Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

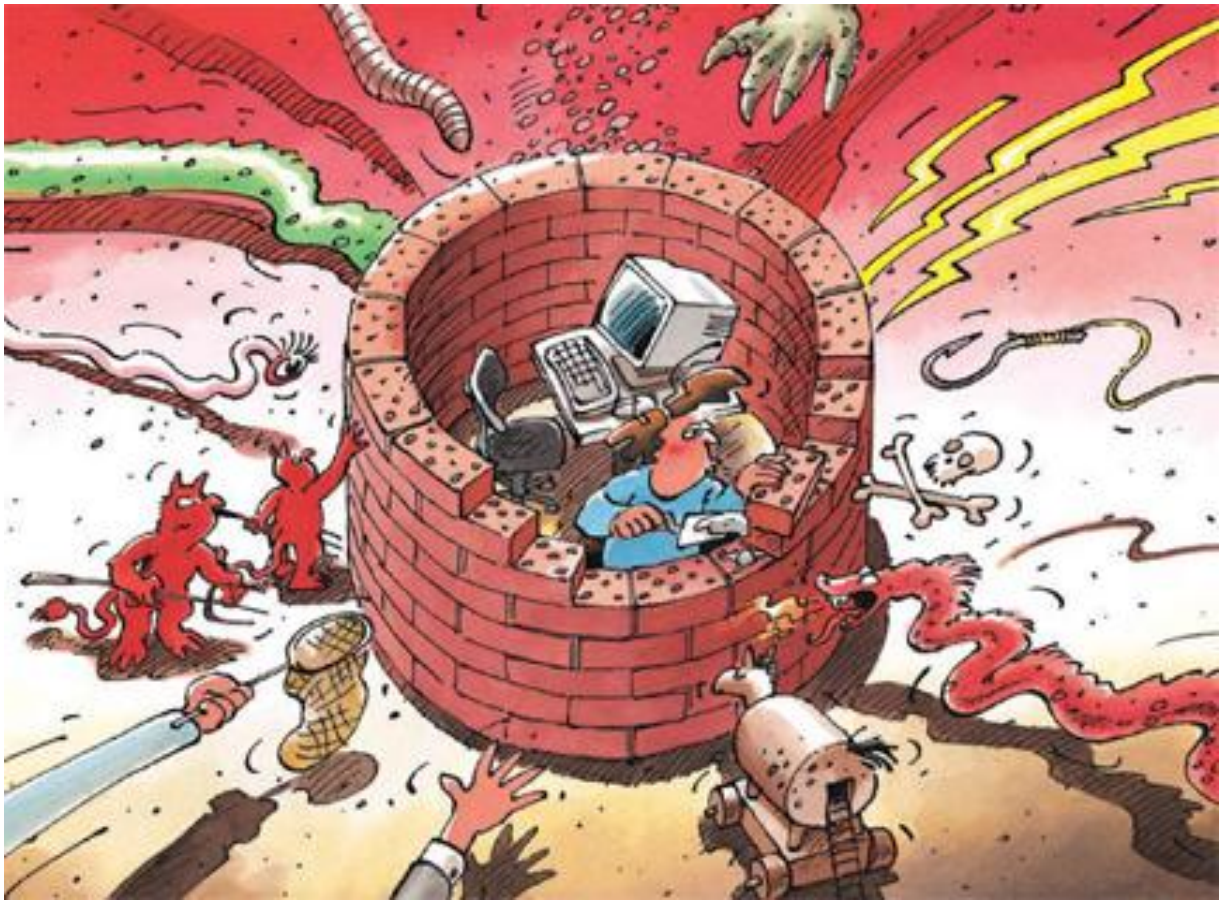
Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
www.melani.admin.ch

Sicurezza delle informazioni

La situazione in Svizzera e a livello internazionale

Rapporto semestrale 2014/II (luglio – dicembre)



Indice

1 Argomenti principali dell'edizione 2014/II

- **Decimo anniversario di MELANI**

  Il 1º ottobre 2014 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha celebrato il decimo anniversario della sua istituzione. Sono stati dieci anni caratterizzati da un enorme sviluppo nelle tecnologie dell'informazione e della comunicazione (TIC). Il numero crescente di piattaforme, servizi e utenti di Internet ha inciso anche sulle strutture criminali. In questo intervallo di tempo si è sviluppato un vero e proprio mercato cibernetico clandestino in cui ci si può procurare tutto quanto serve a sferrare un attacco. Tuttavia anche alcuni Stati hanno potenziato e affinato i propri metodi di spionaggio e sorveglianza. Nel capitolo 3.1 vengono illustrati fatti e riflessioni in merito agli sviluppi di Internet negli ultimi dieci anni.

  ► Situazione attuale in Svizzera: capitolo 3.1

- **Ancora falle di sicurezza nella crittografia**

  Dopo Heartbleed, il protocollo *SSL* è stato nuovamente colpito da una grave falla di sicurezza. A differenza di Heartbleed, la falla denominata Poodle non è un errore di programmazione, bensì di concezione. L'unico modo di porvi rimedio consiste nel disattivare lo standard di crittografia ormai obsoleto. Sono state inoltre individuate anche numerose altre falle, in parte serie. Nella banca dati gestita dalla ditta MITRE, che censisce tutte le vulnerabilità di programmi pubblicamente note, nel 2014 è stato registrato un totale senza precedenti di 7945 falle di sicurezza in tutto il mondo. Si pone pertanto sempre più urgentemente la questione dei processi che regolano la gestione delle falle di sicurezza riscontrate.

  ► Situazione attuale a livello internazionale: capitolo 4.9, capitolo 4.10, capitolo 4.11
  ► Tendenze / Prospettive: capitolo 5.5

- **Sistemi mal protetti – un pericolo non solo per gli operatori**

  Webcam aperte, reti wireless mal protette e *sistemi di gestione di contenuti (Content Management Systems, CMS)* obsoleti sono bersagli privilegiati. A prima vista sembrerebbe che gli attacchi causino un danno solo all'operatore, invece spesso hanno altre ripercussioni. Siti Web compromessi possono infatti essere usati indebitamente a scopi di *phishing* o per diffondere *malware* e account di posta elettronica compromessi per l'invio di spam. Nel frattempo la Svizzera si colloca al terzo posto su scala mondiale per invii di spam in rapporto alla sua popolazione.

  ► Situazione attuale in Svizzera: capitolo 3.2, capitolo 3.4, capitolo 3.5

- **Spionaggio – sul posto di lavoro, in viaggio e nelle comunicazioni**

  Sussiste un interesse permanente, e pertanto una pressione costante, per dati sensibili. Gli esempi illustrati nel presente rapporto dimostrano che siamo esposti sempre e dovunque a tentativi di spionaggio: sul posto di lavoro, nei viaggi di lavoro o durante una chiamata con il cellulare.

  ► Situazione attuale a livello internazionale: capitolo 4.5, capitolo 4.6, capitolo 4.10

- **L'interconnessione totale è intelligente e sicura?**

  Nel frattempo non è solo il telefono ad essere diventato intelligente, ma anche automobili (smart car / smart drive), spazi abitativi (smart home) o addirittura interi edifici (smart building) e non da ultimo impianti industriali (smart factory / smart manufacturing) sono in grado di rilevare, ottenere, elaborare, inviare dati e derivarne comandi per eseguire azioni fisiche. I rischi connessi alla interconnessione totale sono descritti nel capitolo 5.2.

  ► Tendenze / Prospettive: capitolo 5.2

2 Introduzione

Il ventesimo rapporto semestrale (luglio – dicembre 2014) della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI spiega le principali tendenze nel campo dei rischi e dei pericoli connessi alle tecnologie dell'informazione e della comunicazione (TIC). Esso fornisce una panoramica degli eventi che si sono verificati in Svizzera e all'estero, illustra i principali sviluppi in ambito di prevenzione e sintetizza le principalli attività degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono contenute in un **glossario** (**capitolo 6**) alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate a colori.

I temi scelti del presente rapporto semestrale sono brevemente riassunti nel **capitolo 1**.

I **capitoli 3 e 4** affrontano le tematiche legate ai malfunzionamenti e ai crash, agli attacchi, alla criminalità e al terrorismo che interessano le infrastrutture TIC. I principali eventi che si sono verficati nella seconda metà del 2014 sono illustrati mediante esempi scelti. In particolare, il capitolo 3 affronta i temi nazionali e il capitolo 4 tratta quelli internazionali.

Il **capitolo 5** presenta le tendenze e una prospettiva delle evoluzioni attese.

Il **capitolo 5.6** contiene una selezione di interventi parlamentari con riferimento alle tematiche legate alla sicurezza delle informazioni.

In occasione del decimo anniversario della istituzione della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI una tabella riassuntiva degli eventi più significativi degli ultimi dieci anni che riguardano Internet e la sicurezza delle informazioni è acclusa alla presente edizione del rapporto semestrale.

3 Situazione attuale delle infrastrutture TIC a livello nazionale

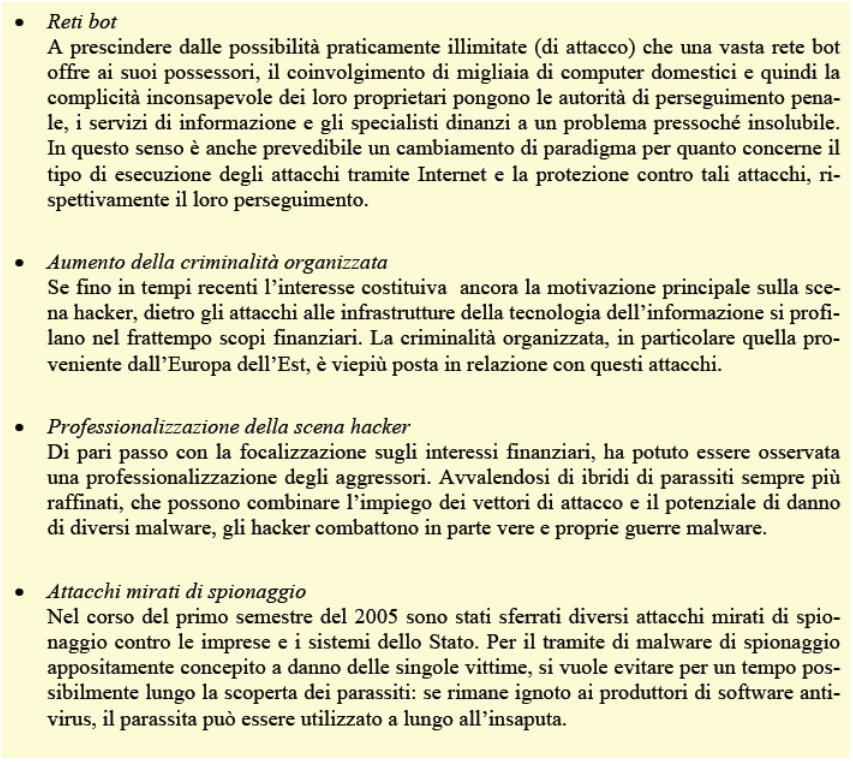
3.1 Decimo anniversario di MELANI – Retrospettiva

Il 1º ottobre 2014 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha celebrato il decimo anniversario della sua istituzione. Sono stati dieci anni caratterizzati da enormi progressi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC). In questo lasso di tempo sono state sviluppate piattaforme, *protocolli* e apparecchi di comunicazione nuovi. Basti pensare allo sviluppo dei *social media* oppure alla rapidissima evoluzione degli *smartphone*. Ricordiamo anche che quando è stata istituita la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI Facebook era ancora agli esordi, essendo stato creato appena otto mesi prima. Il servizio di messaggistica breve Twitter è stato addirittura avviato nel 2006 e il primo iPhone è stato lanciato sul mercato solo l'anno dopo. Inoltre il numero degli utenti di Internet è esploso: da 900 milioni nel 2004 sono passati a ben tre miliardi nel 2014[1].

È ovvio che il progresso tecnologico e sociale favorisce anche i criminali e altri attori malintenzionati che colpiscono traendo profitto dalle nuove opportunità. L'incremento del numero di nuovi utenti inesperti di Internet produce anche nuove vittime. Nuovi servizi e applicazioni hanno creato ulteriori opportunità di individuare e quindi sfruttare falle di sicurezza. Ad esempio l'uso di software standardizzati per sistemi di gestione di contenuti, che spesso non vengono aggiornati regolarmente, ha generato innumerevoli nuove vulnerabilità[2].

[1] http://de.statista.com/statistik/daten/studie/186370/umfrage/anzahl-der-internetnutzer-weltweit-zeitreihe/ (stato: 28 febbraio 2015).

[2] vedi rapporto semestrale attuale, capitolo 3.5



- *Reti bot*
  A prescindere dalle possibilità praticamente illimitate (di attacco) che una vasta rete bot offre ai suoi possessori, il coinvolgimento di migliaia di computer domestici e quindi la complicità inconsapevole dei loro proprietari pongono le autorità di perseguimento penale, i servizi di informazione e gli specialisti dinanzi a un problema pressoché insolubile. In questo senso è anche prevedibile un cambiamento di paradigma per quanto concerne il tipo di esecuzione degli attacchi tramite Internet e la protezione contro tali attacchi, rispettivamente il loro perseguimento.

- *Aumento della criminalità organizzata*
  Se fino in tempi recenti l'interesse costituiva ancora la motivazione principale sulla scena hacker, dietro gli attacchi alle infrastrutture della tecnologia dell'informazione si profilano nel frattempo scopi finanziari. La criminalità organizzata, in particolare quella proveniente dall'Europa dell'Est, è viepiù posta in relazione con questi attacchi.

- *Professionalizzazione della scena hacker*
  Di pari passo con la focalizzazione sugli interessi finanziari, ha potuto essere osservata una professionalizzazione degli aggressori. Avvalendosi di ibridi di parassiti sempre più raffinati, che possono combinare l'impiego dei vettori di attacco e il potenziale di danno di diversi malware, gli hacker combattono in parte vere e proprie guerre malware.

- *Attacchi mirati di spionaggio*
  Nel corso del primo semestre del 2005 sono stati sferrati diversi attacchi mirati di spionaggio contro le imprese e i sistemi dello Stato. Per il tramite di malware di spionaggio appositamente concepito a danno delle singole vittime, si vuole evitare per un tempo possibilmente lungo la scoperta dei parassiti: se rimane ignoto ai produttori di software antivirus, il parassita può essere utilizzato a lungo all'insaputa.

Figura 1: Temi principali della prima edizione del rapporto semestrale MELANI: reti bot, aumento della criminalità, professionalizzazione degli hacker e attacchi mirati di spionaggio.

Tuttavia, dall'analisi del primo rapporto semestrale MELANI del 2005 emerge che i temi sono rimasti in gran parte immutati: già nel 2005 si parlava di attacchi di spionaggio mirati, *phishing*, *DDoS*, *defacements* e *social engineering*. Fin dal primo rapporto semestrale erano noti i rischi e pericoli per gli utenti di telefonia mobile, al pari della questione sempre ancora attuale dell'anonimità in Internet. Tuttavia, mentre gli argomenti fondamentali sono rimasti pressoché immutati, nel corso degli ultimi dieci anni l'attività di hackeraggio si è enormemente professionalizzata e specializzata. Oggi i criminali cibernetici si specializzano in ambiti diversi come la ricerca di vulnerabilità, lo sviluppo di malware o l'invio di e-mail di spam. Dieci anni fa era in corso il passaggio dall'«hackeraggio per diletto» all'«hackeraggio a scopi finanziari» e gli attori del settore erano limitati a pochi criminali. Da allora si è sviluppato un vero e proprio mercato clandestino cibernetico dove ci si può procurare tutto quanto serve per un attacco. Tutttavia, anche alcuni Stati hanno ampiamente potenziato e affinato i loro metodi di spionaggio e sorveglianza.

L'enorme incremento del numero degli attacchi è palese. Diversamente da quanto avveniva nel 2005, gli utenti di Internet non sono più confrontati con eventi isolati, ma con una minaccia costante dei loro dati o mezzi di comunicazione. Servizi come la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI e i suoi svariati partner che operano nel campo della sicurezza di strutture critiche dell'informazione sono chiamati ogni volta ad affrontare nuove sfide. Per raccoglierle devono essere esaminate ed eventualmente rivedute le contromisure. Da un lato, le aziende devono far confluire costantemente nelle proprie strategie di gestione dei rischi le conoscenze acquisite in un contesto in rapida evoluzione e di conseguenza devono adeguare i loro processi. Dall'altro lato, si sono stabilite una certa routine e tranquillità. Se, ad esempio, l'ondata di *phishing* che nel 2005 si era riversata sulla Svizzera aveva destato scalpore e aveva sortito un'ampia eco nei media e gestire un tale evento equivaleva ad addentrarsi in un territorio sconosciuto, difendersi da tali attacchi di *phishing*, che oggi avvengono più volte al giorno, è ormai diventato routine. Anche l'interesse dei media si limita ormai a casi singoli di vittime famose o che hanno registrato perdite clamorose.

