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 2015/I (gennaio – giugno)

29 OTTOBRE 2015

CENTRALE D'ANNUNCIO E D'ANALISI PER LA SICUREZZA DELL'INFORMAZIONE
http://www.melani.admin.ch

1 Indice / Sintesi

2 Editoriale

Pascal Lamia, 48 anni, dirige dal 2008 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Care lettrici, cari lettori,

il 1° ottobre 2014 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha celebrato il decimo anniversario della sua costituzione. Negli ultimi dieci anni ci sono stati annunciati innumerevoli casi. Dal normale tentativo di frode agli attacchi di spionaggio, MELANI vanta ormai una vasta esperienza. Dal 2004 numerosi operatori di infrastrutture critiche hanno potuto beneficiare del nostro sostegno nei settori della prevenzione e della gestione degli attacchi cibernetici.

MELANI deve il proprio successo in primo luogo all'economia privata. Senza una «public private partnership» estremamente ben funzionante, ossia senza una cooperazione di successo tra la Confederazione e l'economia privata, MELANI non avrebbe infatti mai potuto assumere l'importanza che riveste oggi. Desidero pertanto ringraziare sentitamente tutte le persone dell'amministrazione e dell'economia privata che negli ultimi dieci anni hanno trasformato MELANI in ciò che è oggi.

Abbiamo voluto sfruttare l'inizio della seconda decade di attività di MELANI per far realizzare un nuovo logo. Esso simboleggia da un lato i flussi di dati digitali nel mondo e riproduce dall'altro le interconnessioni esistenti a livello internazionale. Senza un network personale di organizzazioni partner ubicate in tutto il mondo, oggi sarebbe impossibile fronteggiare con successo le minacce cibernetiche.

Anche questo rapporto semestrale rappresenta un passo avanti nella seconda decade di attività di MELANI: è stato infatti completamente rielaborato sotto il profilo strutturale allo scopo di renderne ancora più semplice e gradevole la consultazione.

Auguro a tutti una piacevole lettura.

Pascal Lamia

3 Tema principale: la sicurezza dei siti Web

Negli ultimi 15 anni Internet ha registrato una crescita significativa. Ogni giorno vengono messe online migliaia di nuovi siti Web. Secondo Netcraft[1] attualmente vi sarebbero oltre 850 milioni di siti Web attivi. Uno dei motivi del forte incremento del numero di siti Web risiede molto probabilmente nell'impiego di *Content Management System (CMS)* quali ad esempio «WordPress», «Typo3», «Joomla» e «Drupal». Grazie a un CMS gli utenti di Internet possono pubblicare molto facilmente contenuti in rete senza disporre di conoscenze approfondite delle TIC. Sono inoltre disponibili numerosi *plug-in* che consentono di adeguare un sito Web alle proprie esigenze. Grazie alla loro semplicità d'uso i CMS vengono utilizzati di frequente anche da webmaster amatoriali e da piccole e medie imprese (PMI) per pubblicare le proprie informazioni su Internet.
Se da un lato un CMS può risultare estremamente pratico, dall'altro esso costituisce un obiettivo allettante per gli hacker. Gran parte delle pagine di *phishing* e delle *infezioni da drive-by* vengono installate su siti Web amministrati con CMS non aggiornati. Come in molti programmi, anche nel caso dei CMS vengono regolarmente riscontrate falle di sicurezza per le quali il rispettivo produttore mette in genere a disposizione tempestivamente opportuni aggiornamenti. Nel 2014, ad esempio, sono state rilevate ed eliminate 14 falle nel solo caso del software CMS Drupal, nove nel caso di Joomla! e addirittura 29 nel caso di WordPress[2].
Su Internet i siti Web realizzati con una versione di un CMS vulnerabile possono essere individuati e attaccati in modo automatizzato. Per i criminali è dunque relativamente facile individuare un gran numero di siti Web vulnerabili e manipolarli. Per ogni operatore di siti Web sarebbe quindi essenziale un aggiornamento regolare (patching) del software CMS , ciò nonostante, in molti casi viene dedicata troppa poca attenzione a questo aspetto. Attraverso l'impiego di CMS obsoleti (e poco sicuri) i gestori di siti Web non mettono a rischio soltanto altri utenti di Internet ma anche sé stessi: nella prima metà del 2015 sono stati annunciati a MELANI diversi casi in cui erano stati compromessi CMS obsoleti. I dati contenuti nel CMS erano stati copiati e utilizzati in seguito per ricattarne i proprietari. In questo caso esiste un rischio soprattutto per le PMI, poiché in molti CMS sono salvati anche dati dei clienti.
Generalmente, gli aggiornamenti di sicurezza per i CMS vengono messi a disposizione rapidamente dai produttori. A differenza della maggior parte dei sistemi operativi, l'aggiornamento non avviene però in modo automatico ma deve spesso essere avviato manualmente dall'operatore. Purtroppo la maggioranza degli operatori di siti Web che utilizzano un CMS per il proprio sito lo installano una prima volta e poi continuano per anni a gestire la pagina con la stessa versione di CMS (generalmente obsoleta e poco sicura). Gli esempi di vulnerabilità illustrati di seguito per WordPress, che possono essere estesi a tutti gli altri CMS, chiariscono meglio questo tipo di comportamento.

