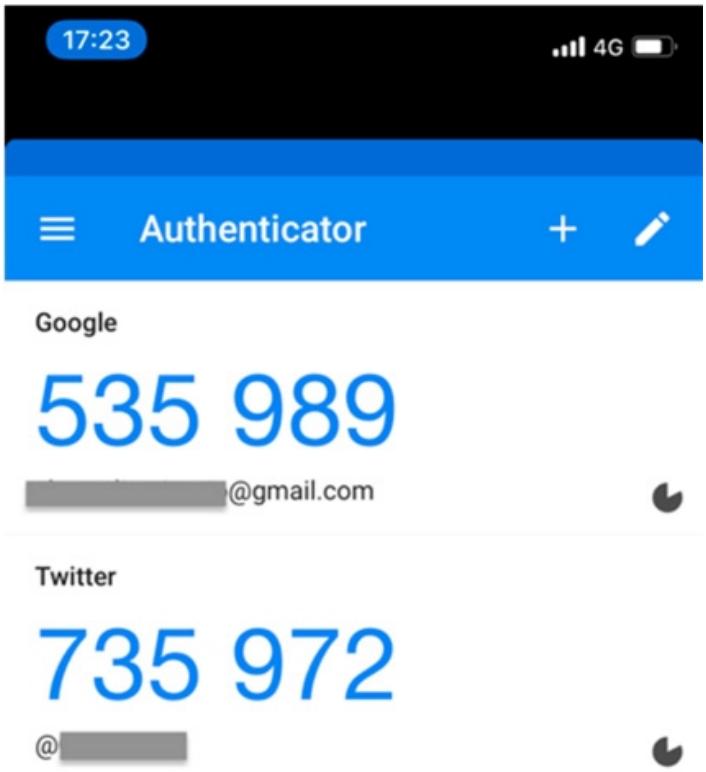
[Torna al capitolo] Figura 58 – L'autentificazione a 2 o 3 fattori



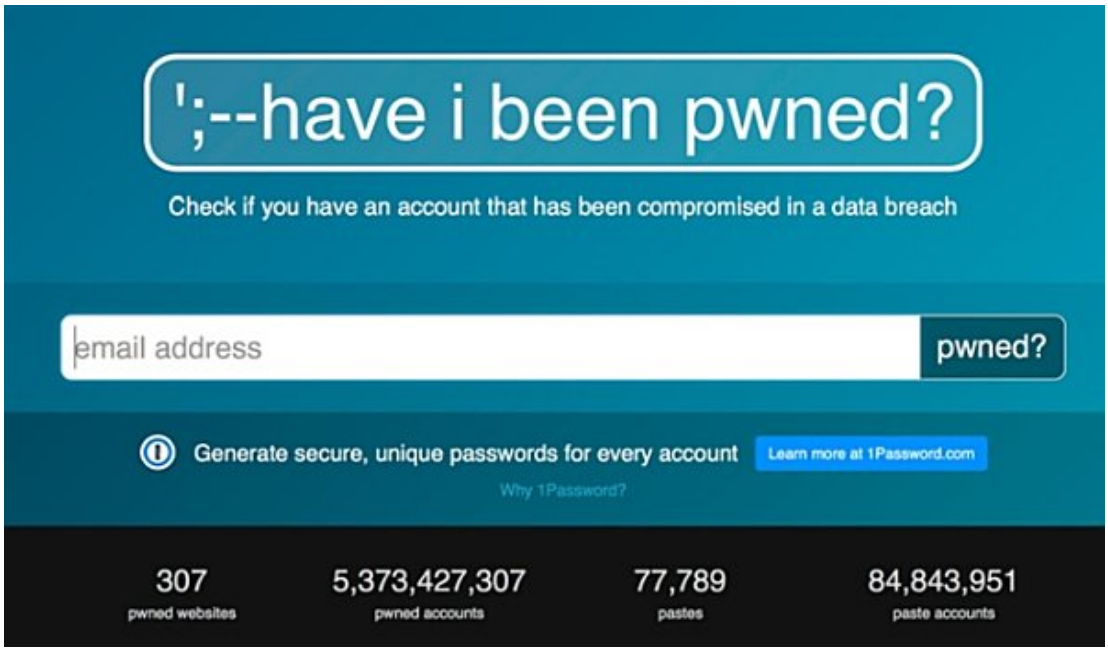
[Torna al capitolo] Figura 59 — Un token hardware