Sapevate che negli ultimi dieci anni la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha:

- pubblicato 20 rapporti semestrali
- organizzato 33 workshop per operatori di infrastrutture critiche
- pubblicato 111 newsletter
- inserito 141 operatori di infrastrutture critiche nel sistema d'informazione MELANI
- elaborato1765 informazioni di e per operatori di infrastrutture critiche
- sollecitato per oltre 3000 volte i provider affinché disattivassero siti Internet di *phishing*
- risposto a oltre 9000 richieste della popolazione
- ottenuto dalla popolazione oltre 27000 informazioni riservate mediante il modulo pubblico di notifica.

Per illustrare queste tendenze MELANI ha preparato un poster sotto forma di scheda cronologica, articolato intorno a tre tematiche presentate in parallelo: Internet, le sue minacce e gli interventi di MELANI. Non ha la pretesa di essere esauriente, alla luce del numero di eventi di attualità che hanno costellato il decennio, ma mira a rappresentare questi temi da una prospettiva dinamica e a fissare punti di riferimento rilevanti. È disponibile in allegato a questo rapporto (si vedo il documento accluso).

3.2 Spam – gli Svizzeri sono vittime ma anche autori

Accanto alle solite e-mail di *spam* che vantano gli effetti di qualche medicinale o farmaco per curare la disfunzione erettile e che da ormai oltre un decennio inondano le caselle della posta di utenti Internet, nella seconda metà del 2014 sono state spedite sempre più frequentemente e-mail contenenti *codice nocivo* (malware) in un allegato. Contrariamente agli anni precedenti, MELANI ha rilevato sempre più e-mail che invece di un file eseguibile (in genere con l'estensione *.exe*, *.pif*, *.scr* oppure *.com*) contenevano un documento di testo in *Rich Text Format* (estensione di file *.rtf*) nel quale era integrato il codice nocivo; il destinatario era incoraggiato ad aprire il file infettato cliccando due volte sull'allegato.

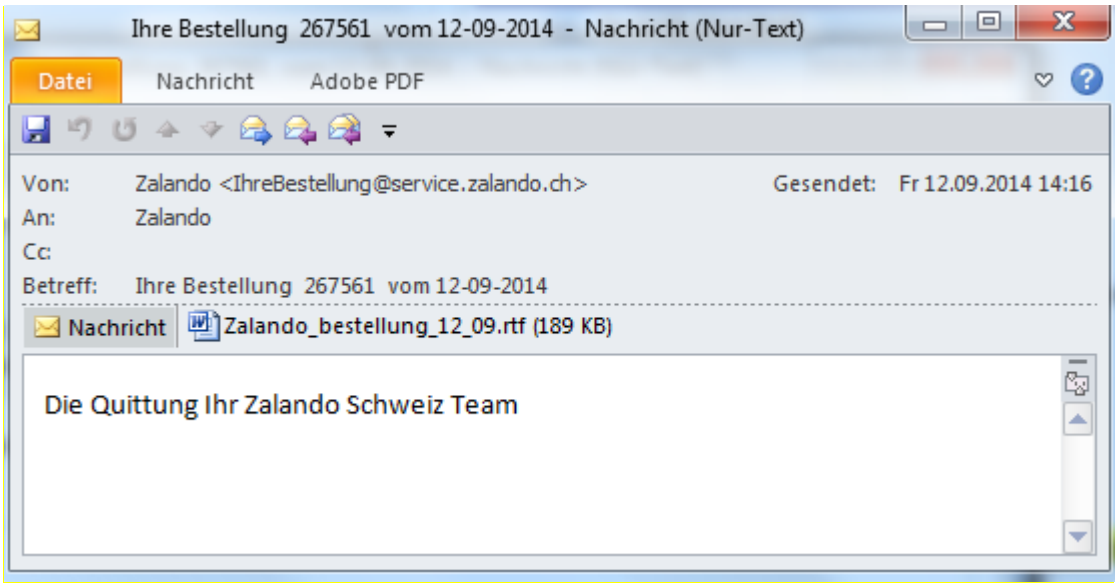


Figura 2: E-mail falsificata con Zalando quale presunto mittente e documento .rtf nocivo in allegato.

Molte di queste campagne di spam erano studiate su misura per la Svizzera e sembravano provenire da noti rivenditori online quali Zalando o Le-Shop. Nonostante gli errori linguistici presenti nel testo, molti utenti sono stati indotti ad aprire il documento, eseguire il codice nocivo infettando il proprio dispositivo con un trojan di e-banking.

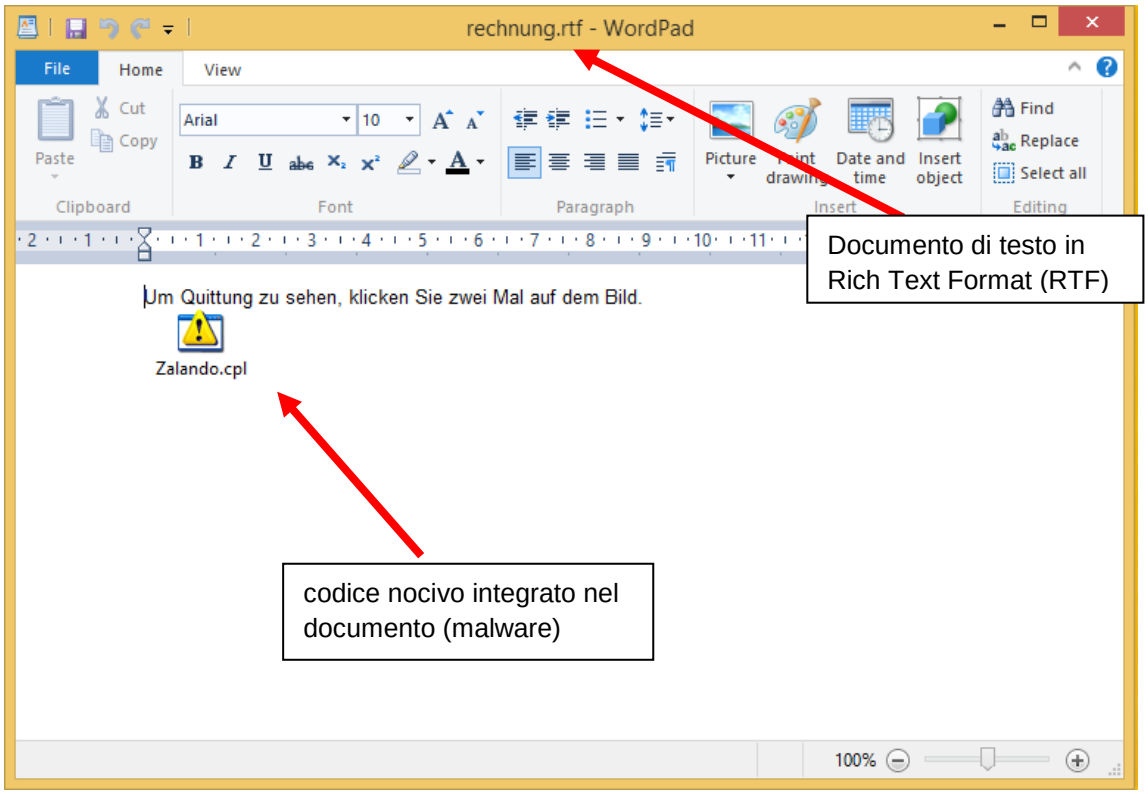


Figura 3: Esempio di un file RTF nocivo

Tuttavia, gli utenti svizzeri non sono soltanto il bersaglio di e-mail di spam, ma sono spesso anche i mittenti di questi invii digitali indesiderati. È quanto emerge da un rapporto pubblicato

nel mese di luglio del 2014 dal produttore di antivirus Sophos[3] nel quale il numero di mail di spam inviate viene messo in relazione con il numero di abitanti di un determinato Paese. La Svizzera è risultata terza in classifica nel secondo trimestre del 2014. MELANI è a conoscenza di diversi casi in cui il mittente delle e-mail di spam era in Svizzera. In uno di questi, oltre 18 000 e-mail di spam sono state inviate da un account di posta elettronica svizzero, colpito dagli hacker. I dati di login erano stati per lo più precedentemente sottratti agli ignari proprietari degli account di posta elettronica mediante un attacco di *phishing.* In altri casi il malware era presente nel computer colpito.

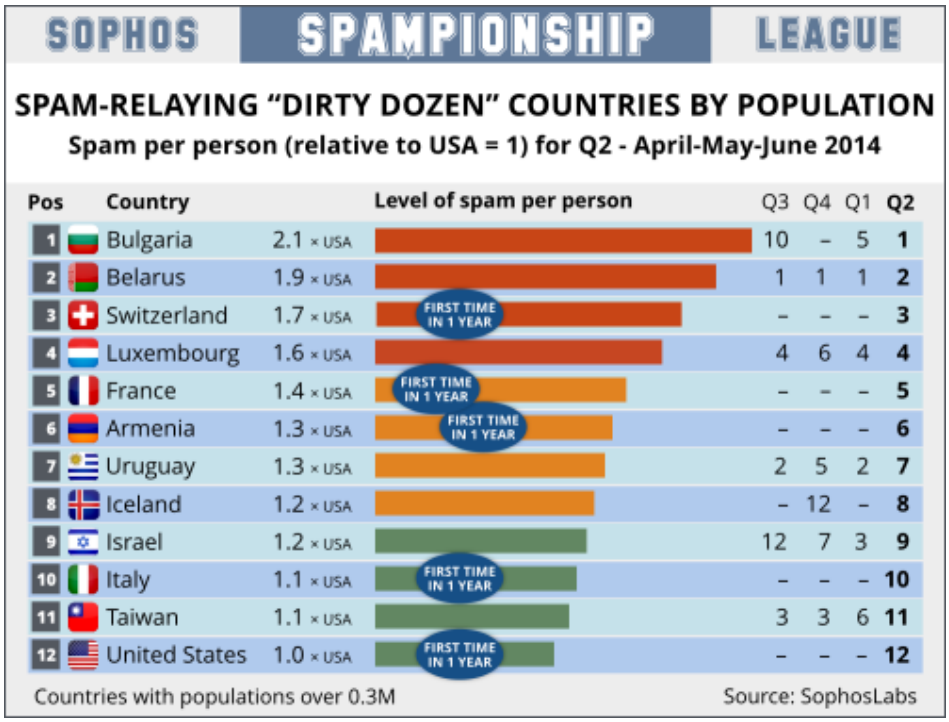


Figura 4: Statistiche in tema di spam (fonte: Sophos)

MELANI raccomanda prudenza nell'uso della posta elettronica e rimanda al suo decalogo comportamentale:
http://www.melani.admin.ch/themen/00166/00172/index.html?lang=it

Per evitare o almeno limitare il plagio di indirizzi e-mail, MELANI raccomanda inoltre ai provider di posta elettronica l'uso di tecnologie adeguate quali ad esempio SPF e DKIM:

Sender Policy Framework (SPF):
http://www.openspf.org/

DomainKeys Identified Mail (DKIM):
http://www.dkim.org/

[3] Sophos: Dirty Dozen Spampionship – which country is spewing the most spam? https://nakedsecurity.sophos.com/2014/07/22/dirty-dozen-spampionship-which-country-is-spewing-the-most-spam/ (stato: 28 febbraio 2015).

3.3 Il settimanale «Weltwoche» – vittima di un attacco cibernetico

Internet sta diventando sempre più un'arena in cui gli utenti reagiscono ad avvenimenti polarizzanti, specie su argomenti di natura religiosa e politica e funge regolarmente da valvola di sfogo. Un esempio attuale è dato dalle reazioni all'attentato contro la rivista satirica Charlie Hebdo: in contrasto con le manifestazioni di solidarietà su scala mondiale «Je suis Charlie» sulle più diverse piattaforme dei social media, in Francia numerosissimi *siti Web* sono stati *deturpati (defacements)* e invasi da propaganda islamista. Questi *defacements* non richiedono un grande know-how e generano perlopiù un grande interesse mediatico, ottenendo in tal modo l'effetto auspicato.

Anche la Svizzera è stata più volte bersaglio di tali attacchi motivati da considerazioni politiche o religiose. Si ricordi, ad esempio, l'attacco *DDoS* ai danni di PostFinance dopo che aveva bloccato il conto del fondatore di Wikileaks Julien Assange nel 2010[4] o il defacement di varie centinaia di siti Web in seguito all'accettazione dell'iniziativa contro la costruzione di minareti nel 2009[5].

La pubblicazione nel settimanale Weltwoche del 28 novembre 2014 di un articolo critico nei confronti del Corano, scritto da Andreas Thiel, ha parimenti avuto ripercussioni su Internet: un attacco *DDoS* ha reso inutilizzabile per lungo tempo il sito Web della rivista[6].

L'incremento nel numero e in parte la mera furia degli attacchi *DDoS* dei mesi scorsi è uno tendenza preoccupante. A Natale, ad esempio, il gruppo di hacker Lizard Squad è stato di fatto in grado di cancellare dalla rete per almeno 24 ore due dei maggiori servizi online nel campo dell'intrattenimento, Sony Playstation Network e Xbox Live. È difficile stimare la portata del danno arrecato. È pertanto raccomandabile per ogni azienda, le cui attività economiche dipendono dall'accessibilità del suo sito Web e/o dall'affidabilità di Internet, di chiarire con i responsabili del loro sito Web e dell'hosting i rischi legati a tali attacchi e di pianificare misure di difesa. Oltre ai provvedimenti tecnici propri di riconoscimento e difesa, rientra tipicamente tra queste anche l'esame dell'idoneità del provider *upstream* e dei suoi obblighi contrattuali in caso di attacco.

3.4 Sistemi poco protetti – 141 webcam aperte in Svizzera

Un numero sempre maggiore di dispositivi è dotato di un'interfaccia *Ethernet* o *WLAN* e può essere collegato a Internet. I più comuni sono le webcam, le memorie di massa, le stampanti, gli scanner e i server di musica o di video. In futuro questa gamma si allargherà ulteriormente (cfr. in merito il capitolo 5.2 «L'interconnessione totale è intelligente e sicura?»). Si dimentica facilmente che questi dispositivi sono previsti e preconfigurati perlopiù per essere utilizzati in una rete interna e quindi spesso non sono protetti o lo sono soltanto con una password standard debole. La protezione è garantita attraverso il *firewall* centrale o il *router*, che impediscono l'accesso diretto ai dispositivi da Internet. Se manca questa protezione e i dispositivi sono collegati direttamente a Internet oppure se sono resi

[4] Rapporto semestrale MELANI 2010/2, capitolo 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=it (stato: 28 febbraio 2015).

[5] Rapporto semestrale MELANI 2009/2, capitolo 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=it (stato: 28 febbraio 2015).

[6] http://www.tagesanzeiger.ch/schweiz/standard/Nach-KoranKritik-Weltwoche-ist-Opfer-einer-CyberAttacke/story/19607439 (stato: 28 febbraio 2015).

intenzionalmente accessibili dalla rete, sono visibili a tutti e, in teoria, se una password è debole o addirittura manca, chiunque può accedervi.

Un caso al riguardo è stato pubblicato sulle prime pagine dei giornali nel mese di novembre del 2014. Numerose testate hanno riportato l'hackeraggio di migliaia di webcam attraverso le quali era possibile richiamare immagini dal vivo da un sito Web russo. Tra queste figuravano anche 141 webcam situate in Svizzera[7]. Oltre alle poco spettacolari viste di garage, ce n'erano di più problematiche come ad esempio le immagini registrate da videocamere di sorveglianza di bambini (*baby cams*). Un'analisi più precisa ha però rivelato che l'hackeraggio era consistito solo nell'utilizzare password standard. Gli utenti avevano dimenticato di modificare le password predefinite.