Il 70 per cento delle installazioni di WordPress in Svizzera è vulnerabile

Nell'aprile del 2015 è emersa una falla in WordPress che ha consentito a un hacker di sferrare un *attacco di Cross Site Scripting (XSS)* contro ogni sito Web vulnerabile, attraverso la redazione di un commento con un *JavaScript* preparato a questo scopo sul sito in questione (CVE-2015-3429). Nonostante WordPress abbia pubblicato il giorno stesso un aggiornamento di sicurezza per rimuovere la vulnerabilità, già il 6 maggio 2015 è emersa una seconda falla che ha consentito a un hacker di sferrare un ulteriore attacco di cross site scripting (XSS) contro WordPress (CVE-2015-3440). Anche in questo caso WordPress ha reagito prontamente pubblicando un aggiornamento di sicurezza il giorno seguente.

[1] http://news.netcraft.com/archives/2015/08/13/august-2015-web-server-survey.html (stato: 31 agosto 2015).
[2] https://cve.mitre.org (stato: 31 agosto 2015)

La velocità di reazione degli operatori interessati è stata tuttavia spaventosamente lenta. Ad esempio, del 6% di siti Web svizzeri che è gestito con WordPress, oltre il 70% dei siti Web è rimasto vulnerabile, nonostante la disponibilità degli aggiornamenti di sicurezza.[3]

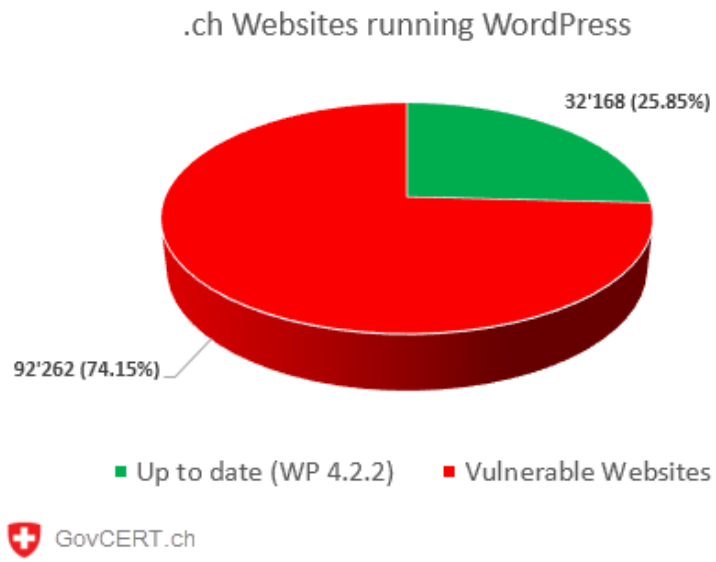


Figura 1: Utenti di WordPress ancora vulnerabili nei confronti delle falle di sicurezza CVE-2015-3440 e CVE-2015-3429 (in rosso) due mesi dopo la pubblicazone del patch.

Aggiornamenti regolari – necessari, ma non sufficienti!

Le conclusioni tratte dall'analisi condotta da MELANI preoccupano e inducono a interrogarsi sul perché tanti operatori di siti Web impieghino versioni vulnerabili dei CMS. Una possibile spiegazione potrebbe risiedere, in una certa misura, oltre che nella scarsa sensibilità e nella mancanza di tempo, anche nella comodità. Molti di loro non riconoscono la necessità di effettuare il *patching* del loro CMS o non sono consapevoli delle conseguenze che le installazioni di CMS vulnerabili potrebbero avere. L'utilizzo di un CMS comporta però sempre anche una certa responsabilità che occorre assumersi. Oltre a un *patch management* tempestivo esistono anche altre misure in grado di aumentare la sicurezza dei sistemi CMS:

- **Autenticazione a due fattori**

  Oltre all'autenticazione abituale (nome di utilizzatore e password) per l'accesso all'interfaccia di amministrazione, MELANI consiglia l'implementazione di un'autenticazione a due fattori. La password unica (anche chiamata *OTP, One Time Password*) può essere aggiunta attraverso per esempio « Google Authenticator ». Per poterlo utilizzare bisogna installare un'applicazione sul proprio smartphone (Android, iOS, Blackberry), la quale ogni 30 secondi genera una nuova OTP. Sul webserver (CMS) si deve installare un plug-in specifico : diversi sistemi di Content Management, come WordPress o Typo3, dispongono di tale *plug-in*.

[3] Blog postato su GovCERT.ch: «Outdate WordPress: Thousands of websites in Switzerland are vulnerable» http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable (stato: 31 agosto 2015)

- **Limitazione degli accessi di amministratore a determinati indirizzi IP**

  Una simile limitazione può basarsi su *indirizzi IP* precisi, su intervalli di indirizzi IP oppure sulla *geolocalizzazione* di un IP. Per diversi CMS esistono già dei plug-in specifici .

- **Limitazione degli accessi di amministratore mediante file .htaccess**

  Questo permette non solo di limitare l'accesso attraverso un intervallo di indirizzi IP ma anche di aggiungere un'autenticazione supplementare (nome utilizzatore e *password).*

- **Messa in sicurezza del computer del Webmaster**

  I siti web e i CMS sono spesso compromessi attraverso il furto dei dati di accesso *FTP*. Questo avviene sovente attraverso l'uso di un cavallo di Troia installato sul computer del webmaster. È quindi compito di quest'ultimo garantire la sicurezza del proprio computer e utilizzare un programma antivirus aggiornato. Si consiglia inoltre, quando possibile, di utilizzare una comunicazione FTP criptata (sFTP).