[Torna al capitolo] Figura 60 – Le app che generano il secondo fattore di autenticazione

[Torna al capitolo] Figura 61 – Codice a 6 cifre generato da Google Authentication

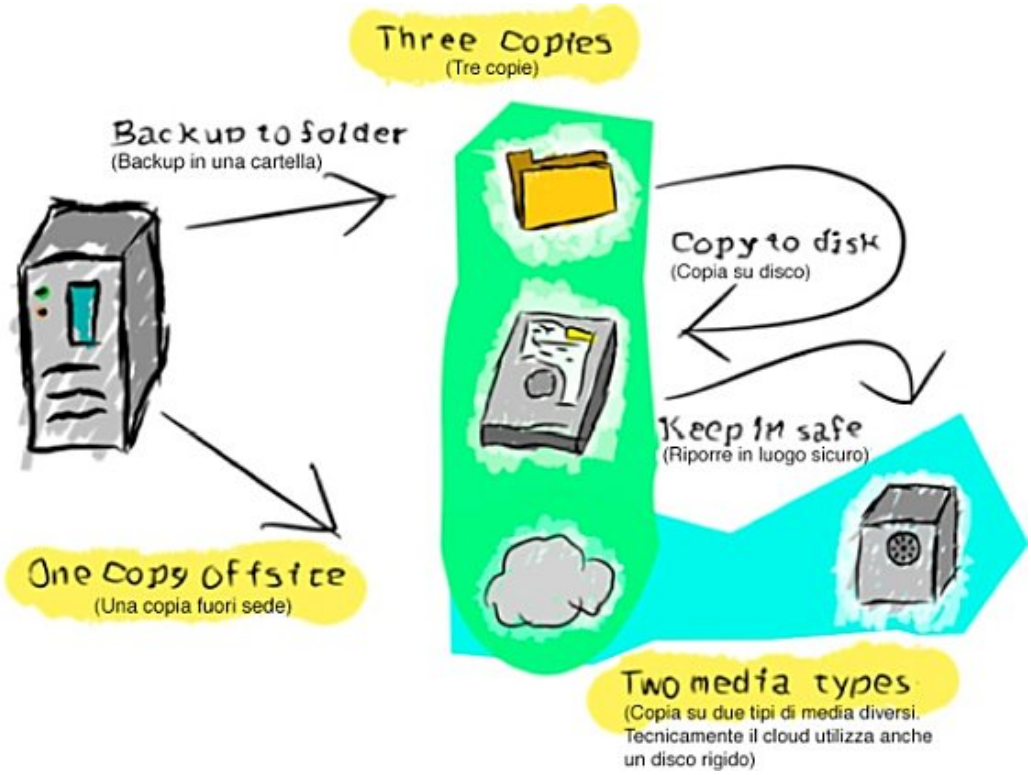


[Torna al capitolo] Figura 62 – Il sito che consente di verificare se il nostro username è stato violato



[Torna al capitolo] Figura 63 – Il logo della giornata mondiale del backup

[Torna al capitolo] Figura 64 – La regola del 3-2-1



[Torna al capitolo] Figura 65 – Tipologie di Penetration Test a seconda del livello di conoscenza del sistema attaccato

Indice dei nomi citati

Su ciascun numero è attivo un link che porta all'occorrenza del termine.

S

T

U

V

W

Z

goWare <e-book> team

goWare è una startup costituita da autori, editor, redattori e sviluppatori che condividono la visione sul futuro delle nuove tecnologie e la passione per l'editoria.
Raccogliere, selezionare e organizzare i contenuti allo scopo di renderli a portata di touch è la sfida quotidiana di goWare come casa editrice digitale.
Operativamente goWare è costituita da due team: goWare <app> team, che si occupa di concepire e sviluppare applicazioni per iPhone e iPad e goWare <e-book> team, specializzato in editoria digitale, creazione di ebook, consulenza e formazione in campo editoriale. Il goWare team è composto da Roberto Avanzi, Elisa Baglioni, Stefano Cipriani, Valeria Filippi, Mirella Francalanci, Patrizia Ghilardi, Mario Mancini, Alice Mazzoni, Alessio Orlando, Lorenzo Puliti, Maria Concetta Ranieri.