I dispositivi collegati direttamente a Internet devono essere particolarmente protetti. Questo consiste non solo nel selezionare password che soddisfino i requisiti più attuali, ma anche nell'aggiornare tempestivamente i dispositivi con il software o il *firmware* più recente.

Nella fattispecie quindi non si tratta tanto di hackeraggio quanto piuttosto di negligenza da parte dell'operatore. È una chiara dimostrazione di come anche l'accesso a fotocamere e videocamere possa essere al centro dell'attenzione dei criminali. Ciò è dovuto, tra l'altro, anche al fatto che nel frattempo molti dispositivi sono stati dotati di webcam. Smartphone, tablet, laptop e anche diversi apparecchi televisivi possiedono infatti una fotocamera e una videocamera incorporata. D'altro canto, la sensibilità degli utenti nei confronti delle fotocamere e videocamere incorporate è ancora bassa. Quando ad esempio un dispositivo dotato di fotocamera e videocamera è infettato con malware diventa vulnerabile. A seconda dell'ubicazione di tale dispositivo, ciò può comportare grandi svantaggi per la vittima di un tale attacco, soprattutto se si pensa a tutti i posti in cui si porta uno smartphone.

MELANI raccomanda di coprire le webcam con un nastro adesivo quando non si utilizzano. Attualmente sono in commercio anche apposite protezioni per fotocamere e videocamere con le quali è possibile coprirne temporaneamente la lente.

Figura 5: copertura temporanea della lente della camera in posizione aperta (a sinistra) e chiusa[8]

[7] http://www.tagesanzeiger.ch/digital/internet/141-Schweizer-Webcams-gehackt-und-live-ins-Netz-gestellt/story/20973442 (stato: 28 febbraio 2015).

[8] http://www.soomz.io (stato: 28 febbraio 2015).

3.5 CMS – vulnerabilità e sensibilità insufficiente da parte degli amministratori web

Una gran parte delle pagine di *phishing* e delle *infezioni da drive-by downloads* viene installata su siti Web amministrati con sistemi di gestione dei contenuti *(Content Management Systems, CMS)* non aggiornati. Solo nel 2014 sono state individuate 14 vulnerabilità nel software di CMS Drupal, 9 in Joomla! e addirittura 29 in Wordpress[9]. L'aggiornamento sistematico del software di CMS è pertanto fondamentale per tutti gli amministratori di siti Web, eppure in molti casi viene prestata troppo poca importanza proprio in questo ambito. Molti amministratori di siti Web installano un CMS, trascurando però di effettuarne regolarmente l'aggiornamento. Questi siti Web vulnerabili possono essere rilevati automaticamente con appositi tool e attaccati. In questo modo è relativamente facile per i criminali rintracciare e manipolare un grande numero di siti Web.

In un caso particolarmente grave Google ha addirittura bloccato 11 000 siti Web dall'indice di ricerca, dopo che apparentemente oltre 100 000 installazioni di WordPress erano già state infettate con il malware «Soak Soak» che a sua volta era stato installato sui PC dei visitatori di tali siti Web.

In un altro caso la compromissione è avvenuta senza sfruttare una lacuna di sicurezza. Gli hacker hanno messo gratuitamente a disposizione di amministratori di CMS un *plug-in* oppure un tema (di design) manipolato. Questi però contenevano un malware che consentiva l'accesso ai server web. Decine di migliaia di server sono stati infettati con questo malware chiamato «CryptoPHP», diffuso soprattutto per colpire Drupal, WordPress o Joomla. Dopo che si è verificata l'infezione con CryptoPHP, il codice viene utilizzato per la cosiddetta *Black Hat Search Engine Optimization (BHSEO*) tramite la quale vengono inserite perlopiù parole chiave o pagine manipolate in siti Web allo scopo di influenzare il *ranking* dei motori di ricerca. Accedendo ai server Web gli hacker sono anche in grado di modificare i contenuti di siti Web e di introdurre infezioni da «drive-by download» o siti di *phishing*, oppure semplicemente informazioni errate. Inoltre i server Web infettati con CryptoPHP agiscono come elementi di una *botnet*.

Gli attacchi ai CMS possono essere notevolmente ridotti effettuando il suddetto *patching* (esecuzione tempestiva degli aggiornamenti di sicurezza). Tuttavia, esiste una serie di misure ulteriori per contribuire alla sicurezza dei CMS. Le raccomandazioni sono reperibili sul sito Web di MELANI sotto «Liste di controllo e guide»[10].

3.6 Malware estorsivo in aumento: il nuovo malware Synolocker – segnalati casi anche in Svizzera

La tipologia di *ransomware* muta costantemente. Se fino a pochi anni fa un *ransomware* si limitava a bloccare lo schermo (che era però possibile sbloccare con qualche stratagemma), le versioni attuali hanno un potenziale di dannosità molto maggiore. Dopo «Cryptolocker», che è stato il tema principale trattato nell'ultimo rapporto semestrale, nel periodo in esame è apparso un nuovo malware denominato «Synolocker». Anche in Svizzera sono stati segnalati a MELANI numerosi casi. In caso di infezione vengono crittografati tutti i dati contenuti in un dispositivo di archiviazione collegato alla rete (*Network Attached Storage, NAS*) colpito e viene presentata una richiesta di denaro in cambio della chiave privata

9 http://www.cvedetails.com (stato: 28 febbraio 2015).

10 http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=it

necessaria per la decrittografia. Sul computer della vittima arriva soltanto la chiave pubblica di crittografia asincrona. La decodifica è pressoché impossibile senza la chiave privata corrispondente. In questo caso, non è necessaria un'azione dell'utente per propagare l'infezione che sfrutta in modo mirato una falla di sicurezza nei dispositivi NAS della ditta Synology. Non si tratta neppure di una falla sconosciuta, ma di una lacuna per la quale è disponibile una *patch* dal mese di dicembre del 2013[11]. La stessa vulnerabilità era apparentemente già stata sfruttata nel mese di febbraio del 2014 da un diverso malware. In quella circostanza gli hacker avevano installato programmi di minaggio di bitcoin sui dispositivi NAS dell'utente e generato bitcoin a sua insaputa[12].

Proprio nel caso di router, dispositivi NAS e apparecchiature simili troppo spesso si dimentica di installare gli aggiornamenti (si veda in merito anche il rapporto semestrale 1/2014[13]). Questo è particolarmente grave se le apparecchiature sono collegate direttamente a Internet.

Nel mese di agosto del 2014 è comparso un nuovo trojan di crittografia denominato «CTB-Locker». Esso è caratterizzato dal fatto che comunica in modo crittografato con i suoi server di comando e utilizza il *servizio di anonimizzazione Tor* per cancellare le sue tracce. Questo rende più difficile alla polizia e alle ditte di sicurezza rintracciare e analizzare i server di comando.

Nella seconda metà del 2014 vi sono state però anche buone notizie: i fornitori di servizi di sicurezza TIC FireEye e Fox-IT hanno messo a disposizione un servizio gratuito che consente alle vittime di Cryptolocker di ripristinare i dati crittografati dal malware[14]. L'FBI è intervenuta contro la *botnet* Cryptolocker e ha potuto mettere al sicuro le chiavi private che consentono di decrittografare i dati. Anche nel caso di Synlocker non è escluso che mediante ricerche e indagini le chiavi di crittografia possano essere salvate in un secondo tempo, come nel caso di Cryptolocker. Per questo motivo i dati già crittografati da Synolocker e non più ripristinabili devono essere assolutamente conservati.

I dati archiviati sul computer devono essere copiati regolarmente su supporti dati esterni (*backup*), che devono essere collegati al computer solo durante il processo di backup. I sistemi operativi e tutte le applicazioni installate sui computer (ad es. Adobe Reader, Adobe Flash, Sun Java ecc.) devono essere sistematicamente aggiornati con la funzione di aggiornamento automatico, se è disponibile. Queste raccomandazioni si applicano anche al *firmware* di *router*, *NAS*, server di musica, ecc.

3.7 Swiss Internet Security Alliance – collaborazione per potenziare la sicurezza in rete

Allo scopo di unire le forze e opporre un fronte comune alla criminalità cibernetica, il 12 settembre 2014, fornitori di servizi Internet, banche e altri partner hanno fondato Swiss

---

11 http://www.heise.de/security/meldung/Jetzt-updaten-Aeltere-Synology-NAS-Geraete-anfaellig-fuer-Ransomware-2287427.html (stato: 28 febbraio 2015).

12 http://www.synology-forum.de/showthread.html?50468-Aktive-Hackangriffe-auf-DSM-Versionen-kleiner-4-3-3810-Update-3 (stato: 28 febbraio 2015).

13 Rapporto semestrale MELANI2014/1, capitolo 4.13: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=it (stato: 28 febbraio 2015).

14 https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html (stato: 28 febbraio 2015).

Internet Security Alliance (SISA). I membri di questo partenariato intersettoriale intendono sottolineare il proprio impegno a favore della sicurezza dei loro servizi e clienti. SISA riunisce le competenze di esperti dei settori più diversi e ne promuove lo scambio. Capitalizza il sapere, l'esperienza e la competenza tecnica dei suoi membri tra i quali si annoverano asut, Centralway, Credit Suisse, cyscon Svizzera, l'università di Lucerna, Hostpoint, la Banca Migros, PostFinance, Raiffeisen, Sunrise, Swisscard, Swisscom, SWITCH, UBS, upc cablecom e Viseca. Vantano un'esperienza pluriennale nella gestione della sicurezza su Internet. L'associazione è aperta ad altri interessati.[15]

[15] https://www.swiss-isa.ch (stato: 28 febbraio 2015).

4 Situazione attuale delle infrastrutture TIC a livello internazionale

4.1 Attacco cibernetico alla rete di Sony Pictures Entertainment

Il 24 novembre 2014 è apparso sugli schermi delle postazioni di lavoro della Sony Pictures Entertainment (SPE) in tutto il mondo un messaggio indicante che la rete aziendale era stata attaccata da un gruppo hacker chiamati «Guardians of Peace». Il gruppo asseriva di aver copiato dati interni dalla rete aziendale e minacciava di pubblicarli. Il malware era apparentemente in grado non solo di rubare dati, ma anche di cancellarli. L'intera rete era rimasta inaccessibile per vari giorni. I «Guardians of Peace» sostenevano di essere in possesso di dati per un volume di 100 terabyte, ovvero l'equivalente di 150 000 CD. Affermavano di aver copiato dati personali, come il libro paga dei 6000 collaboratori e dei quadri, e-mail interne, ma anche film non ancora usciti. Effettivamente ai primi di dicembre sono emerse cinque pellicole inedite sulle borse di scambio; in rete circolava anche una versione della sceneggiatura del nuovo film di James Bond «Spectre». Già il 21 novembre 2014 la direzione aziendale di Sony Pictures Entertainment aveva ricevuto un messaggio di ricatto per e-mail accompagnato da una richiesta di denaro. Un altro gruppo denominato «God's Apostels» minacciava Sony Pictures Entertainment di sferrare un «attacco integrato», se non avesse pagato un risarcimento per un non meglio specificato danno arrecato. Il termine di pagamento indicato nella mail era il 24 novembre, ovvero lo stesso giorno dell'attacco[16]. Tuttavia la natura della relazione tra i gruppi «Guardians of Peace» e «God's Apostels» non è mai potuta essere appurata.
Si è rapidamente supposto che l'attacco fosse collegato all'uscita prevista del film «The Interview», una commedia che racconta di un complotto della CIA per assassinare il capo di Stato della Corea del Nord Kim Jong-un e che sarebbe dovuta uscire nei cinema per Natale 2014. Nel mese di luglio del 2014 l'ambasciatore nordcoreano presso le Nazioni Unite ha presentato una denuncia al Segretario generale dell'ONU in merito alla trama del film. Già il 1º dicembre negli ambienti americani si presumeva che l'attacco a spese della Sony fosse opera di un autore nordcoreano[17]. L'8 dicembre è apparsa una comunicazione del gruppo «Guardians of Peace» sul sito Web dell'host provider GitHub che esigeva in termini espliciti di rinunciare a proiettare il film: «Stop immediately showing the movie of terrorism which can break the regional peace and cause the War!».
Il 19 dicembre l'FBI, che era stato chiamato a chiarire il caso, ha pubblicato i primi risultati dell'inchiesta[18]. L'Ufficio federale investigativo ha dichiarato di avere sufficienti elementi per concludere che dietro l'attacco si celasse il Governo della Corea del Nord; ad esempio, il malware che ha cancellato i dati ha elementi in comune con un malware precedentemente sviluppato in Corea del Nord. Sono state evidenziate similitudini nel codice di programmazione, negli algoritmi di crittografia e nei meccanismi di cancellazione senza contare una coincidenza significativa tra le infrastrutture impiegate e precedenti attacchi di probabile origine nordcoreana. Gli indirizzi IP programmati nel malware hanno comunicato con una nota infrastruttura nordcoreana. Sussistono inoltre similitudini con gli attacchi a

[16] http://www.hotforsecurity.com/blog/leaked-emails-reveal-that-hackers-demanded-money-from-sony-pictures-before-attack-10964.html (stato: 28 febbraio 2015).
[17] http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202 (stato: 28 febbraio 2015).
[18] http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (stato: 28 febbraio 2015).

banche sudcoreane e organismi di radiodiffusione avvenuti nel marzo 2013 (DarkSeoul)[19] di cui l'FBI attribuisce ugualmente la paternità alla Corea del Nord.
Il Ministero degli Affari esteri della Corea del Nord ha immediatamente respinto le accuse affermando di essere in grado di dimostrare che l'attacco non fosse collegato al Governo della Corea del Nord e invitando nel contempo gli Stati Uniti ad avviare indagini comuni.
Il 7 gennaio 2015 il direttore dell'FBI James Comey ha reiterato nel corso di una conferenza sulla sicurezza delle TIC a New York, che i servizi segreti statunitensi avevano pressoché la certezza che gli attacchi provenissero dalla Corea del Nord[20], senza tuttavia fornire maggiori dettagli. L'FBI avrebbe scoperto errori gravi commessi dagli hacker. Il gruppo «Guardians of Peace» ha postato vari annunci sul suo sito Facebook e avrebbe utilizzato indirizzi IP nordcoreani per accedere all'account di Facebook[21]. Scoperto l'errore, l'accesso è stato effettuato da computer in altri Paesi per confondere le tracce.
Persistono anche i rumori secondo cui la Corea del Nord non avrebbe agito da sola. Alcuni esperti sospettano la partecipazione di ex-collaboratori di Sony nell'attacco, in particolare si sono fatte congetture intorno al ruolo di un collaboratore licenziato nel maggio 2014[22].

Gli USA hanno rafforzato le sanzioni contro la Corea del Nord a seguito dell'attacco a Sony Pictures Entertainment. Sono state decretate sanzioni contro dieci rappresentanti del Governo di Pyongyang nonché contro tre organizzazioni e imprese.

In risposta ai ripetuti attacchi cibernetici sferrati ad aziende statunitensi e al Governo degli Stati Uniti, gli USA intendono creare una nuova autorità denominata «Cyber Threat Intelligence Integration Center» che avrà il compito di canalizzare e analizzare le informazioni provenienti da fonti diverse.

Questo episodio prova che in ambito cibernetico è molto difficile dimostrare in maniera convincente attacchi che si sospettano essere di matrice statale. Da un lato, contrariamente agli attacchi convenzionali, ci sono più opportunità di occultare l'origine di un attacco e anche di confondere le acque. Dall'altro lato, è limitativo immaginare che un attacco statale sia esclusivamente opera di un funzionario dell'amministrazione pubblica nascosto dietro uno schermo. La distinzione tra tipologie di attacchi statali, siano essi sferrati su incarico di uno Stato o tollerati dalle autorità, è assai sfumata. Nel migliore dei casi è possibile risalire ad hacker che possono essere associati a un determinato Paese. Riuscire a dimostrare la responsabilità dello Stato è però un'altra cosa e le indagini dovrebbero essere effettuate in loco. Purtroppo questo non è generalmente possibile in casi del genere.
Pertanto spesso la prova si evince analizzando le motivazioni degli attacchi. Se non sono di tipo pecuniario, si può rapidamente dedurre che sono opera di professionisti e hanno un'origine statale. Poco dopo il caso della vendita di CD contenenti dati fiscali rubati sono entrati sul mercato anche freelancer che rubano dati per conto proprio e li offrono dietro compenso agli Stati. La struttura del mercato cibernetico clandestino è sicuramente troppo complicata perché questa semplice formula possa essere applicata a tutti i casi. Anche nella fattispecie è ipotizzabile che siano intervenuti più attori, ognuno dei quali ha contribuito a creare questo complesso di casi.