- **Web Application Firewall**

  Gli attacchi provenienti dal web posso essere bloccati con l'aiuto di un «Web Application Firewall» (WAF), prima che l'attacco stesso possa raggiungere l'applicazione presa di mira. Ci sono diverse soluzioni WAF. La più conosciuta nel mondo open source è «ModSecurity».

- **Individuazione tempestiva delle lacune di sicurezza**

  Lo scopo è quello di identificare le lacune di sicurezza potenziali prima che lo facciano i criminali. Diverse soluzioni, a pagamento o gratuite, sono disponibili sul mercato.

La lista di controllo e le istruzioni complete sono disponibili sul sito Web www.melani.admin.ch:

Misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti (CMS):

https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

Qui trovate inoltre delle istruzioni e una lista di controllo per il comportamento da tenere quando l'attacco è già avvenuto:

https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/anleitung-webseitenbereinigung.html

4 La situazione a livello nazionale

4.1 Spionaggio

Nel primo semestre si sono verificati in particolare due casi di spionaggio che hanno suscitato l'interesse del pubblico e in cui la Svizzera è stata direttamente o indirettamente coinvolta. A questo proposito occorre distinguere i casi in cui l'attacco riguarda un particolare obiettivo in Svizzera da quelli in cui vengono utilizzate infrastrutture svizzere come base per attività di spionaggio nei confronti di terzi. Va da sé che nel settore dello spionaggio non vengono resi pubblici tutti i casi rilevati. Quando si parla di spionaggio economico, tipicamente le aziende sono molto riservate, poiché temono un danno di immagine. In generale è possibile affermare che esiste un interesse costante e, di conseguenza, una costante pressione sui dati sensibili. Un caso di particolare rilievo nel primo semestre del 2015 è quello riguardante la scoperta e la pubblicazione di un malware di nome «Duqu2» che sembra essere stato attivo soprattutto nel contesto dei dibattiti sul programma nucleare con l'Iran.

4.1.1 Duqu *reloaded*: un software di spionaggio altamente sofisticato contro i partecipanti ai negoziati sul nucleare

Nel marzo del 2015 il Wall Street Journal, basandosi su fonti della Casa Bianca, aveva parlato di un'intercettazione di dibattiti interni agli USA relativi all'accordo sul nucleare con l'Iran. In quel caso gli USA avevano sospettato che l'autore potesse essere Israele. [4,5] Alcuni politici israeliani hanno tuttavia smentito prontamente e con decisione un possibile coinvolgimento di Israele. Il 10 giugno 2015 la società di servizi di sicurezza IT Kaspersky ha reso noto in un rapporto che, sia il fornitore di servizi di sicurezza stesso, sia alcuni luoghi dove si sono svolti i colloqui relativi ai negoziati sul nucleare con l'Iran, erano oggetto di un attacco di spionaggio attuato grazie all'impiego di malware. La programmazione del malware presenta aspetti peculiari «molto simili o addirittura quasi identici»[6] a quelli del malware Duqu divenuto noto nel 2011 e presenta inoltre delle analogie con il malware Stuxnet. Per questo motivo Kaspersky ha battezzato il malware «Duqu2». Come in quasi tutti i casi di spionaggio, gli schemi d'attacco non consentono di trarre conclusioni univoche riguardo ai possibili autori.

Nei casi scoperti, gli obiettivi erano costituiti, tra l'altro, dalle celebrazioni per il 70° anniversario della liberazione del campo di concentramento di Auschwitz-Birkenau e dai negoziati con il P5+1 sul programma nucleare iraniano. Esperti informatici hanno rilevato la presenza del malware in tre località in cui si stavano svolgendo i negoziati con il P5+1. Gli ultimi round di negoziati si sono svolti a Losanna, Montreux, Ginevra, Monaco di Baviera e Vienna.[7]

Alla luce di alcuni indizi del Servizio delle attività informative della Confederazione (SIC), in Svizzera il Consiglio federale ha autorizzato la Procura pubblica federale, già il 6 maggio 2015[8], ad avviare un procedimento penale contro ignoti per questo caso. Durante la

---

4 http://www.wsj.com/articles/israel-spied-on-iran-talks-1427164201 (stato: 31 agosto 2015)

5 http://www.theguardian.com/world/2015/mar/24/israel-spied-on-us-over-iran-nuclear-talks (stato: 31 agosto 2015)

6 http://www.zeit.de/digital/internet/2015-06/duqu-2-kaspersky-labs (stato: 31 agosto 2015)

7 http://www.kaspersky.com/about/news/virus/2015/Duqu-is-back (stato: 31 agosto 2015)

8 http://www.heise.de/newsticker/meldung/Kaspersky-Trojaner-hatte-auch-Atomverhandlungen-im-Visier-2689929.html (stato: 31 agosto 2015)

perquisizione, operata a metà maggio a Ginevra, sono stati sequestrati diversi apparecchi.[9] Anche in Austria le autorità hanno avviato delle indagini per sospettato spionaggio nell'ambito del caso. In Austria le indagini si sono concentrate sull'hotel viennese «Palais Coburg», dove si erano svolti diversi incontri legati ai negoziati sul nucleare.[10]

Il software di spionaggio non puntava soltanto agli obiettivi veri e propri, ma ha colpito direttamente anche la società di servizi di sicurezza Kaspersky. Apparentemente gli hacker avrebbero perquisito la rete aziendale per cercare di arrivare a dati che avrebbero dovuto facilitare un attacco agli obiettivi. Le aziende che si occupano di sicurezza informatica rappresentano una colonna portante della fiducia di base in Internet. Attacchi sganciati al fine di approfittare di servizi del genere per altri scopi, nuocciono quindi gravemente alla percezione di Internet come strumento degno di fiducia e perciò utilizzabile anche per attività commerciali. Per questo motivo occorrerà quindi discutere delle linee guida per questo settore in futuro.