Manifesto di goWare

Il contenuto in digitale è un'altra cosa

Pensiamo che i contenuti digitali siano differenti da quelli distribuiti attraverso i media tradizionali, diversi nel formato, nel design, nel pubblico che li fruisce.
Lavoriamo per valorizzare questa diversità, curando nel dettaglio la realizzazione di ebook ed enhanced book pensati per un'esperienza di lettura autenticamente digitale.

"Surpass the print experience"

Non c'è bisogno di tradurlo, le parole del team iBooks della Apple suonano come l'11° comandamento. La chiave è la generosità. Ci sono tanti piccoli-grandi accorgimenti per migliorare la lettura dell'ebook. Per esempio non c'è più il vincolo della foliazione, si può essere generosi con l'interlinea, gli spazi, le paragrafature, i colori: la costipazione è finita, coloriamo le parole e arieggiamo la pagina! È il vero trionfo della volontà sulla necessità.

Abbasso il piombo!

Gli ebook di goWare sono progettati e realizzati per vivere in un ecosistema digitale. Ci ispiriamo a Wikipedia: la lettura digitale ha bisogno di link per farci spaziare da un contesto a un altro. È inoltre sincopata: la cementificazione del testo è finita! Abbasso il piombo, viva il link. La partecipazione distratta non ci spaventa.

Il valore di un ebook non sta solo nel contenuto ma nella relazione

All'interno di un ecosistema digitale, il valore economico di un libro non sta più soltanto nella quantità di copie che il suo editore/produttore riesce a vendere a un prezzo massimizzato, quanto nelle idee e nella relazione che riesce a creare con il proprio pubblico e i media sociali; lavoriamo su questa relazione in modo che diventi il veicolo per costruire il rapporto economico.

Siamo nomadi

Sia i nativi che gli immigrati digitali non sono per niente stanziali, sono nomadi, si spostano continuamente da un dispositivo all'altro e da una piattaforma all'altra. I nostri contenuti sono pensati per spostarsi con loro.

Dillo subito, e con una narrazione possibilmente visuale

Curati, interessanti e veloci da leggere, gli ebook di goWare vanno al sodo e non contemplano solo il testo: la narrazione visuale e quella musicale sono parte integrante della progettazione.

Dove stiamo andando?

«Where we going man? I don't know, but we gotta go» scrive Jack Kerouac in On the road. Il team di goWare ha sempre in mente queste parole da cui ha tratto anche parte del suo nome. Innumerevoli sono le incognite che gravano sul presente e sul futuro dell'editoria

digitale: nessuno sa bene dove approderemo, per ora occorre andare e occorre sperimentare.

Salve, lettore globale

I nostri ebook sono rivolti ai lettori italiani esigenti che pensano globalmente, convinti che siamo tutti parte di un medesimo insieme economico, culturale se non ancora linguistico: il mondo. La rivoluzione digitale significa prima di tutto questo. Tutte le opinioni sono un patrimonio, meglio se differenti, ancor meglio se fuori dal coro.

Detto altrimenti...

... cioè con le parole della poetessa inglese Ruth Padel
Di' addio al potrebbe-esser-stato [...]
vai perché sei vivo,
perché stai morendo o sei, forse, già morto
Vai perché devi.

goWare – Tecnologia

Ti potrebbero interessare anche

GDPR kit di sopravvivenza. Capirlo, applicarlo ed evitare sanzioni sulla privacy e il trattamento dei dati personali di Giorgio Sbaraglia e Francesco Amato

Disruptive innovation: economia e cultura nell'era delle start-up. Come la Internet generation – Jobs, Jeff, Zuckerberg – è diventata disruptive di Fabio Menghini

La Rete tra libertà e controllo. Dagli alchimisti di Nasdaq al caso Snowden di Glauco Benigni

Così il digitale ci cambia la vita di Glauco Benigni

Scopri gli altri ebook di goWare