---

19 Rapporto semestrale MELANI 2010/2, capitolo 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=it (stato: 28 febbraio 2015).

20 http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (stato: 28 febbraio 2015).

21 http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (stato: 28 febbraio 2015).

22 http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/ (stato: 28 febbraio 2015).

4.2 Attacchi a impianti industriali

Gli impianti industriali sono sempre più connessi in rete. Da un lato, questo ne facilita il controllo e la manutenzione a distanza, ma dall'altro comporta un rischio maggiore di accessi non autorizzati e manipolazioni. Questi impianti, che interessano gli attori statali con mire strategiche non da ultimo per scopi militari, stanno nel frattempo attirando l'attenzione anche di molti esperti di sicurezza e hacker dilettanti. Di conseguenza, sono un tema del 31º congresso del Chaos Computer Club tenutosi nel mese di dicembre del 2014 riguardava i sistemi di controllo *SCADA* e industriali[23]. Nel frattempo vengono effettuate simulazioni di sistemi di controllo come quelli, ad esempio, degli stabilimenti chimici, che permettono di testare le capacità di hackeraggio. Sono inoltre disponibili *exploit kit* programmati specificamente per rilevare e sfruttare eventuali falle di sicurezza negli impianti industriali.

Un rapporto pubblicato nel mese di dicembre del 2014 dal Bundesamt für Sicherheit in der Informationstechnik (Ufficio federale tedesco per la sicurezza informatica, BSI)[24] riporta un attacco mirato a un'acciaieria che ha causato danni a un altoforno. Gli hacker avrebbero ottenuto l'accesso alla rete aziendale dell'impresa mediante *spear phishing* e sofisticato *social engineering,* infiltrandosi in questo modo nelle reti di produzione. Successivamente guasti di singoli componenti di comando o di interi impianti hanno interferito con la corretta riduzione dell'alimentazione dell'altoforno e l'impianto ha subito ingenti danni. Il BSI ritiene che gli hacker non solo fossero esperti in tema di sicurezza classica delle TIC, ma che avessero anche conoscenze approfondite dei metodi di pilotaggio nell'industria e dei processi produttivi impiegati. Il rapporto del BSI si limita ad attenersi scrupolosamente ai fatti e non si esprime in merito alla matrice degli attacchi.

Le motivazioni degli autori di azioni di mero sabotaggio non sono molteplici: o si tratta di un'impresa concorrente che vuole trarre un vantaggio oppure di un (ex) collaboratore scontento che vuole prendersi una rivincita nei confronti dell'ex datore di lavoro sfruttando le informazioni privilegiate di cui dispone o ancora di soggetti che intendono scoprire o provare fin dove sia possibile arrivare. Al contrario, il sabotaggio della produzione di acciaio della Germania da parte di uno Stato estero a questo punto appare invece poco realista. Il potenziale del sabotaggio cibernetico viene tuttavia viepiù preso in considerazione in strategie militari e scenari di guerra.

Per i criminali, la capacità di sabotaggio si traduce, fra l'altro, nell'opportunità di ricattare il gestore di un impianto[25]. Ciò risulta particolarmente interessante per i malintenzionati laddove un impianto dipende dal suo collegamento ad altri reti e sistemi per il suo funzionamento e in caso di minaccia non può essere isolato rapidamente. È inoltre altrettanto concepibile che una volta introdotto un malware questo si attivi in un determinato momento, indipendentemente dall'operatività della connessione a Internet. In un caso del genere, scollegare il sistema dalla rete non sarebbe sufficiente per scongiurare il pericolo; il malware andrebbe individuato e reso inoffensivo. A seconda del grado di complessità del sistema questo può costituire una sfida, non sapendo bene cosa si stia cercando.

In sede di collegamento in rete di sistemi fisici è importante non tralasciare l'aspetto della sicurezza. I vettori di attacco correnti dei sistemi di controllo sono la rete aziendale, i *supporti di dati rimovibili* e accessi remoti non sufficientemente protetti. Rimedi in questa sede sono la rigorosa segmentazione delle reti (schermare i sistemi di controllo dalla rete aziendale e quando sia necessario procedere allo scambio di dati controllarlo bene), l'uso di supporti di

[23] https://events.ccc.de/congress/2014/wiki/

[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[25] Vedi anche il capitolo 5.3 del presente rapporto semestrale.

dati amovibili dedicati, compreso il loro controllo regolare nonché la messa in sicurezza degli accessi remoti mediante metodi di autenticazione sicuri e il trasferimento cifrato di dati. A questo proposito si veda la lista di controllo MELANI «Misure di protezione dei sistemi industriali di controllo (ICS)»[26].

4.3 Attacchi nel settore dell'energia e del petrolio

Nel mese di agosto del 2014 è stato reso noto che in Norvegia erano state attaccate circa 300 aziende che operano nel settore energetico e petrolifero. Con i loro metodi di *social engineering*, gli aggressori hanno avuto almeno parzialmente successo: le autorità norvegesi preposte alla sicurezza hanno affermato che gli hacker avrebbero identificato per mezzo di ricerche funzioni e personale chiave delle aziende per inviare loro in un secondo tempo e-mail personalizzate, apparentemente legittime, con malware in un allegato. All'apertura dell'allegato si installava automaticamente un *exploit kit* che esplorava il sistema alla ricerca di vulnerabilità e, in caso di successo, caricava un software di spionaggio altamente sofisticato. In questo modo era possibile estorcere segreti commerciali e ottenere dati che consentivano l'accesso ad altri sistemi.

Le imprese che operano nel settore energetico, in particolare nel settore delle forniture di petrolio e gas, già da molto tempo sono sottoposte a una crescente pressione di attacchi cibernetici[27]. Questo può essere legato all'importanza politica, ma soprattutto economica di questo settore. Alcuni attori tentano di avvantaggiarsi rispetto ai concorrenti – siano essi statali o privati – mediante informazioni riservate ottenute attraverso lo spionaggio. Altri cercano in modo mirato di sabotare le attività di aziende del settore energetico per trarre direttamente vantaggio dal calo della loro produzione o dalle oscillazioni dei loro corsi azionari. Infine, deve essere evidenziata la persistente importanza strategica (militare) delle fonti energetiche fossili, particolarmente per l'approvvigionamento di carburante, che coinvolge gli attori statali sia sul piano della difesa che dell'attacco.

4.4 Terminali POS (Points of Sale) nel mirino degli hacker

In passato abbiamo già avuto l'opportunità di tematizzare la problematica degli attacchi a terminali di *punti vendita (POS)*, come nel caso che ha colpito la catena commerciale statunitense Target[28]. Scopo principale di questi attacchi è carpire i dati delle carte di credito, anche se talvolta vengono sottratti contemporaneamente anche altri dati personali. Alla fine del 2014 un caso simile è nuovamente finito sulle prime pagine dei giornali: il 14 settembre 2014 la catena commerciale statunitense Home Depot confermava di essere stata vittima di un furto di dati di circa 56 milioni di carte di credito e debito di clienti, perpetrato tra i mesi di aprile e settembre del 2014. Il comunicato ha confermato e precisato numerose informazioni che erano state pubblicate nelle settimane precedenti da giornali o blog specializzati. Il metodo adottato per l'attacco ricorda molto quello osservato nel caso di Target: un malware di tipo RAM scraper è stato installato nei punti vendita dopo una compromissione iniziale ai danni di un fornitore dell'azienda.

---

[26] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=it (stato: 28 febbraio 2015)

[27] Rapporto semestrale MELANI 2014/1, capitolo 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=it (stato: 28 febbraio 2015).

[28] Rapporto semestrale MELANI 2013/2, capitolo 4.4, Attacchi ai punti vendita dei negozi Target: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=it (stato: 28 febbraio 2015).

Questo modus operandi non è comunque l'unico di cui si avvalgono i criminali per compromettere terminali POS. Già nel mese di luglio del 2014 infatti, l'azienda di sicurezza FireEye aveva richiamato l'attenzione sul malware «BrutPOS» che sfrutta interfacce di gestione remota dei terminali protetti da password deboli. FireEye spiega che per identificare questi sistemi vulnerabili, «BrutPOS» utilizzerebbe una botnet composta di oltre 5500 terminali infetti. A tale scopo, vengono provate password «standard» come per esempio «admin», «client», «password». Dopo essersi infiltrati nel sistema, i criminali cercano di prelevare i dati di carte di credito mediante *RAM scraping*.

Questi esempi evidenziano che i terminali POS continuano a suscitare l'interesse di determinati gruppi criminali. Ingenti mezzi sono investiti per penetrare questi sistemi in quanto sono bersagli che consentono di realizzare cospicui profitti. I dati rubati delle carte di credito sono spesso rivenduti su forum «underground» e infine utilizzati per effettuare acquisti all'insaputa del detentore della carta. Se le imprese americane sono state maggiormente attaccate, è perché sono bersagli comparativamente molto interessanti per il loro ragguardevole fatturato e in quanto spesso sono assai mal protette. Ampiamente diffuso in Europa, il sistema di pagamenti mediante carta di credito con chip e PIN è invece poco utilizzato negli Stati Uniti[29]. Anche se sono possibili attacchi a fornitori che utilizzano questo sistema, gli attacchi a sistemi che ne sono privi presentano attualmente un rapporto costi-benefici più interessante per i malintenzionati.

Più specificamente, il caso della botnet BrutPOS evidenzia l'importanza di proteggere ogni interfaccia che consente l'accesso remoto a un apparecchio o a un sistema. MELANI ha messo in guardia a più riprese contro il rischio che comporta la tendenza a collegare alla rete sempre più apparecchiature di pilotaggio dei processi fisici sia nell'industria produttiva sia nella domotica. Anche se gli apparecchi o i sistemi coinvolti sono molto diversi, le norme di protezione dell'accesso remoto rimangono tendenzialmente le stesse.

4.5 Spionaggio – Casi selezionati della seconda metà del 2014

Regin – Trovati indizi della sua paternità

Anche nel secondo semestre sono stati nuovamente scoperti alcuni casi di spionaggio. Hanno prodotto il maggiore scalpore i rapporti di Symantec, Kaspersky e F-Secure nel mese di novembre del 2014 concernenti un malware denominato «Regin»[30]. Durante diversi anni il trojan Regin avrebbe spiato, inosservato, varie vittime tra cui obiettivi in Russia e Arabia saudita, ma anche in Paesi dell'Europa occidentale come Belgio o Austria. Regin consentirebbe ai suoi programmatori interventi di controllo e spionaggio in grande stile e sarebbe stato impiegato contro organizzazioni governative, amministratori di infrastrutture, aziende, enti di ricerca e privati. Sono degne di rilievo le attività di spionaggio esplicate da fornitori di servizi di telecomunicazione che risultano coinvolti in un caso su quattro. Al riguardo Symantec ha scoperto una funzione che riguarda la stazione base GSM. Kaspersky, che ha analizzato il malware per conto suo, ha aggiunto che nel mese di aprile del 2008 Regin avrebbe carpito codici di accesso di amministratori, coni quali si sarebbe

[29] In questo Paese, come in numerosi altri nel mondo, la maggior parte delle carte di credito in circolazione registra i dati su carta magnetica.

[30] http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance (stato: 28 febbraio 2015).
http://www.kaspersky.com/about/news/virus/2014/Regin-a-malicious-platform-capable-of-spying-on-GSM-networks (stato: 28 febbraio 2015).

potuto manipolare le reti GSM nel Medio Oriente. Poco dopo è comparsa la notizia sul sito Web di «The Intercept» che Regin sarebbe stato, fra l'altro, utilizzato anche contro l'impresa di telecomunicazioni Belgacom. In base ai documenti divulgati dall'informatore Edward Snowden si presume che l'attacco sia opera dei servizi segreti britannici GCHQ. In gennaio 2015 Kaspersky ha pubblicato ulteriori prove della paternità dell'attacco. L'azienda di sicurezza ha rilevato analogie tra Regin e un malware di nome Qwerty. Il *codice sorgente* di Qwerty era stato pubblicato in precedenza dalla rivista tedesca «Der Spiegel» e proviene dal compendio dei documenti di Edward Snowden. Qwerty sembrerebbe essere il modulo *keylogger* di Regin[31].

Alla fine del 2014 alcuni giornali hanno riportato il rinvenimento del malware Regin in un computer della Cancelleria federale tedesca. Si suppone che all'inserimento di una chiavetta USB sia scattato l'antivirus della Cancelleria. Sembrerebbe che la chiavetta fosse stata usata in precedenza sul computer privato di un collaboratore. Una portavoce del Governo ha poi dichiarato che la rete governativa non era stata infettata[32].

Red October reloaded?

Nel mese di dicembre del 2014 l'impresa di sicurezza Bluecoat ha scoperto un attacco di spionaggio mirato che si caratterizzava fra l'altro per la sua abilità di infettare anche dispositivi di telefonia mobile con Android o iOS nonché Blackberry. Gli iPhones e gli iPads potevano invece essere infettati soltanto se erano state precedentemente disattivate le restrizioni d'uso (*Jailbreak*). Il malware utilizza inoltre un meccanismo di comando e controlllo inusuale. I computer infettati comunicano via https e WebDav con uno stesso server del servizio svedese di *Cloud* chiamato CloudMe. Il malware di nome «Inception» era utilizzato prevalentemente per spiare dirigenti dei settori petrolifero e del gas, della finanza, militare, delle autorità e delle ambasciate. Si propagava mediante e-mail di *spear phishing* con cavalli di Troia camuffati in documenti allegati. Kaspersky, che ha pubblicato anche informazioni relative a questa campagna di spionaggio denominata Cloud Atlas[33], ha il sospetto che potrebbe trattarsi di una nuova versione del malware «Red October» («Ottobre Rosso»). Dopo la pubblicazione del rapporto Kaspersky su Red October nel mese di gennaio del 2013 la rete di spionaggio è stata immediatamente smantellata. In Cloud Atlas sono state rinvenute tracce che ricordano la campagna Red October, ovvero questi due attacchi di *spear phishing* condividono non solo un profilo di target simile, ma anche un documento simile.

Cloud Atlas è un esempio tipico di un *Advanced Persistent Threat (APT)*, un sofisticato attacco di spionaggio mirato che si caratterizza per professionalità (*advanced*), ma soprattutto per durata (*persistent*). Quando un APT viene scoperto e quindi bloccato, è probabile che gli hacker si siano già infiltrati nel sistema da un'alta parte o che sferrino un nuovo attacco quanto prima.

---

31 http://www.spiegel.de/netzwelt/netzpolitik/nsa-trojaner-kaspersky-enttarnt-regin-a-1015222.html (stato: 28 febbraio 2015).
http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html (stato: 28 febbraio 2015).

32 http://www.heise.de/newsticker/meldung/Offenbar-Spionagesoftware-Regin-auf-Rechner-im-Kanzleramt-entdeckt-2507042.html (stato: 28 febbraio 2015).

33 https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/ (stato: 28 febbraio 2015).

Sandworm – attacchi alla NATO e a membri del Governo ucraino

Alla fine del mese di ottobre del 2014 l'impresa di sicurezza iSight ha reso nota una campagna di spionaggio mirata contro membri del Governo dell'Ucraina, dell'Unione europea e della NATO che sfruttava, fra l'altro, una falla di sicurezza di Windows[34]. Ulteriori bersagli di attacco erano un'azienda francese di telecomunicazioni nonché un'impresa polacca del settore energetico. Lo sfruttamento di una falla di sicurezza in Microsoft Windows e in Windows Server (CVE-2014-4114) sinora sconosciuta lascia supporre che sia stata opera di un professionista[35].

Dall'estate del 2014 persistono attacchi a funzionari del Governo ucraino che vengono sferrati con l'invio di documenti PowerPoint, sfruttando la suddetta falla. iSight è stata in grado di far risalire le prime attività del gruppo al 2009. Sebbene sia gli interessi che alcune espressioni linguistiche rimandino alla matrice russa, anche in questo caso la paternità degli attacchi non è potuta essere pienamente appurata.