Per maggiori informazioni sul tema vedi il Rapporto Semestrale MELANI 2013/2, capitolo 5.1
https://www.melani.admin.ch/melani/it/home/dokumentation/berichte/lageberichte/rapporto-semestrale-2013-2.html

4.1.2 Linee Swisscom apparentemente intercettate dal BND e dalla NSA

Secondo le dichiarazioni rese dal deputato austriaco Peter Pilz, il Bundesnachrichtendienst (BND) tedesco e l'americana National Security Agency (NSA), nell'ambito dell'operazione Eikonal[11], avrebbero apparentemente setacciato, in base a determinate parole chiave, i dati di transito nel nodo Internet di Francoforte. L'obiettivo della ricerca consisteva nell'ottenere informazioni relative a persone sospettate di terrorismo e trafficanti di armi. Le parole chiave sono state trasmesse al BND dalla NSA. In questo contesto, nel corso del tempo, sarebbero state peraltro osservate ripetutamente parole chiave strane e non rilevanti per l'argomento, ricollegabili eventualmente solo indirettamente a questa operazione.
Al centro dell'operazione c'erano 250 linee di transito. Tra queste figuravano, secondo un elenco fornito da Pilz, anche nove linee i cui punti terminali in Svizzera erano gestiti da Swisscom e che conducevano rispettivamente a Praga, Sydney, Tokio, Seoul, Lussemburgo, Varsavia e Mosca. La Svizzera sarebbe stata dunque tra i 64 Paesi interessati dalle misure di intercettazione del BND e/o della NSA. Fonte delle affermazioni del deputato tedesco è un contratto tra il BND e Deutsche Telekom pubblicato nel 2004. Tuttavia secondo alcune dichiarazioni di Swisscom, queste linee non sono attualmente più di sua proprietà.[12]

9 http://www.srf.ch/news/international/cyber-spionage-bei-atomkonferenz-in-genf (stato: 31 agosto 2015)
10 http://www.tagesschau.de/ausland/duqu-103.html (stato: 31 agosto 2015)
11 http://www.zeit.de/politik/deutschland/2015-04/bnd-nsa-kooperation-verantwortliche (stato: 31 agosto 2015)
12 http://www.nzz.ch/schweiz/bnd-und-nsa-sollen-swisscom-kunden-ausspioniert-haben-1.18549890 (stato: 31 agosto 2015)

Il Servizio delle attività informative della Confederazione ha pubblicato l'opuscolo «Prophylax», dedicato tra l'altro all'ambito tematico dello spionaggio economico. L'opuscolo fa parte di un'iniziativa di prevenzione e di sensibilizzazione nel campo della non proliferazione e dello spionaggio economico e ha lo scopo di sensibilizzare le aziende e le istituzioni educative. Esso informa inoltre sui rischi e le attività illegali che possono essere scoperte e impedite nonché sugli sforzi di lotta e prevenzione intrapresi dalle autorità.

http://www.vbs.admin.ch/internet/vbs/it/home/documentation/publication/snd_publ.html

4.2 Furto di dati

Il furto di dati in formato elettronico può essere compiuto da attori animati da diverse motivazioni: gli Stati sono interessati ai dati stessi se questi possono procurare loro, ad esempio, un vantaggio di tipo strategico o economico; per i criminali informatici, un furto di dati, può essere invece fonte di un rapido guadagno. Il ricorso all'estorsione è dunque una delle modalità operative maggiormente adottate attualmente. Per poter estorcere del denaro alla loro vittima, i criminali devono disporre di un mezzo di pressione – ed è qui che i dati rubati possono rivelarsi utili per loro. MELANI ha affrontato questa tematica nel precedente rapporto semestrale[13] .

4.2.1 Rex Mundi

Rex Mundi è un attore specializzatosi in questo tipo di modalità operativa. Si è conquistato una certa notorietà dopo aver mietuto numerose vittime, in particolare in Belgio, nel 2014. Nel gennaio 2015 la Svizzera è stata a sua volta colpita con l'attacco a un'azienda nella area romanda. L'attacco è identico sotto ogni profilo a quanto osservato fino a quel momento. Inizialmente è stato sferrato un attacco tramite *iniezione sql* per accedere a una banca di dati. Quest'ultima contiene informazioni raccolte con un modulo di contatto, disponibile sul sito Web della ditta, utilizzato dal pubblico. Si tratta di dati personali (indirizzi, numeri telefonici ecc.) e comunicazioni trasmessi tramite questo modulo. Per non divulgare tali informazioni, i criminali chiedevano il pagamento di un riscatto. Rex Mundi è ben consapevole dei potenziali danni d'immagine che potrebbe causare grazie all'eco suscitato dall'attacco e fa leva su questa minaccia per tentare di estorcere del denaro. Per aumentare le pressioni sull'azienda, Rex Mundi ha utilizzato, come di consueto, Twitter per divulgare l'accaduto, le proprie rivendicazioni e le reazioni della vittima. Poiché la ditta non ha ceduto al ricatto, l'8 gennaio i dati sono stati diffusi tramite un sito Web ospitato sulla rete Tor. Presagendo questa reazione, l'azienda aveva però previdentemente iniziato a contattare i propri clienti per informarli della fuga di informazioni e dei possibili utilizzi che i criminali avrebbero potuto farne, come ad esempio un attacco di *social engineering*.