Presunti diversi attacchi ad aziende israeliane

Alla fine del mese di luglio del 2014 il giornalista indipendente Brian Krebs ha pubblicato che negli anni 2011 e 2012 sarebbero stati rubati a più riprese i piani dello scudo antimissile «Iron Dome» dell'esercito israeliano[36]. Krebs cita quale fonte l'impresa di sicurezza statunitense CyberESI che ha analizzato la campagna. Le vittime sarebbero i tre produttori di armi israeliani Rafael Advanced Defense Systems, Israel Aerospace Industries e Elisra Group. Si suppone che l'aggressore sia un noto gruppo cinese conosciuto con il nome di APT1 o unità PLA 61398. Le aziende colpite non hanno confermato gli attacchi.

Autorità nucleari statunitensi

Negli ultimi tre anni sarebbero state perpetrate con successo almeno tre azioni di hackeraggio di presunta matrice statale ai danni della Nuclear Regulatory Commission, l'autorità nucleare statunitense. In due circostanze gli indizi ricondurrebbero a un Paese preciso, che non viene però citato pubblicamente. Nextgov[37] asserisce che sono state impiegate metodologie di attacco comuni come *phishing* e *spear phishing*. È interessante rilevare che per il terzo attacco è stato utilizzato l'account di posta elettronica di un collaboratore per inviare un file .PDF compromesso a 16 colleghi, stratagemma che rende più difficile per il destinatario riconoscere la natura nociva della mail. Questa è una prassi consolidata per aggirare la protezione di un sistema aziendale al fine di raggiungere computer «interessanti», aprendo una breccia in stazioni intermedie in cui è più facile infiltrarsi.

Gli attacchi mirati di spionaggio non sono eventi isolati. Sussiste un interesse permanente e pertanto una pressione costante per i dati sensibili. Risulta comunque difficile stabilirne la paternità. Anche se, dato il profilo delle vittime, si presume che la maggioranza degli *Advanced Persistent Threats (APT)* sia di origine statale, la differenza tra hacker statali e criminali non è chiaramente definita.

---

34 http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/ (stato: 28 febbraio 2015)

35 http://www.isightpartners.com/2014/10/cve-2014-4114/ (stato: 28 febbraio 2015).

36 http://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/ (stato: 28 febbraio 2015).

37 http://www.nextgov.com/cybersecurity/2014/08/exclusive-nuke-regulator-hacked-suspected-foreign-powers/91643/ (stato: 28 febbraio 2015).

Amnesty International mette a disposizione strumenti di rilevamento per rintracciare software di sorveglianza

Nel mese di novembre del 2014 Amnesty International ha rilasciato un programma che sarebbe in grado di riconoscere software statali di sorveglianza quali «FinFisher». Con l'ausilio di FinFisher si possono per esempio intercettare conversazioni Skype, e-mail e addirittura controllare a distanza la video- e fotocamera dei dispositivi. Questo software viene impiegato fra l'altro anche contro attivisti dei diritti umani e dissidenti in Paesi con regimi autoritari e laddove la libertà d'opinione è limitata. Non è chiaro quanto sia efficiente il tool nel riconoscere i vari tipi di software di sorveglianza[38].

4.6 Attacco di spionaggio durante i viaggi di lavoro

Già da tempo si consiglia particolare prudenza nell'uso di collegamenti *WLAN* pubblici. L'esempio sinora più famoso di un attacco a una rete WiFi è noto con il nome di «Firesheep»: in una rete non sicura, ovvero aperta (per esempio in un Internet café), questa estensione permette di effettuare facilmente un *dirottamento di sessione* e catturare quindi dati dell'utente come la sua password. Questo attacco però funziona soltanto quando vengono trasmessi dati non crittografati senza un protocollo di trasmissione sicuro https. Nel mese di novembre del 2014 il fornitore di servizi di sicurezza Kaspersky ha pubblicato un rapporto intitolato Darkhotel, relativo a un gruppo di hacker che hanno sferrato in reti wireless di hotel attacchi mirati, molto più nocivi di quelli conosciuti finora[39]. Da quattro anni sarebbero stati attaccati in maniera mirata manager di alto livello durante i loro viaggi di lavoro in Asia. La modalità fa pensare a uno spionaggio economico. Tuttavia sono state colpite anche persone comuni. L'attacco viene sferrato appena la vittima, dopo aver effettuato il check in, utilizza il proprio computer e tenta di accedere alla WLAN del proprio hotel. Sullo schermo appare un messaggio indicante che un determinato programma deve essere aggiornato, ad esempio Google-Toolbar, Adobe Flash o Windows Messenger. Ovviamente il presunto aggiornamento è invece un malware in grado di carpire dati dal computer.

D'altronde, lo scorso semestre il Secret Service degli Stati Uniti ha messo in guardia contro *keylogger* nei computer pubblici in hotel o aeroporti. In una comunicazione rivolta al settore della ristorazione esortavano gli addetti ai lavori a controllare i computer messi a disposizione del pubblico. Motivo del comunicato è stato l'arresto di persone sospettate di aver introdotto *keylogger* nei computer di diversi business center di grandi alberghi di Dallas/Fort Worth[40].

Chi utilizza una WLAN dovrebbe essere sempre prudente nella navigazione. Non si devono accettare programmi che verrebbero installati durante il tentativo di login nella rete WiFi. Inoltre, si deve verificare scrupolosamente che il computer sia sempre aggiornato, altrimenti bastano le cosiddette *infezioni di siti Web* per infettarlo. Chi deve elaborare dati critici per il proprio lavoro fuori sede dovrebbe considerare piuttosto l'alternativa della funzione hotspot personale del proprio cellulare e la sua funzione di *roaming*, nonostante questa soluzione sia molto costosa.

[38] http://www.amnesty.ch/de/themen/weitere/meinungsaeusserungsfreiheit/dok/2014/detekt-software-zum-aufdecken-von-ueberwachung (stato: 28 febbraio 2015).

[39] http://blog.kaspersky.com/darkhotel-apt/ (stato: 28 febbraio 2015).

[40] http://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-centers/ (stato: 28 febbraio 2015).

Dai computer pubblici non bisognerebbe accedere a servizi che richiedono un login o una password. Questo servizio degli hotel dovrebbe essere utilizzato soltanto, ad esempio, per informarsi sulle attrazioni turistiche della città.

4.7 Furti di dati in grande stile

Anche quest'anno diversi furti di dati hanno fatto notizia. Un caso si è distinto in particolare, non tanto per il numero di record rubati, ma per il modus operandi dei ladri. Nel mese di agosto uno dei maggiori gestori di strutture ospedaliere degli Stati Uniti ha denunciato il furto di 4,5 milioni di dati di pazienti. Specialmente nel settore della sanità i pazienti esigono un elevato livello di protezione dei dati in quanto sensibili. Contemporaneamente anche nel settore della sanità la digitalizzazione avanza molto celermente. Se questo, da un lato, porta vantaggi e contribuisce a limitare gli errori, dall'altro comporta determinati rischi.

Nel caso specifico, il «Community Health System», uno dei maggiori gestori di strutture ospedaliere degli Stati Uniti, aveva denunciato nel mese di agosto del 2014 un'intrusione nei propri sistemi informatici nella quale erano stati sottratti dati di quasi 4,5 milioni di pazienti che erano stati curati in un ospedale del gruppo nei cinque anni precedenti. L'azienda di sicurezza Mandiant ha chiamato in causa hacker cinesi. Secondo l'impresa che gestisce 206 ospedali in 29 Stati federali, sarebbero stati rubati, fra l'altro, nomi, indirizzi, numeri telefonici, dati anagrafici e i numeri di previdenza sociale (*Social Security Number, SSN*). Non è stato possibile accertare quale fosse lo scopo esatto degli hacker e se dietro l'attacco ci fossero anche attori statali.

Il settore finanziario è un ulteriore bersaglio di furti di dati. Ha fatto notizia a questo proposito l'attacco ai danni della grande banca statunitense J.P. Morgan. Scoperto a metà agosto 2014, l'attacco avrebbe consentito di copiare dal server dell'istituto di credito dati di circa 76 milioni di famiglie e sette milioni di aziende. Sono stati sottratti dati di clienti come nomi, indirizzi, numeri telefonici e indirizzi e-mail, mentre non ci sono sinora indizi del furto di dati più sensibili come numeri di conto, dati anagrafici, password o codici di sicurezza sociale. J.P. Morgan afferma di aver identificato il vettore di attacco: una falla di sicurezza presente già dal mese di giugno del 2014. Non è dato di sapere con esattezza di che tipo di vulnerabilità si trattasse. Sono stati disattivati i conti in pericolo e modificate le password di tutti i tecnici delle TIC. Secondo le autorità, gli indizi portano ad hacker altamente professionali, che forse si trovano in Russia. Si suppone che gli attacchi siano stati motivati dalle sanzioni USA contro la Russia, ma mancano le prove.

Diversa è l'annuncio fatto dall'azienda Holdsecurity all'inizio del mese di agosto del 2014 che afferma di aver scoperto un furto di dati da parte di hacker russi di proporzioni senza precedenti: 1,2 miliardi di combinazioni di login/password. I dati di accesso proverrebbero dal oltre 420 000 siti Web, tra cui anche alcuni di aziende note. La caratteristica di questo caso è che l'azienda coinvolta ha annunciato in concomitanza con la denuncia della scoperta il lancio di un nuovo servizio che permetterebbe di verificare se si è vittima di questo o altri furti di dati.[41]

Sovente le aziende di sicurezza mettono tali dati a disposizione delle autorità competenti o dei provider colpiti affinché ne possano informare le vittime. La questione della gestione responsabile di tali informazioni acquisirà sempre maggiore importanza in futuro ed è trattata nei dettagli nel capitolo 5.5.

[41] http://www.forbes.com/sites/kashmirhill/2014/08/05/huge-password-breach-shady-antics/ (stato: 28 febbraio 2015).

4.8 iCloud attaccata dagli hacker – foto di persone famose in Internet

Alla fine del mese di agosto del 2014 sono state pubblicate prima sul sito 4chan e poi su varie altre piattaforme foto rubate che ritraggono persone famose senza veli. È emerso rapidamente che le foto provenivano da vari account iCloud, il servizio di memorizzazione nel cloud (nuvola) di Apple. Sono state formulate varie ipotesi circa il metodo utilizzato per accedere alle fotografie, ma i sospetti si sono rapidamente concentrati sul software Find My iPhone, utilizzato per localizzare apparecchi persi o rubati. Secondo il parere ufficiale di numerosi esperti questo programma sarebbe stato vulnerabile a un attacco *brute force* che consiste nel testare in modo automatico un grande numero di password per accedere a un servizio. Il sospetto è stato rafforzato dal fatto che poco prima che scoppiasse lo scandalo un *proof of concept* (PoC) relativo a questo metodo era stato pubblicato sul sito GitHub. Una misura di sicurezza classica per proteggersi dagli attacchi brute force consiste nel bloccare il servizio dopo un determinato numero di tentativi di accesso infruttuosi. Questa modalità non era stata predisposta per Find My iPhone all'epoca, ma è stata implementata poco dopo lo scandalo delle foto rubate. Inoltre, occorre precisare che Apple ha respinto l'ipotesi di una vulnerabilità di Find My iPhone o di un altro suo servizio. In una dichiarazione ufficiale, l'impresa attribuisce la fuga a un attacco mirato per ricercare nomi di utenti, password e domande di sicurezza di determinati account[42].

Questo non è l'unico caso in cui la sicurezza dei servizi di memorizzazione nel cloud sono stati messi in dubbio. Anche Dropbox, ad esempio, è stata nel mirino quando dati di accesso al servizio sono stati postati sul sito Pastebin, un'applicazione web che permette agli utenti di inviare frammenti di testo, nel mese di ottobre del 2014. Questi casi diversi riportano nuovamente al centro dell'attenzione la problematica della sicurezza dei dati memorizzati nel cloud. Questa modalità di salvataggio dei dati offre a un hacker la possibilità di accedere in remoto a numerosi dati personali compromettendo un sistema o un account vulnerabile. Nel caso di iCloud o di servizi simili, inoltre si deve precisare che numerosi utenti non sono consapevoli che le foto che scattano con un dispositivo sono sincronizzate automaticamente con un account nel cloud. Questo parametro può infatti essere attivato per default. È pertanto di fondamentale importanza che l'utente verifichi una per una tutte le «app» e che ne disattivi la sincronizzazione automatica, se lo desidera.

Per gli utenti che scelgono di utilizzare il cloud, in questo come in altri casi, si raccomandano le norme di sicurezza che si applicano ad altri account online, come la posta elettronica. Suggeriamo di scegliere individualmente per ciascun servizio una password complessa contenente diversi tipi di caratteri. Inoltre, MELANI raccomanda, laddove possibile, di preferire le opzioni di *autenticazione a due fattori*[43]. Infine, il caso della pubblicazione di foto di persone famose senza veli ribadisce che il miglior mezzo per evitare la fuga di materiale compromettente rimane quello di non produrlo, o perlomeno di non salvarlo su un supporto digitale collegato in rete.

[42] http://www.bbc.com/news/technology-29039294 (stato: 28 febbraio 2015).

[43] Un elenco di siti che autorizzano l'autenticazione a due fattori è disponibile alla pagina: https://twofactorauth.org (stato: 28 febbraio 2015).

4.9 Nuove gravi falle di sicurezza in parti di software

Lo scorso semestre, oltre a numerose falle riscontrate in applicazioni come Flash, Acrobat, Java e Office, sono state scoperte anche vulnerabilità gravi in sistemi operativi e librerie di base.

Poodle

Dopo Heartbleed, una nuova grave falla di sicurezza ha colpito *SSL*, un protocollo di rete per il trasferimento sicuro di dati. A differenza di Heartbleed, la falla denominata Poodle[44] non è un errore di programmazione, ma è una falla contenuta nel protocollo stesso, più esattamente nella versione 3 di *SSL*. La vulnerabilità consiste nel fatto che *SSL/TLS* prima protegge l'integrità dei dati e li crittografa solo in un secondo tempo. Poiché solitamente la crittografia avviene per blocchi di caratteri di lunghezza prestabilita, in coda ad ogni riga viene attaccato il numero esatto di caratteri necessario affinché ogni blocco sia della lunghezza adeguata. L'ultimo *byte* contiene l'indicazione del numero dei caratteri di riempimento. Il punto debole sta proprio qui. I caratteri di riempimento e l'ultimo byte sono anch'essi crittografati, ma non ne viene verificata l'integrità. Un hacker può quindi aggiungere indisturbato caratteri a piacere, anche segmenti delle righe che vorrebbe gli fossero decrittografate. Per questo basta che l'hacker sia in grado di sferrare attacchi del tipo «*Man in the Middle*», interponendosi in una comunicazione. Questo è possibile, ad esempio, in una rete WiFi aperta.[45]

Per questo motivo MELANI raccomanda agli amministratori di siti Web di disattivare completamente SSLv3 e di utilizzare, per quanto possibile, esclusivamente protocolli di crittografia TLS 1.1 o TLS 1.2. Nel frattempo, SSLv3 non è più supportato nella maggioranza dei browser attuali.

Shellshock

La falla Shellshock[46] ha colpito, tra l'altro, quasi tutti i sistemi operativi di tipo Unix. Attraverso questa falla di sicurezza codici di programma possono essere eseguiti senza controllo. La vulnerabilità è stata scoperta in «Bash Shell», un software ampiamente usato. Attacca server e client, ma anche dispositivi come *router* o *gateway di sicurezza*. Sono state trovate più falle, corrette di volta in volta. La vulnerabilità deriva dal fatto che le variabili di ambiente trasferite non sono controllate correttamente per cui a una determinata variabile più essere trasferito un codice aggiuntivo, quindi anche un codice nocivo.

```
$ env x='() { :;}; echo VULNERABLE' bash -c ""
```

Gli scenari d'attacco sono molteplici:

- HTTP / server web tramtie l'interfaccia CGI
- SSH
- DHCP
- SIP
- e molti altri

---

44 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 (stato: 28 febbraio 2015).

45 Qui trovate una descrizione dettagliata del funzionamento della falla Poodle: https://nakedsecurity.sophos.com/2014/10/16/poodle-attack-takes-bytes-out-of-your-data-heres-what-to-do/ (stato: 28 febbraio 2015).

46 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271 e gli altri numeri di CVE 2014-7169, 2014-7186, 2014-7187, 2014-6277, 2014-6278 (stato: 28 febbraio 2015).

Una volta che la falla è stata resa nota, MELANI ha constatato un aumento massiccio dei tentativi di scansione e di exploit che nel frattempo si sono ridimensionati, senza tuttavia scomparire del tutto.