Oltre al danno d'immagine per l'azienda coinvolta, anche la natura e il valore delle informazioni divulgate possono costituire un problema. Ciò accade chiaramente se tra questi dati figurano informazioni riservate sull'azienda e la sua attività. Ma nel caso di Rex Mundi il problema consiste piuttosto nell'utilizzo che può essere fatto dei dati personali dei clienti, come i tentativi di truffa effettuati grazie al *social engineering*. Il valore di queste informazioni può costituire d'altro canto un'opportunità per monetizzare l'attacco in caso di mancato

[13] MELANI Halbjahresbericht 2014/2, Kapitel 5.3: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (Stand: 31. August 2015)

pagamento da parte dell'azienda. Basti pensare in particolare a una possibile rivendita dei dati sul mercato nero. Più in generale, questo tipo di casi solleva nuovamente la questione della sicurezza dei siti Web pubblici, spesso vettori di diversi tipi di attacchi.

Questo problema è stato spesso discusso da MELANI (cfr. ad esempio il Rapporto semestrale 2014/2, paragrafo 3.5 «CMS – vulnerabilità e sensibilità insufficiente da parte degli amministratori web») e costituisce inoltre l'oggetto del seguente documento:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/misure-per-contribuire-alla-sicurezza-dei-sistemi-di-gestione-de.html

4.3 Sistemi di controllo industriali

Il tema dei sistemi industriali di controllo sta acquistando un'importanza crescente, poiché oggi un numero crescente di processi è controllato tramite le TIC. Rientra in quest'ambito tematico anche *Industria 4.0*, la quarta rivoluzione industriale. Il termine «sistemi industriali di controllo» viene tuttavia utilizzato in senso molto lato e può comprendere praticamente tutto ciò che va dal comando di una centrale atomica sino alla gestione di edifici. In alcune circostanze ciò può creare una certa confusione. Nei capitoli che seguono tratteremo soprattutto sistemi critici. Tra i sistemi caratterizzati da una criticità elevata figurano senz'altro quelli che contribuiscono all'approvvigionamento di energia elettrica.

4.3.1 «Honeypot» centrale idroelettrica – 31 attacchi

Una possibilità per scoprire quanto sono reali i rischi di un attacco consiste nel ricorso ai cosiddetti honeypot. In questo caso vengono messi in Internet, in modo controllato, sistemi che simulano i veri sistemi obiettivo attirando così gli attacchi, senza tuttavia che questi possano arrecare loro danni.

Nel febbraio del 2015 il Sonntagszeitung[14] ha pubblicato uno studio sull'argomento in relazione alle centrali idroelettriche per effettuare il quale era stato installato un sistema che per tre settimane si era spacciato per una centrale idroelettrica. Ne sono risultati 31 attacchi, tre dei quali da parte di hacker che hanno cercato di provocare, rispettivamente, un errore o un crash del sistema. Sebbene si sia trattato di un esperimento modello che, sicuramente non può essere paragonato in ogni aspetto ai sistemi in funzione, tuttavia esso evidenzia l'interesse nutrito dagli hacker nei confronti di questi sistemi. Non è la prima volta che un esperimento ha consentito di dimostrare che è possibile penetrare nei sistemi di controllo di piccole centrali idroelettriche e di illustrare le modalità di questi attacchi. Già due anni fa un rapporto di questo tipo aveva fatto notizia: all'epoca erano bastati 15 minuti per acquisire il controllo su una centrale elettrica nel Canton Glarona. [15] Anche se l'hackeraggio di una piccola centrale elettrica non deve necessariamente avere ripercussioni per la rete elettrica, un attacco ben orchestrato contro numerosi piccoli sistemi potrebbe provocare improvvise oscillazioni della corrente elettrica e causare quindi possibili reazioni a catena, fino a portare a un blackout su vasta scala.

[14] http://www.sonntagszeitung.ch/read/sz_08_02_2015/nachrichten/Angriff-auf-die-Stromversorgung-27051 (stato: 31 agosto 2015)

[15] http://www.srf.ch/sendungen/10vor10/spur-von-snowden-entlastung-fuer-sachs-angriffe-via-internet (stato: 31 agosto 2015)

Si pone la questione fondamentale del perché, nonostante le note vulnerabilità e apparentemente anche a dispetto dell'interesse nutrito da parte degli hacker (quanto meno nei confronti dei sistemi honeypot), non si verifichino blackout o avarie significative. Non è facile rispondere a questa domanda. Una possibilità è costituita dalla mancanza di un modello operativo da parte degli hacker: poiché oltre a un accesso virtuale esiste generalmente anche un accesso fisico ai sistemi, questi possono essere staccati facilmente da Internet nel caso di un attacco (requisiti di autonomia per le soluzioni transitorie subordinate). Un altro possibile motivo è una certa remora da parte degli hacker, motivati in primo luogo da ragioni economiche, dato che le conseguenze (ad esempio in termini di vite umane) che un attacco a un simile sistema potrebbe avere non sono note con precisione.