Kerberos

Un'altra falla (MS14-068[47]) che può avere gravi ripercussioni, in particolare per le aziende, sta nell'implementazione di Kerberos in *Active Directory,* il servizio directory di Microsoft. La falla consente a un utente malintenzionato di portare i suoi privilegi di account al livello più alto (amministratore di dominio) e quindi di avere il completo controllo della *Active Directory*. Ciò significa che, in linea di principio, un unico attacco andato a buon fine (ad es. mediante un malware) contro un solo utente di un'azienda può compromettere l'intera *Active Directory* e quindi permettere agli hacker di assumere il controllo di tutte le risorse Windows. MELANI raccomanda di colmare la falla, ma soprattutto di creare e sottoporre regolarmente a test piani di emergenza per il ripristino delle *Active Directories.* Inoltre, devono essere particolarmente protetti gli account con i privilegi più elevati.

SChannel

Un'ulteriore falla di sicurezza di Windows (MS14-066)[48] ha colpito Secure Channel. SChannel è l'implementazione di Microsoft del protocollo di crittografia SSL/TLS che consente di scambiare in modo crittografato informazioni sensibili attraverso una rete aperta. Microsoft ha affermato che un hacker potrebbe sfruttare la falla di sicurezza mediante pacchetti di rete appositamente predisposti ed eseguire un codice arbitrario da remoto nel sistema da lui violato. La società Cisco ha menzionato inoltre in un post sul suo blog numerosi *overflow del buffer*[49]. Questa patch ha creato grosse difficoltà a Microsoft e ha dovuto essere migliorata a più riprese per contrastarne effetti collaterali indesiderati come problemi di performance.

In generale MELANI osserva che gli hacker si concentrano fortemente sui software più diffusi in rete come Flash, Acrobat e Java. Non appena viene rilasciata una nuova patch, gli hacker la analizzano sotto il profilo della vulnerabilità rimossa e integrano nei loro *exploit kit* un nuovo attacco che prende sistematicamente di mira le apparecchiature non ancora aggiornate. Questo avviene solitamente in pochi giorni. Singoli *exploit kit* dispongono addirittura di falle finora sconosciute (*0-day exploits*) che utilizzano per gli attacchi a terminali. Per questo motivo MELANI raccomanda ai privati e alle PMI di automatizzare gli aggiornamenti e alle aziende più grandi di implementare una modalità rapida di gestione delle patch con processi e ordine di priorità chiaramente definiti.

4.10 Falla di sicurezza negli standard di telefonia mobile

Nel mese di dicembre del 2014 esperti TIC del gruppo berlinese che fa capo a Karsten Nohl hanno reso pubblica una falla di sicurezza nella rete di telefonia mobile che è in grado di aggirare la crittografia considerata sicura nella rete *UMTS,* consentendo, ad esempio, di intercettare *SMS*. Il protocollo SS7 (Signaling System 7) colpito dalla falla è utilizzato per scambiare informazioni tra singoli provider di servizi di telecomunicazioni, ad esempio per inviare SMS o effettuare chiamate tramite reti diverse. Il protocollo stesso risale agli anni

47 https://technet.microsoft.com/en-us/library/security/ms14-068.aspx (stato: 28 febbraio 2015).

48 https://technet.microsoft.com/en-us/library/security/MS14-066 (stato: 28 febbraio 2015).

49 http://blogs.cisco.com/security/talos/ms-tuesday-nov-2014 (stato: 28 febbraio 2015).

Ottanta ed è quindi relativamente obsoleto. Sebbene sia già stato rinnovato due volte per inserire nuove funzioni, il problema principale dell'assenza di un'autenticazione tra i partner non è mai stato risolto. Finché i grossi provider erano poco numerosi e si conoscevano tra loro, fidandosi reciprocamente, non vi erano problemi. Tuttavia, attualmente il mercato mondiale della telefonia mobile è conteso da una molteplicità di provider più o meno affidabili di cui alcuni vendono l'accesso a SS7 a terzi.

Con questa falla di sicurezza un hacker può scegliere i seguenti vettori di attacco:

- Tracciamento di un dispositivo:
  ogni apparecchio si aggancia alla cella radio più vicina. Per rintracciare la cella utilizzata momentaneamente da una persona da sorvegliare, all'hacker basta conoscere il suo numero di telefono. L'ubicazione della cella radio agganciata può quindi essere ritrovata in una banca dati. In aree densamente popolate e con molte celle radio un utente può essere localizzato abbastanza precisamente. Se poi sono noti anche l'*International Mobile Subscriber Identity (IMSI)* e il Global Title (indirizzo utilizzato per il routing delle chiamate) sussistono altri vettori di attacco che funzionano anche se il provider dovesse bloccare alcune funzioni del protocollo.

- Intercettazione e ascolto di conversazioni:
  quando un dispositivo è collegato a una rete estera, in determinate situazioni vengono effettuate richieste al «provider nazionale». Se un hacker sovrascrive i dati del provider nazionale con il proprio indirizzo, il dispositivo «cade» nella rete dell'hacker che è così in grado di deviare le chiamate, indirizzandole a se stesso, e di intercettarle, svolgendo un ruolo di *Man in the Middle* all'insaputa della vittima.

- Intercettazione di mTAN (codici di autenticazione di transazioni mobili):
  anche l'aggiornamento delle informazioni su come raggiungere un determinato dispositivo avviene senza autenticazione, creando in questo modo vulnerabilità. Un hacker può far credere che la sua vittima si trovi nella sua rete informandone il provider originario e facendo in seguito effettivamente deviare le chiamate o gli SMS verso la propria rete. In questo modo può, ad esempio, catturare un mTAN, ossia l'autenticazione via SMS per l'e-banking.

- Intercettazione di IMSI:
  per comunicare a un dispositivo una chiamata in entrata si utilizza un'identità temporanea (TIMSI) che viene trasmessa in rete in modalità non crittografata. Se un malintenzionato la intercetta, può richiedere alla centrale telefonica l'ID reale dell'apparecchio (IMSI). Un hacker che conosce l'IMSI ha ampio margine di manovra e può ottenere il numero telefono reale o richiedere la chiave di crittografia del collegamento attivo.

Gli scenari d'attacco sono relativamente facili da eseguire e molto probabilmente vengono applicati anche da attori dell'ambito statale e parastatale. Per questa ragione le informazioni sensibili, come ad esempio i segreti commerciali, non devono essere scambiate su cellulare, specialmente se uno degli interlocutori si trova all'estero ed effettua una chiamata in roaming. MELANI sta discutendo con i provider di telefonia cellulare in Svizzera su come risolvere per quanto possibile queste vulnerabilità[50].

[50] Quelle: Tobias Engel, http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2553/original/31c3-ss7-locate-track-manipulate.pdf (stato: 28 febbraio 2015).

4.11 Vulnerabilità – neanche MacOSX è risparmiato

MELANI constata che sono viepiù sfruttate lacune nel sistema operativo MacOSX sia per attacchi mirati sia per diffondere malware in generale. Analogamente a quanto avviene in ambiente Windows, vengono spesso sfruttate vulnerabilità in Java o in un plugin di browser come Acrobat Reader o Flash.

Nei mesi scorsi due famiglie di malware hanno destato grande scalpore:

- iWorm[51] è una *backdoor* che può essere impiegata per diversi scopi. È interessante la modalità per la quale il malware riceve istruzioni sui server di controllo con cui deve comunicare. A questo scopo si avvale di messaggi pubblicati sul sito di social news «Reddit» dagli aggressori per generare l'URL del Command & Control server attuale. La diffusione di iWorm avviene essenzialmente attraverso copie pirata compromesse distribuite tramite il software BitTorrent[52].

- Wirelurker[53] è un malware che contiene un componente MacOSX e un componente iOS. Se il malware è attivo su un dispositivo OSX, aspetta di essere collegato a un dispositivo iOS (iPhone, iPad) con una chiavetta *USB*. Il malware seleziona quindi varie informazioni (numeri telefonici, dati di iTunesStore, ecc.) e le invia a un Command & Control server. Poiché un collegamento con una chiavetta USB è considerato affidabile, il malware può essere diffuso quale normale app. A questo scopo l'app necessita di un certificato enterprise e di un profilo di fornitura (*provisioning profile*) che «certificano» l'integrità del malware e il gioco è fatto. Questa procedura lancia una richiesta all'utente. Se questo l'accetta, il malware viene installato. Nei dispositivi con *Jailbreak* questo passo viene saltato. Con tali certificati enterprise un'impresa può installare applicazioni proprie sui suoi dispositivi iOS. Il malware per OSX si diffonde come iWorm attraverso copie pirata di software commerciali.

MELANI constata altresì che account iTunes e iCloud, oltre ad essere bersaglio di attacchi con malware, sono viepiù presi di mira con attacchi di *phishing*. Con la più classica delle metodologie, gli utenti sono indotti da un'e-mail che non desta sospetti a inserire i propri dati di login in un server colpito dagli hacker, consentendo loro l'accesso al proprio account.

L'interfaccia Thunderbolt contiene inoltre una vulnerabilità da prendere molto sul serio che la rende bersaglio anche di attacchi mirati[54]. Questa vulnerabilità consente a un hacker che ha fisicamente accesso a un dispositivo di modificare direttamente il *firmware* EFI del Mac infettando un dispositivo modificato da Thunderbolt, come ad esempio un adattatore Gigabit. Un malware diffuso con questa modalità è molto difficile da scoprire, poiché si carica prima del sistema operativo ed è quindi in grado di occultarsi da questo e sfuggire a un eventuale antivirus. Apple ha rilasciato una patch che chiude la falla perlomeno per OSX Yosemite (10.10.2).

51 http://news.drweb.com/show/?i=5977&lng=en (stato: 28 febbraio 2015).

52 http://www.thesafemac.com/iworm-method-of-infection-found/ (stato: 28 febbraio 2015).

53 https://www.paloaltonetworks.com/resources/research/unit42-wirelurker-a-new-era-in-ios-and-os-x-malware.html (stato: 28 febbraio 2015).

54 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4498 (stato: 28 febbraio 2015).

5 Tendenze / Prospettive

5.1 Raccolta e scambio di informazioni al tempo di Big Data

Già verso la fine del secolo scorso si è insinuatastart la credenza che dati e informazioni fossero il nuovo oro. Innumerevoli startup di Internet spuntarono come funghi, con piani commerciali in cui la raccolta di dati e informazioni era registrata negli attivi. Si trascurava intenzionalmente di riflettere su come trasformare dati in denaro. Altrettanto implacabile fu il risveglio sui mercati quando, accanto a numerosi dati e informazioni accumulati, furono presentate essenzialmente cifre rosse. L'euforia pioneristica si trasformò in una vera e propria prostrazione e nel mese di marzo del 2000 la bolla delle dot.com esplose quasi con la stessa velocità con la quale si era formata. Una quindicina d'anni dopo specialmente le imprese di Internet sembrano aver imparato la lezione: i servizi in rete sono resi a pagamento oppure, in alternativa, i servizi gratuiti sono offerti in cambio di dati personali. Che si tratti di Facebook, Google o Twitter, la raccolta e il vaglio di dati e informazioni produce nel frattempo un considerevole controvalore monetario.

Vista positivamente, la raccolta di dati e informazioni consente di valutare profili, personalizzare la pubblicità e offrire ai clienti servizi sempre più su misura. In una loro interpretazione di questo fatto e, al fine di offrire il prodotto sicurezza in termini razionali, certi servizi di intelligence tendono a richiamare l'attenzione sul fatto che per trovare l'ago (perlopiù terroristico) ci vuole innanzitutto un pagliaio. Anche sul piano internazionale e interstatale la raccolta e lo scambio di informazioni stanno diventando una panacea, ad esempio, nella lotta agli abusi nell'ambito della sottrazione d'imposta o nella collaborazione internazionale nella ricerca di persone. Tuttavia, perlomeno per quanto concerne il rilevamento e la valutazione di dati personali a livello statale e il loro scambio in ambito internazionale, occorre partire dal presupposto che il quadro giuridico è restrittivo, a differenza di quanto avviene nella raccolta di dati a livello privato.

In ogni caso, in questa tendenza si stanno profilando due problematiche fondamentali. Da un lato, la raccolta centralizzata di dati e informazioni concentra anche gli attacchi. Non deve sorprendere che negli attacchi alle imprese il volume di dati sottratti sia in continuo aumento. Se dieci anni fa qualche migliaia di indirizzi e-mail rubati facevano notizia, oggi ce ne vorrebbero almeno un paio di milioni e dovrebbero essere corredati dalle relative password. Il fatto che i nostri dati possano essere sottratti a imprese alle quali non siamo consapevoli di averli mai messi direttamente a disposizione non ci deve sorprendere, in quanto informazioni e dati sono oggetti di un intenso commercio. Nella maggior parte dei casi un primo scambio è avvenuto con il permesso implicito del proprietario dei dati che in un determinato momento ha accettato le condizioni generali o le disposizioni sulla protezione dei dati per poter finalmente ordinare un libro tanto atteso o aprire un account di social media. Proprio in tema di sicurezza tecnica della proprietà dei dati è rafforzato il principio dell'anello più debole della catena. Per quanto sia preciso un accordo, per quanto sia rigoroso un contratto sulla raccolta e sullo scambio tecnico di dati, non esiste la piena garanzia che questi non possano andare a finire nelle mani sbagliate. Questo vale non solo per i privati, ma anche per le istituzioni statali, come illustrato, ad esempio, dal caso di hackeraggio del sistema d'informazione Schengen (SIS) in Danimarca[55].

[55] Rapporto semestrale MELANI 2013/2, capitolo 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=it (stato: 28 febbraio 2015).

D'altro canto si pone la domanda dell'uso di questo immenso flusso di dati. Nel settore privato si può desumere la prevalenza di considerazioni di economia di mercato. Il detentore dei dati spera di ottenere un compenso cedendo i dati. È senz'altro ragionevole voler vendere i propri dati al miglior offerente. La situazione è diversa quando è formulata una richiesta di inviare questi dati alle autorità preposte alla sicurezza di un Paese. Anche nelle relazioni internazionali si pone la questione dell'uso dei dati.
La semplificazione della lotta alla sottrazione d'imposta con lo scambio automatico di informazioni è senz'altro opportuna. È tuttavia urgente disciplinare anche l'uso di tali informazioni negli Stati beneficiari. La Svizzera, ad esempio, si è fortemente adoperata nel quadro dell'OCSE affinché in sede di scambio automatico di informazioni non ci si concentri solo sulle categorie di dati da rilevare, ma anche sull'uso adeguato degli stessi. Evidentemente, come ha dimostrato nel 2014 una sentenza del Tribunale amministrativo federale, non possiamo avere la garanzia che lo Stato partner stia sempre ai patti[56].

Nella fattispecie, risalente all'estate del 2012, in cui un cittadino svizzero era sospettato di insider trading, le autorità pachistane richiesero l'assistenza amministrativa dell'autorità svizzera di vigilanza sui mercati finanziari (FINMA). La FINMA concesse l'assistenza amministrativa e il cittadino svizzero accusato presentò un ricorso presso il Tribunale amministrativo federale, adducendo che le competenti autorità pachistane non erano in grado di garantire il rispetto del principio di specialità e riservatezza. E-mail delle autorità pachistane nonché scambi di corrispondenza tra queste e la FINMA apparvero sulla stampa pachistana, confermando la violazione del segreto d'ufficio. La FINMA sospese immediatamente la procedura di assistenza amministrativa.

Con la tendenza verso Big Data con tutti i vantaggi e gli svantaggi correlati, si impongono oltre alle questioni di sicurezza tecnica e responsabilità degli amministratori di tali raccolte di dati anche le questioni fondamentali della *due diligence* in materia di valorizzazione e uso delle informazioni. Sono sollecitati in primo luogo tutti coloro che forniscono volontariamente i propri dati e che devono essere consapevoli di quanto accade agli stessi. Sono sollecitate anche le autorità statali, in quanto garanti della raccolta e trasmissione legittima dei dati, a vigilare affinché non sia fatto uso improprio delle informazioni fornite. Lo sviluppo di procedure di audit e controllo più snelle per garantirlo sarà una delle maggiori sfide del prossimo futuro.

5.2 L'interconnessione totale è intelligente e sicura?

Internet – la rete delle reti – collega sistemi TIC e permette di trasferire informazioni e dati. Non è costituita solamente dal World Wide Web che pubblica siti Web. Su Internet, infrastruttura mondiale per le telecomunicazioni, le persone possono comunicare anche con le macchine e possono impartire loro istruzioni che hanno poi ripercussioni sul mondo fisico. Nel frattempo le macchine sono anche in grado di comunicare tra di loro, ovviamente (per ora) solo dopo essere state programmate. Microcomputer capaci di comunicare assumono ruoli sempre più importanti in diversi aspetti della vita. La rilevazione di stati mediante sensori e l'esecuzione di comandi da parte di attuatori per sortire un effetto permettono di automatizzare notevolmente i processi, aiutando l'uomo non solo nel mondo virtuale, ma anche in quello fisico.

56 http://www.bvger.ch/publiws/download;jsessionid=F01EA73D27D15FF364A9203975D0B648?decisionId=f736b6ed-38ba-4d10-bf8f-c0312d05030f (stato: 28 febbraio 2015).

Nel quadro di questo sviluppo sono stati creati termini quali *Internet of things* (Internet delle cose o degli «oggetti intelligenti»), *pervasive computing* (informatica pervasiva), *ubiquitous computing* (informatica onnipresente), *wearable computing* (informatica indossabile, laddove dispositivi di rilevamento e valutazione di dati sono direttamente incorporati in indumenti o gioielli). Nel frattempo, non è solo il telefono ad essere diventato «intelligente»: anche automobili (*smart car / smart drive*), spazi abitativi (*smart home*) o addirittura interi edifici (*smart building*) e non da ultimo impianti industriali (*smart factory / smart manufacturing*)[57] sono in grado di rilevare, ottenere, elaborare, trasmettere dati e derivarne comandi ed eseguire azioni.

Il successo della tecnologia basata su Internet e il bisogno di interoperabilità fanno sì che sempre più applicazioni di scambio di dati siano basate su protocolli Internet. Ad esempio, nelle case «intelligenti» i sensori e gli attuatori della domotica sono collegati alla WLAN domestica perché l'infrastruttura è già presente e gli abitanti della casa vorrebbero comunque poter comandare i dispositivi con lo smartphone, anch'esso già collegato alla rete domestica. Questo comporta per forza interfacce tra il World Wide Web, esposto allo scambio globale di dati e informazioni, e dispositivi locali come il sensore della temperatura del riscaldamento o la lampadina nel salotto di casa. Accendere il riscaldamento e lo scaldabagno nella casa di vacanza mediante smartphone prima del proprio arrivo può avere senso, un po' meno accendere o spegnere le luci se si è assenti e probabilmente non ha senso utilizzare questa funzione per alzare e abbassare uno schermo per la riproduzione domestica di contenuti teatrali o cinematografici (*home theatre*). Sebbene i produttori di questi sistemi offrano solo raramente il comando «di serie» dell'ambiente domestico via Internet (solitamente questo sfrutta la rete domestica), ipoteticamente l'opzione esiste e può quindi essere sfruttata[58]. Tuttavia, tutti questi sistemi devono essere protetti non solo da attacchi della rete, ma anche da minacce locali. Oltre alla WLAN anche altre interfacce senza fili (ad es. *i bluetooth* o l'*NFC*) potrebbero costituire una porta d'accesso se non vengono adeguatamente implementati e protetti.

Dal lato degli utenti, lo smartphone sta diventando viepiù un dispositivo di identificazione e di servizio nonché di raccolta e valutazione di dati. Lo si può osservare con forza, tra l'altro, dalle app nell'ambito della salute che stanno diventando di moda. Si deve tenere adeguatamente conto della sicurezza dello smartphone per ragioni di protezione dei dati e di sicurezza. Occorre riflettere anche sulle procedure da adottare in caso di compromissione o perdita dello smartphone per prevenirne l'abuso da parte di persone non autorizzate e per trasferire consuete funzioni e dati su un dispositivo sostitutivo.

Con tutte le comodità che ci regala un ambiente «*smart*» dobbiamo mantenere uno spirito critico nei confronti della raccolta, dell'elaborazione e della memorizzazione dei dati e riflettere su come ce la caveremmo senza il supporto del nostro braccio destro collegato in rete. Sapremo arrangiarci se non funziona lo sciacquone della toilette intelligente[59] perché manca la carta igienica o è interrotta la connessione Internet? Si deve sempre tenere presente che il comando di processi fisici con strumenti informatici in rete può sempre essere bersaglio di manipolazioni dolose da parte di persone non autorizzate. Il loro scopo può essere quello di creare intenzionalmente disagi, oppure di nuocere seriamente o ancora di

---

57 Nella sua strategia high tech il Governo tedesco parla di «*Industria 4.0*» secondo la quale deve essere promossa l'informatizzazione delle tecniche di produzione: http://www.bmbf.de/de/9072.php

58 Cfr. in merito il Rapporto semestrale MELANI 2013/2, capitolo 5.5: Attacchi ai router domestici: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=it (stato: 28 febbraio 2015).

59 http://www.heise.de/newsticker/meldung/31C3-Hacker-nehmen-vernetzte-Toiletten-ins-Visier-2507287.html (stato: 28 febbraio 2015).

sfruttare il controllo dei dispositivi e i servizi a scopi estorsivi nei confronti degli utenti autorizzati.

5.3 Estorsione – varie modalità

Tra i vari mezzi utilizzati dai criminali per trarre profitto economico dai loro attacchi ce n'è uno che ha registrato un incremento spettacolare nel corso degli ultimi anni: l'estorsione. Con sempre maggiore frequenza, infatti, i malintenzionati mirano ad estorcere denaro, utilizzando come strumento per fare pressione perlopiù dati appartenenti alla vittima.

In una prima categoria di modus operandi, i criminali accedono a dati sensibili per ricattare le vittime minacciando di divulgarli. In mancanza di un versamento di denaro a loro favore i dati saranno pubblicati. Nel corso dei sei mesi in esame sono stati resi pubblici numerosi casi di questo tipo che avevano per bersaglio imprese. Possiamo citare, in particolare, la condotta del gruppo di hacker Rex Mundi che ha fatto numerose vittime con una modalità operativa identica. Viene effettuata un'*iniezione SQL* nel sito dell'impresa che consente di accedere a una base di dati contenente, tipicamente, informazioni relative ai clienti e ai loro scambi con l'azienda. In un secondo tempo gli hacker contattano l'impresa target: se la richiesta di pagamento non è assecondata, i dati rubati saranno pubblicati. Sono stati rivelati anche attacchi più sofisticati sempre a scopi estorsivi in cambio della non divulgazione di informazioni sensibili. Facciamo riferimento, in particolare, all'attacco a Sony Pictures, di cui al capitolo 4.1 del presente rapporto. In casi analoghi i criminali contano sulla disponibilità di un'azienda a pagare il riscatto per evitare di rendere pubblica la falla e il danno all'immagine.

Se viene fatta leva su minacce di ledere la riservatezza dei dati per ottenere denaro, una tendenza ancora più marcata, specie per gli individui, è quella dei ransomware che prendono di mira la disponibilità dei dati. Le diverse famiglie di ransomware, dai più semplici che congelano il computer della vittima a Cryptolocker e alle sue varianti che crittografano i dati contenuti nel dispositivo infettato, risultano essere una fonte di reddito inesauribile per i criminali. Numerosi esperti concordano nell'affermare che questa tendenza è destinata a durare nel tempo. La ragione principale del loro successo risiede nella propensione delle vittime a pagare per recuperare l'accesso ai propri dati o al proprio dispositivo, propensione che sembra elevata stando a una ricerca dell'Università del Kent secondo la quale il 40 per cento delle vittime di Cryptolocker pagano nella speranza di riavere i propri dati[60]. Agli occhi del criminale quello che conta non è tanto il valore intrinseco dei dati ricercati e le possibilità di rivenderli quanto piuttosto il valore che la vittima attribuisce agli stessi e dal quale scaturisce la sua decisione di cedere al ricatto nella speranza di recuperarli. È pertanto un ragionamento pericoloso trascurare la tutela dei propri dati personali partendo dal presupposto che non avrebbero valore agli occhi di un potenziale aggressore: dal momento in cui questi dati hanno un valore (anche sentimentale) per l'utente diventano preziosi anche per un potenziale ricattatore.

In futuro i criminali che applicano questi metodi estorsivi potranno esplorare nuovi orizzonti. Un esempio recente evidenzia le possibilità a disposizione degli hacker di prendere di mira siti Web poco sicuri. In questo caso[61] il modus operandi consiste nel crittografare la banca dati del sito per poi chiedere un riscatto all'amministratore che ne desidera recuperare l'accesso bloccato. Un'altra prospettiva inquietante è legata allo sviluppo dell'Internet delle cose (*Internet of things*) e all'interconnessione in crescita esponenziale dei dispositivi che sembrano offrire ai potenziali criminali infinite possibilità di ricatto. Ogni sistema di controllo

[60] http://www.kent.ac.uk/news/science/528/cryptolocker-victims-pay-out (stato: 28 febbraio 2015).

[61] https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html (stato: 28 febbraio 2015).

domestico, ogni strumento o apparecchiatura collegata a Internet è di fatto vulnerabile. Sono assolutamente immaginabili scenari in cui i criminali rendono inutilizzabile un elettrodomestico per ricattare l'utente che desidera poterlo utilizzare di nuovo. Se in molti casi la vittima potrebbe sbloccare da sé l'apparecchio o azionarlo fisicamente, il disagio arrecato e le mancate conoscenze tecniche potrebbero comunque indurre numerose vittime a pagare, in particolare se le somme richieste non sono elevate.

Questi esempi recenti, nonché le prospettive suggerite, evidenziano quanto sia importante non trascurare gli attacchi opportunistici. Tra gli elementi del modello classico «riservatezza - integrità - disponibilità», spesso tendiamo a privilegiare la riservatezza, pensando agli attacchi attuali, ma anche in sede di analisi di nuovi prodotti o servizi. Occorre tener presente che attaccare la disponibilità di dati o servizi è un'attività molto redditizia per i criminali, specialmente se l'utente è selezionato a monte. Questo aspetto già molto attuale per i diversi tipi di ransomware in circolazione, ha un grosso potenziale di sviluppo legato alla crescente interconnessione di servizi e dispositivi. In questo senso, le preoccupazioni relative agli stessi non devono focalizzarsi unicamente sul problema dei dati personali dell'utente che possono essere sottratti e usati, ma anche sulla possibilità di bloccare o rendere inaccessibili questi servizi a scopi estorsivi.

5.4 Navigazione satellitare nella navigazione aerea

Il *Global Positioning System (GPS)* è un sistema globale di navigazione satellitare per la determinazione della posizione e per il cronometraggio. Con un apparecchio ricevente è possibile rilevare in ogni momento i gradi di longitudine e latitudine della propria posizione. Oggi i ricevitori GPS si trovano praticamente ovunque: sugli smartphone, sulle macchine fotografiche digitali e persino sulle automobili. La navigazione satellitare viene viepiù implementata in applicazioni importanti in ambito di sicurezza.

Un esempio in quest'ambito è quello dell'aviazione civile. Il 17 febbraio 2011 l'Ufficio federale dell'aviazione civile (UFAC) ha autorizzato per la prima volta in Svizzera una procedura di volo di avvicinamento con supporto satellitare sulla pista Nord 14 dell'aeroporto di Zurigo[62]. Il 18 ottobre 2012 la società di gestione dell'aeroporto e la società per il controllo della navigazione aerea Skyguide hanno guidato un decollo con supporto satellitare sulla pista 34. Per la prima volta in Svizzera è stata applicata una procedura di decollo con un raggio predefinito della virata di volo. Il 14 ottobre 2014 è atterrato all'aeroporto di Zurigo[63] il primo aereo Swiss mediante sistema di avvicinamento di precisione con supporto satellitare. Si procederà tuttavia al potenziamento dell'intera flotta soltanto quando la procedura di volo di avvicinamento con supporto satellitare potrà essere applicata nella maggioranza degli aeroporti.

Non si deve dimenticare che la navigazione satellitare non è stata sviluppata per un impiego specifico nell'aviazione civile e che può essere disturbata leggermente intenzionalmente o meno. Ricorderemo il caso delle perturbazioni del sistema GPS all'aeroporto di Newark. Dopo mesi di ricerche ininterrotte si scoprì che tali perturbazioni erano prodotte da un conducente di autocarri che viaggiava regolarmente ad alta velocità nei pressi dell'aeroporto ed era munito di «*GPS jammer*».

---

62 Rapporto semestrale MELANI 2011/1, capitolo 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=it (stato: 28 febbraio 2015).

63 http://www.swiss.com/corporate/de/medien/newsroom/medienmitteilungen/medienmitteilung20141015 (stato: 28 febbraio 2015).

I segnali GPS attuali non possono pertanto essere utilizzati da soli. È necessario un sistema ausiliario che sorveglia l'integrità dei dati e ha lo scopo di rilevare guasti e manipolazioni. Inoltre, il grado di esattezza del segnale GPS normale, che ammette un margine di precisione compreso tra 9–17 metri, è troppo poco accurato per voli di avvicinamento di precisione. Influssi esterni come radiazioni ionizzanti, ma anche i cambiamenti dei satelliti GPS possono causare deviazioni. Il sistema ausiliario impiegato a Zurigo si chiama *Ground Based Augmentation System (GBAS)*, in italiano sistema di incremento satellitare. Con quattro stazioni di riferimento di cui è nota la posizione assoluta, è possibile calcolare la cosiddetta correzione differenziale rispetto al «GPS standard». Ciò corrisponde al margine di errore del segnale GPS attuale che viene successivamente trasmesso per radio all'aereo[64]. Deve essere prestata un'attenzione speciale per garantire la sicurezza della trasmissione della correzione differenziale in termini di integrità.

In Europa viene impiegato anche un altro sistema di navigazione aerea: *lo European Geostationary Navigation Overlay Service (EGNOS)*[65]. Anche in questo caso punti di riferimento distribuiti in Europa contribuiscono a migliorare il grado di precisione delle misurazioni e a verificare l'integrità del segnale GPS. Se il sistema GPS invia dati errati, il sistema se ne accorge entro sei secondi e ne informa il pilota. La correzione differenziale è trasmessa agli aerei attraverso satelliti geostazionari. Il segnale viene diffuso anche via Internet. I ricevitori GPS esistenti sono in grado di captare il segnale e di valutarlo. Il margine di errore è inferiore a 10 metri. EGNOS è un progetto comune dell'Agenzia spaziale europea, dell'UE e dell'organizzazione europea per la sicurezza del traffico aereo Eurocontrol ed è considerato il precursore del sistema europeo di navigazione satellitare Galileo. È più economico rispetto al GBAS, poiché non richiede un sistema ausiliario a terra. Oltre ad essere più preciso rispetto al GPS, che è gestito da Stati non europei, si distingue da questo per essere controllato dai suddetti gestori e perché la qualità del suo segnale può essere sorvegliata costantemente.

EGNOS trasmette il segnale di correzione, che è disponibile pubblicamente, agli aerei tramite un satellite geostazionario. EGNOS è semplicemente un ampliamento e un perfezionamento del segnale GPS attuale. Come per il GPS, una manipolazione del segnale sarebbe difficile ma, come per tutti i sistemi tecnici, non completamente esclusa. La sua sicurezza dipende dai singoli componenti e dai loro produttori. La sicurezza in questo settore è di importanza cruciale. Le aziende che forniscono i componenti per EGNOS devono soddisfare requisiti di sicurezza speciali. Le aziende svizzere che desiderano partecipare al programma Galileo ed EGNOS sono pertanto sottoposte alla verifica di esperti di sicurezza del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS).[66]

I moderni sistemi TIC destano sempre nuove aspettative anche in ambiti nei quali la sicurezza è di primaria importanza. In molti casi si tratta della modernizzazione, ma anche dell'implementazione di sistemi che possono essere gestiti con maggiore efficienza e un minore impatto ambientale. Nell'analisi del rischio, la maggiore efficienza auspicata deve essere tuttavia soppesata con considerazioni legate alla sicurezza. I sistemi TIC possono costituire invece un prezioso complemento a sistemi di sicurezza obsoleti. La sfida legata

64 http://www.skyguide.ch/fileadmin/user_upload/publications/Factsheets/1201_Factsheet_Satellitennav_System e_Verfahren_de.pdf (stato: 28 febbraio 2015).

65 http://www.esa.int/Our_Activities/Navigation/The_present_-_EGNOS/What_is_EGNOS (stato: 28 febbraio 2015).