4.3.2 Controllo aperto di sistemi di approvvigionamento idrico

Per la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) non è sempre facile valutare quanto critici siano da considerare i sistemi aperti e se e in che modo siano interessati eventuali sistemi sensibili.[16] È quanto è emerso da un caso rilevato due anni fa in occasione del Chaos Communication Congress (CCC), quando alcuni hacker hanno pubblicato numerose schermate di sistemi in cui erano, apparentemente, riusciti a penetrare. Fra queste immagini c'era anche quella dell'approvvigionamento idrico di un piccolo comune svizzero. Un'analisi più dettagliata e una richiesta al Comune hanno tuttavia rivelato che, anche se l'accesso non è pubblico, i cittadini interessati possono senz'altro accedere a questi dati. Dai grafici è emerso chiaramente quanta acqua fluisce nell'impianto di accumulazione dalle singole fonti. Non erano invece visibili dati critici, né era possibile operare manipolazioni da accesso remoto.

In un caso analogo, emerso nel periodo preso in analisi, la situazione si è rivelata invece più critica. Anche in questo caso si trattava di un caso di approvvigionamento idrico in Svizzera e dell'indicazione di valori relativi a singole fonti e impianti di accumulazione. Attraverso un'analisi più dettagliata MELANI ha rilevato che sul sito Web si trovavano password pre-programmate per prelevare i dati dagli apparecchi di controllo e poter accedere così alle componenti di controllo. Una password così facilmente accessibile costituisce a sua volta un'ulteriore e pericolosa opportunità di attacco

[16] http://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (stato: 31 agosto 2015)

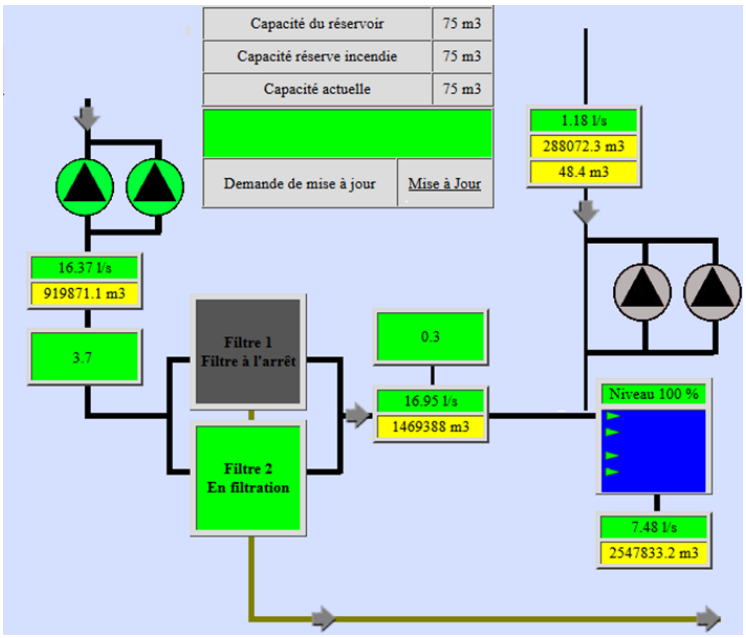


Figura 2: Esempio di una piattaforma accessibile al pubblico di un approvvigionamento di acqua in Svizzera

MELANI mette a disposizione una lista di controllo per la protezione dei sistemi industriali di controllo. Le misure indicate dovrebbero essere integrate in un processo di sicurezza sovraordinato che ne garantisca l'applicazione, una verifica regolare e un costante miglioramento. È altresì importante che il gestore di questo impianto conosca la propria situazione attuale di minaccia, la verifichi regolarmente e faccia confluire gli insegnamenti nell'implementazione e nel miglioramento delle misure di sicurezza. A tale scopo è necessaria una stretta collaborazione tra gli ambiti della gestione dei rischi, della engineering e della gestione aziendale.

https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

Nel febbraio del 2015 l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) ha pubblicato un nuovo studio che fornisce informazioni sulle sfide e le raccomandazioni per lo sviluppo di sistemi per la certificazione delle competenze degli esperti cibernetici che lavorano con sistemi industriali di controllo (ICS) e con il controllo di supervisione e acquisizione dati (SCADA) in Europa.

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

4.4 Attacchi (DDoS, defacement)

I cittadini e le aziende svizzeri continuano a essere oggetto di diversi tipi di attacchi. Un obiettivo di questi attacchi è costituito soprattutto dai loro siti Web. Nel caso delle aziende, in particolare, l'importanza di preservare la credibilità della propria immagine online rende gli attacchi perpetrati attraverso la negazione del servizio (*attacchi DoS*) e il *defacement* (deturpamento) di siti Web particolarmente problematici.

4.4.1 DDoS ed estorsione: ondata di attacchi da parte di DD4BC

L'estorsione è attualmente uno dei metodi privilegiati dai criminali che mirano a realizzare un rapido guadagno finanziario. Come leva per cercare di sottrarre del denaro a una vittima, possono essere utilizzati diversi tipi di attacchi, tra cui quelli operati mediante negazione del servizio (Denial of Service, DoS). DD4BC è un attore che dal luglio del 2014 si è specializzato proprio in questo tipo di attacco ed è caratterizzato in particolare da una grande flessibilità in termini di selezione degli obiettivi. DD4BC ha agito infatti sia in Europa che negli Stati Uniti, in Asia e in Oceania. Gli obiettivi prescelti appartenevano a settori ben precisi e sono stati attaccati in fasi successive. Dopo essersi focalizzato sull'industria dei bitcoin e poi sui casinò online, DD4BC ha mietuto numerose vittime anche tra le banche e le società del settore finanziario.