66 https://www.news.admin.ch/message/index.html?lang=it&msg-id=53264 (stato: 28 febbraio 2015).

all'impiego di tali sistemi non consiste solo nel garantire l'integrità dei dati trasmessi, ma anche la disponibilità dei sistemi. Una perturbazione del segnale GPS costringe gli aerei in fase di avvicinamento a procedere all'atterraggio con sistemi alternativi. Questo non è un problema finché le apparecchiature di terra utilizzate dai vari sistemi rimangono le stesse o quando sussistono sistemi alternativi come il sistema di atterraggio strumentale (ILS). Nel caso di sistemi di atterraggio propri di un determinato scalo, come per l'ILS, eventuali perturbazioni saranno circoscritte a detto aeroporto. Un guasto di EGNOS avrebbe invece ripercussioni sul traffico aereo di tutta l'area europea.

5.5 Falle di sicurezza – responsible disclosure

Gli utenti di Internet sono costantemente esposti direttamente o indirettamente a qualche falla di sicurezza. All'utente medio sono note soprattutto le falle dei prodotti Microsoft nonché Acrobat-Reader e Flash-Player. Allo stesso modo, fanno sempre notizia le vulnerabilità in materia di sicurezza e crittografia rilevate nei componenti. L'esempio più noto è la falla di sicurezza (*vulnerability)* Heartbleed descritta nel precedente rapporto semestrale. Per il periodo in esame, si devono segnalare le falle Poodle e Kerberos (si veda in merito il capitolo 4.9). La banca dati gestita dalla ditta MITRE, che censisce tutte le vulnerabilità dei programmi pubblicamente note, nel 2014 ha registrato un totale senza precedenti di 7945 falle di sicurezza in tutto il mondo[67]. La gamma delle vulnerabilità è però molto più ampia e spazia da siti Web vulnerabili a configurazioni errate, che non sono elencate in questa banca dati. Si presume che praticamente tutti i software impiegati presentino qualche lacuna. Data la tendenza, è viepiù urgente affrontare la questione dei processi per gestire le falle di sicurezza riscontrate.

Ad esempio, la maggior parte degli utenti di Internet ritiene che chi trova le informazioni le metta (gratuitamente) a disposizione delle aziende interessate affinché queste, a loro volta, rilascino un aggiornamento il più rapidamente possibile. Il Security Business è però un mercato molto conteso e la gestione delle informazioni relative alla sicurezza è sempre un esercizio di equilibrismo. Gli interessi in gioco sono molti, ovviamente anche di natura finanziaria. Scoprire una lacuna comporta un certo vantaggio finanziario: lo scopritore ha pur sempre assunto un ruolo che dovrebbe essere assunto dall'azienda produttrice nel quadro della garanzia di qualità. Si ritiene che diverse aziende esplorino attivamente programmi in maniera mirata alla ricerca di falle di sicurezza per trarne profitto. Nel 2012 ha fatto scalpore il caso della società maltese ReVuln che si è specializzata nell'individuazione di falle di sicurezza sconosciute in prodotti SCADA con l'intento non di farne parte ai produttori, bensì di venderle a governi e altri «clienti paganti»[68]. Proprio nel settore delle infrastrutture critiche questo può rivelarsi un'attività lucrativa in quanto è particolarmente forte la pressione affinché tutto funzioni senza problemi e i governi hanno l'obbligo garantire la sicurezza di questi sistemi critici. Questa commercializzazione comporta tuttavia un doppio rischio: da un lato, alcune falle di sicurezza potrebbero non essere rimosse per ragioni di costi e dall'altro, criminali in grado di pagare potrebbero venire a conoscenza dell'esistenza di una vulnerabilità sfruttabile. Anche il commercio delle vulnerabilità da parte dei governi comporta dei rischi, che sono noti sin da prima della pubblicazione dei documenti di Snowden. Già nel 2012, Chaouki Bekrarder, CEO e hacker principale della ditta VUPEN, aveva affermato nel corso di un'intervista che la sua impresa non avrebbe venduto a Google, per un milione di

[67] http://cvedetails.com/browse-by-date.php (stato: 28 febbraio 2015).

[68] http://www.computerworld.com/article/2493333/malware-vulnerabilities/security-firm-finds-scada-software-flaws--won-t-report-them-to-vendors.html (stato: 28 febbraio 2015).

dollari, le falle di sicurezza riscontrate nel browser Google Chrome, bensì ai suoi clienti, segnatamente a partner e a governi facenti parte della NATO[69].

D'altro canto, alcune falle di sicurezza non considerate seriamente dai produttori, con la frustrazione di che le ha scoperte. Finché la falla non è nota pubblicamente, determinati produttori non vedono il motivo di rimuoverla in tempo utile. Si sono verificate regolarmente situazioni in cui è emerso a posteriori che un produttore era al corrente di una determinata lacuna già mesi prima che fosse divulgata pubblicamente, ma aveva trascurato di cercare seriamente un rimedio in questo lasso di tempo, con una certa frustrazione per chi l'aveva individuata che, per esercitare una pressione maggiore, minaccia di rivelare la falla in un determinato momento, costringendo il produttore ad agire tempestivamente. Nella peggiore delle ipotesi, la falla di sicurezza è divulgata prima che sia disponibile un aggiornamento.

Se il primo problema può essere risolto – sempre che sia possibile farlo - soltanto attraverso l'intervento del legislatore statale, il secondo è assolutamente risolvibile. Per esempio il National Cyber Security Center dei Paesi Bassi ha pubblicato un decalogo per insegnare agli informatori e alle vittime a gestire le falle di sicurezza. Il Security Center funge da centrale d'annuncio delle vulnerabilità individuate. Si vuole incoraggiare l'informatore a diffondere le informazioni. In tal senso, gli viene assicurato che entro tre giorni lavorativi sarà valutata la gravità del rapporto sulla vulnerabilità e che sarà indicato entro quanto tempo sarà possibile porvi rimedio. Inoltre, l'informatore viene costantemente aggiornato sui progressi effettuati verso la soluzione del problema. Al momento della pubblicazione, oltre a un encomio, l'informatore riceve una o più magliette di ringraziamento[70].

69 http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/ (stato: 28 febbraio 2015).

70 https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html (stato: 28 febbraio 2015).

5.6 Atti parlamentari

Atto parlamentare	Numero	Titolo	Depositato da	Data del deposito	CN/CS	Ufficio	Stato delle deliberazioni & link
Postulato	14.3739	Control by design. Potenziare i diritti di proprietà per impedire le connessioni indesiderate	Schwaab Jean Christophe	17.09.2014	CN	DFGP	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20143739
Postulato	14.3782	Regole per la «morte digitale»	Schwaab Jean Christophe	24.09.2014	CN	DFGD	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20143782
Interpellanza	14.3884	Intenzioni di vendita di quote Swissgrid	Killer Hans	25.09.2014	CN	DATEC	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20143884
Domanda	14.5642	Internetdiensleistungen. Aufspaltung dominierender Konzerne bei Quasi-Monopolen	Glättli Balthasar	03.12.2014	CN	DEFR	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20145642
Interpellanza	14.4138	Prassi in materia di acquisti pubblici nel settore delle infrastrutture TIC critiche dell'amministrazione federale	Noser Ruedi	10.12.2014	CN	DFF	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20144138
Interpellanza	14.4123	Sviluppo dell'infrastruttura delle TIC. Creare condizioni quadro più favorevoli agli investimenti	Guhl Bernhard	10.12.2014	CN	DATEC	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20144123
Interpellanza	14.4194	Megadati. Potenziale e prospettive di sviluppo dell'industria dei dati in Svizzera	Graf-Litscher Edith	11.12.2014	CN	DFI	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20144194
Postulato	14.4294	Indice web per un Internet libero e aperto. La Svizzera figura solo al 18º posto	Glättli Balthasar	12.12.2014	CN	DATEC	http://www.parlament.ch/i/suche/Pagine/geschaefte.aspx?gesch_id=20144294

6 Glossario

0-day Exploits	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
Active Directory	Active Directory (AD) è il nome del servizio directory di Microsoft e di Microsoft Windows Server.
Advanced Persistent Threat	Questa minaccia provoca un danno molto ingente, che si ripercuote sulla singola organizzazione o su un Paese. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di notevoli risorse.
Attacco DDoS	Attacco Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Autentificazione a due fattori	A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. passwort, PIN ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.)
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezione di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.
Backup	Backup (in italiano: salvaguardia dei dati) designa la copia di dati nell'intento di poterli ricopiare in caso di perdita.
Black Hat Search Engine Optimization (BHSEO)	L'ottimizzazione del motore di ricerca, o «*search engine optimization*» in inglese, è il termine che si applica agli interventi che servono ad attribuire a determinati siti Web un posizionamento più elevato nella classificazione dei motori di ricerca. Quando questi applicano una metodologia che non è accettata, l'ottimizzazione viene denominata «Black Hat».
Bluetooth	Una tecnologia che consente la comunicazione senza fili tra due apparecchi finali e utilizzata soprattutto in ambito di

	telefonia mobile, di laptop, di PDA e di dispositivi di immissione (ad es. il mouse del computer).
Brute force	Il metodo brute force è un algoritmo di risoluzione di un problema che consiste nel verificare tutte le combinazioni teoricamente possibili fino a trovare quella effettivamente corretta.
Byte	Il byte è un'unità di misura delle tecnologie digitali e dell'informatica solitamente composto da una sequenza di 8 bit.
Classificazione da parte dei motori di ricerca	Successione di diversi oggetti comparabili dopo la richiesta di un motore di ricerca, classificati secondo criteri di valutazione
Cloud	Per *cloud computing* si intende la memorizzazione di dati in un centro di calcolo remoto, ma anche l'esecuzione di programmi che non sono installati su un computer locale.
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
Content Management Systeme (CMS)	Un «Content Management System» (acronimo CMS, in italiano «sistema di gestione dei contenuti») è un sistema che rende possibile e organizza la produzione e l'elaborazione comune di contenuti, consistenti in documenti di testo e multimediali, in genere destinati al World Wide Web. Un autore può servirsi di un simile sistema anche senza conoscenze di programmazione o di HTML. In questo caso il contenuto informativo da presentare è detto «content» (contenuto).
Cookie	Piccolo file di testo depositato sul computer dell'utente alla visita di una pagina Web. Con l'ausilio dei cookies è per esempio possibile salvaguardare le impostazioni personali di una pagina Internet. Essi possono però anche essere sfruttati in modo abusivo per registrare le abitudini di navigazione dell'utente e allestire in tale modo un profilo di utente.
Deturpamento di sito Web (defacement)	Modifica non autorizzata di una pagina Web.

Dirottamento di sessione	Il dirottamento di sessione (*session hijacking*) consiste nell'assunzione del controllo di un collegamento attivo tra client e server da parte di un terzo non autorizzato.
Ethernet	Ethernet è una tecnologia che specifica software e hardware per reti di dati collegate con cavi.
Exploit kit	kit che consente a criminali di generare programmi, script o righe di codice mediante i quali è possibile sfruttare le vulnerabilità dei sistemi di computer.
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere – ossia sul vostro computer.
Firma	La firma (signing) consente di accertare l'integrità del messaggio mediante una chiave pubblica di verifica (public key).
Firmware	Dati di comando per il controllo di un apparecchio (ad es. scanner, carte grafiche ecc.), memorizzati in un chip. Questi dati possono di norma essere modificati per il tramite di Upgrades (aggiornamenti).
Gateway di sicurezza	Un gateway di sicurezza è un termine generico che comprende tutti i sistemi TIC che provvedono alla sicurezza TIC di un'organizzazione.
Global Positioning System (GPS)	Il Global Positioning System (GPS), ufficialmente NAVSTAR GPS, è un sistema globale di navigazio-ne satellitare per la determinazione della posizione e la misura del tempo.
Global System for Mobile Communications (GSM)	(già Groupe Spécial Mobile, GSM) Standard delle reti di telefonia mobile integralmente digitali, utilizzato prevalentemente nella telefonia, ma anche per la trasmissione di dati per multiplex o per pacchetti, come pure per la messaggeria breve (short messages).
GPS-Jammer	Apparecchiatura per perturbare i dati GPS.

Infezione da «drive-by-download»	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo scopo di diffondere il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
International Mobile Subscriber Identity (IMSI)	L'International Mobile Subscriber Identity serve a identificare in modo univoco gli utenti delle reti di telefonia mobile GSM e UMTS.
Jailbreak	Con il termine jailbreaking (dall'inglese evasione dalla prigione) si intende il superamento delle limitazioni di uso dei prodotti Apple per il tramite di un apposito software.
Keylogger	Apparecchi o programmi intercalati tra il computer e la tastiera per registrare i dati immessi sulla tastiera.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Malicious Code	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Toia, nonché le Logic Bombs.
Man in the Middle	Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in grado di seguire o di modificare lo scambio di dati.
Message Authentication Code (MAC)	Un Message Authentication Code serve a comprovare l'integrità di dati o messaggi.
Near Field Communication (NFC)	La Near Field Communication è uno standard di tra-smissione secondo gli standard internazionali per lo scambio senza contatto di dati su corte distanze.
Network Attached Storage (NAS)	Un dispositivo NAS è un server di file facile da amministrare.
Pagine di social-network	Pagine Web sulle quali gli utenti si scambiano profili appositamente strutturati. Sovente si comunicano dati personali come nome, data di nascita, immagini, interessi

	professionali e attività del tempo libero.
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato.
Plug-in	Un software di complemento che amplia le funzioni di base di un'applicazione. Esempio: i Plug-In di Acrobat per i browser di Internet consentono la visualizzazione diretta di file PDF.
Point of Sales	Un terminale POS (in Svizzera terminale EFT/POS) è un terminale online per il pagamento senza contanti presso un punto di vendita («point of sale»).
Proof of concept (POC)	Una prova succinta, ma non necessariamente completa, del funzionamento di un'idea o di un metodo. Sovente i codici Exploit sono pubblicati sotto forma di PoC per sottolineare le ripercussioni di una lacuna.
Protocollo di rete	Un protocollo di rete è un protocollo di comunicazione per lo scambio di dati tra computer di una stessa rete.
Provider upstream	Un provider upstream mette a disposizione di un fornitore di servizi Internet (Internet Service provider o ISP) collegamenti a Internet che l'ISP stesso non possiede.
Ram Scraping	Il malware in questione riesce a copiare i dati conte-nuti nella striscia magnetica della carta negli istanti che seguono la sua utilizzazione sul ter-minale di pagamento, quando essi sono disponibili in chiaro nella memoria ad accesso ca-suale (RAM)
Ransomware	Malware tramite il quale i proprietari dei computer infettati sono ricattati (ransom: termine inglese per riscatto). Nel caso tipico i dati sono cifrati e nuovamente messi a disposizione dall'aggressore dopo il pagamento del riscatto per la chiave di

	decodificazione necessaria al loro ripristino.
Rete bot	Un insieme di computer infettati da Malicious Bot. Essi possono essere interamente comandati a distanza da un aggressore (il proprietario della rete bot). A seconda delle dimensioni, una rete può constare di poche centinaia fino a milioni di elaboratori infettati.
Rich Text Format	Rich Text Format (RTF) è un formato di file per testi.
Richiesta (request)	Domanda di un client rivolta a un server in un modello client/server
Roaming	Il roaming GSM è la capacità di un utente di una rete di telefonia mobile di accedere ai servizi di telefonia di una rete estera.
Router	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Servizio di anonimizzazione Tor	Tor è una rete di anonimizzazione di dati di collegamento. Tutela i suoi utenti dall'analisi del traffico di dati.
Sessione	Una sessione (session) designa un collegamento attivo tra client e server.
Short Message Service (SMS)	Short Message Service Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Smartphones	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
Social Engineering	Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni.
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di

	massa, definizione nella quale rientrano anche gli e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
Spear-Phishing	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L'aggressore tenta di introdurre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
SSL	Secure Sockets Layer Un protocollo di comunicazione sicura in Internet. Attualmente lo SSL viene ad esempio utilizzato in ambito di transazioni finanziarie online.
Supporto di dati rimovibile	Supporto dati per computer non incorporato, sostituibile, solitamente portatile
Traboccamento della memoria tampone (Buffer overflow)	Le più frequenti lacune di sicurezza del software attuale che possono tra l'altro essere sfruttate via Internet.
Universal Mobile Telecommunications System (UMTS)	Universal Mobile Telecommunications System (UMTS) è uno standard di telefonia mobile di terza generazione per lo scambio di dati.
Universal Serial Bus seriale (USB)	Universal Serial Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo).
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.