Questo gruppo è stato particolarmente attivo in Svizzera durante il primo semestre del 2015. MELANI è stata informata di una decina di casi che hanno riguardato diverse società, in particolare nel settore finanziario. Gli elementi raccolti coincidono con quanto osservato in altri Paesi, consentendo pertanto di illustrare le modalità operative di questo gruppo. Tutto ha inizio generalmente con un primo attacco DDoS di debole intensità (generalmente 10–15 Gb/s). Dopo questo attacco dimostrativo, teso a fornire un'idea delle possibilità dell'attaccante, quest'ultimo invia un'e-mail di ricatto alla propria vittima. Se questa vuole evitare un attacco più serio, deve pagare una somma compresa tra 30 e 40 bitcoin (pari a un importo compreso tra fr. 7500 e fr. 10 000). Per giustificare il ricatto, DD4BC sostiene di avere la capacità di sferrare un nuovo attacco da 400 a 500 Gb/s. Questo attore non ha tuttavia mai dato prova di tale capacità. In caso di mancato pagamento è stato a volte osservato un attacco che arrivava fino a 30 Gb/s[17], mentre in altri casi la minaccia non è stata messa in pratica.

Un sito Web inaccessibile può significare un mancato guadagno che può essere rilevante per il proprietario in particolare se il servizio attaccato è di natura commerciale. L'hacker spera che la sua vittima, desiderosa di prevenire gli effetti negativi di un simile attacco, scelga di pagare.

MELANI raccomanda alle vittime di questi attacchi di non cedere ai ricatti. Conviene contattare immediatamente l'host del sito Web e il provider upstream per adottare misure di protezione. Inoltre le vittime hanno la possibilità di sporgere denuncia penale presso la polizia cantonale. MELANI ha pubblicato un documento sul tema degli attacchi DDoS e sui modi in cui possono essere affrontati:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/massnahmen-gegen-ddos-attacken.html

4.4.2 Deturpamento di siti nella Svizzera romanda

Nei primi sei mesi di quest'anno hanno fatto discutere nuove ondate di defacement (deturpamenti) di siti Web, osservate in particolare nella Svizzera romanda. Prima di tutto, in seguito all'attacco terroristico alla redazione di Charlie Hebdo, sono stati osservati numerosi defacement di siti Web in Francia, ma anche – seppure in misura più limitata – nella Svizzera romanda. In questa occasione diversi gruppi hanno divulgato un messaggio di propaganda islamista e di giustificazione degli attentati. In Francia le autorità hanno rilevato 1300

[17] Rapporti esterni documentano attacchi fino a 60 Gb/s. Cfr. In particolare: http://pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf (stato: 31 agosto 2015)

attacchi, sfociati nell'hackeraggio di 25 000 siti Web (cfr. 5. 4.3). I siti Web presi di mira in Svizzera sono stati apparentemente attaccati per via della loro appartenenza all'area francofona. Si suppone che i colpevoli non mirassero intenzionalmente pagine svizzere, quanto piuttosto che le abbiano scambiate per pagine francesi.

In aprile sono stati riportati a MELANI e discussi sulla stampa diversi altri casi di defacement riguardanti siti Web della Svizzera romanda. Anche in questi casi i siti attaccati dagli hacker erano stati utilizzati a scopo di propaganda islamista da un gruppo che rivendicava la propria appartenenza allo Stato Islamico. Sarebbe tuttavia esagerato parlare a questo proposito di ondata di defacement. Dopo l'analisi dei vari casi segnalati a MELANI è emerso infatti che questi erano tutti opera di un unico hacker. Secondo il sito zone-h.org, che recensisce i casi di questo tipo, un hacker che si fa chiamare «cwne» avrebbe attaccato tra il 24 e il 26 aprile 180 siti. Tutti i siti avevano lo stesso host. Con ogni probabilità cwne ha dunque sfruttato una falla di sicurezza presente su un server sul quale erano ospitati diversi siti Web (pratica del «mass defacement»). Questo esempio dimostra che, con un unico attacco, è talvolta possibile attuare un gran numero di defacement e ottenere grande visibilità, tanto più se i siti Web coinvolti appartengono ad aziende o organizzazioni situate in un'area geografica ristretta. Ciò che a volte viene percepito dai media o dalla pubblica opinione come un'azione ad ampio raggio deriva in realtà dallo sfruttamento di un'unica falla di sicurezza da parte di un hacker.

A volte si cerca inoltre di stabilire un legame tra i siti pirata e i messaggi diffusi. Questo legame generalmente è inesistente; gli hacker sono semplici opportunisti e mirano genericamente siti Web vulnerabili indipendentemente dal loro contenuto.

Regole di sicurezza elementari come quelle di aggiornamento dei programmi utilizzati sul sito e sul server Web consentono perlopiù di premunirsi contro questo tipo di attacchi. MELANI ha pubblicato a questo riguardo il seguente documento: https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

4.5 Social engineering, phishing

Oltre a tutti gli attacchi tecnici, tra gli hacker sono popolari anche gli attacchi che sfruttano le debolezze umane. Fin dove è possibile arrivare grazie al social engineering è illustrato in modo incisivo da un caso verificatosi negli USA: un manager dell'azienda statunitense Scoular ha trasferito a più riprese un totale di 17,2 milioni di dollari americani a criminali su un conto bancario cinese, convinto di agire su ordine diretto del suo superiore. Uno studio della società di revisione KPMG conferma questa constatazione e dimostra che le aziende fanno ancora troppo affidamento sulla tecnologia nel proteggersi contro gli attacchi cibernetici, trascurando il fattore umano. Andrebbe invece adottato per principio un approccio integrato ed equilibrato che attribuisca alle persone e ai processi lo stesso peso assegnato alle tecnologie.[18]

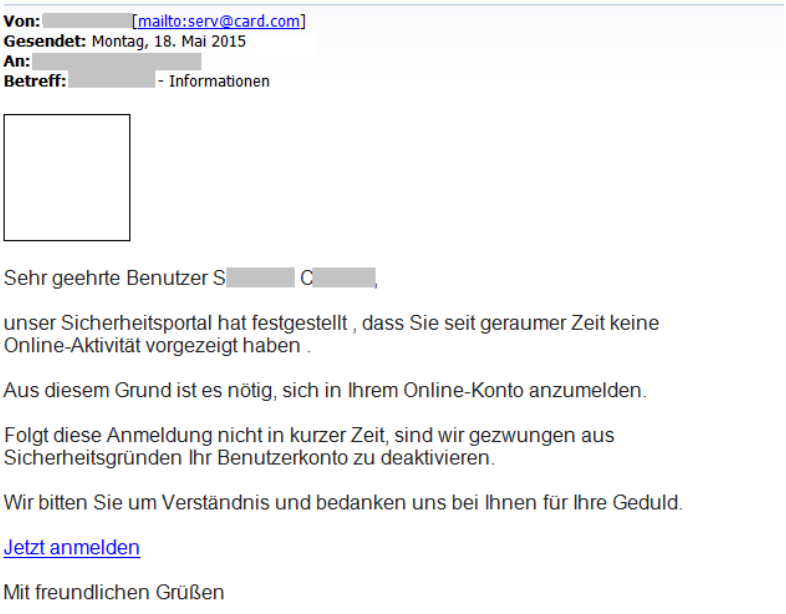
[18] http://www.kpmg.com/CH/de/topics/cyber-security/Seiten/default.aspx?utm_source=mediarelease&utm_medium=email&utm_content=medien-de&utm_campaign=cybersecurity (stato: 31 agosto 2015)

4.5.1 Phishing: attacchi a banche cantonali, dati sulle carte di credito, perfezionamento delle e-mail di phishing

Un ambito tematico rilevante, se non il più rilevante in assoluto, del *social engineering* è tuttora costituito dal *phishing*. Nella maggior parte dei casi osservati si tratta ormai di attacchi standardizzati. In questi casi viene dapprima selezionato un istituto finanziario contro la cui clientelaverrà poi operato un attacco di phishing. In seguito vengono copiati e pubblicati sia il layout del sito Web che quello dell'e-mail; si inventa quindi una storia credibile per la vittima. Dopo di che, per giorni o anche per mesi interi, vengono operati gli stessi attacchi. In questo contesto vi sono ondate di phishing in cui i siti Web vengono addirittura registrati ogni volta presso lo stesso provider. Solo poco tempo dopo la disattivazione della pagina di phishing da parte del provider, la stessa pagina viene nuovamente messa online altrove.

È quanto è accaduto anche nel caso degli attacchi di phishing contro le banche cantonali svizzere, rilevati in più occasioni nel primo semestre del 2015. Una caratteristica di queste ondate di attacchi è il fatto che l'obiettivo non era costituito dalla banca cantonale di un singolo Cantone; erano invece coinvolti in generale clienti di banche cantonali di tutta la Svizzera (tedesca). Solo in una seconda fase la vittima era tenuta a precisare la banca cantonale presso la quale deteneva il proprio conto di e-banking e naturalmente a fornire anche i propri dati personali. Questo ha naturalmente aumentato il numero di potenziali vittime.

A fronte della crescente sensibilità dei clienti dell'e-banking, gli hacker sono tuttavia costretti a inventare metodi di attacco sempre nuovi e più efficaci. Rientra in questo contesto anche l'intestazione personalizzata con nome e cognome, che mira a conquistare la fiducia delle potenziali vittime. Questo metodo ad oggi non si è ancora affermato in modo capillare – probabilmente perché il carico di lavoro richiesto per collegare nome e cognome ai rispettivi indirizzi e-mail è ancora eccessivo. In diverse ondate di phishing osservate nella seconda metà del 2015 è stato tuttavia adottato proprio questo modo di procedere. È difficile dire dove gli hacker abbiano reperito ogni volta questi dati. Essi potrebbero provenire, ad esempio, da account di posta elettronica compromessi e visualizzati dai criminali.



Von: [mailto:serv@card.com]
Gesendet: Montag, 18. Mai 2015
An:
Betreff: - Informationen

Sehr geehrte Benutzer S C,

unser Sicherheitsportal hat festgestellt , dass Sie seit geraumer Zeit keine Online-Aktivität vorgezeigt haben .

Aus diesem Grund ist es nötig, sich in Ihrem Online-Konto anzumelden.

Folgt diese Anmeldung nicht in kurzer Zeit, sind wir gezwungen aus Sicherheitsgründen Ihr Benutzerkonto zu deaktivieren.

Wir bitten Sie um Verständnis und bedanken uns bei Ihnen für Ihre Geduld.

Jetzt anmelden

Mit freundlichen Grüßen

Figura 3: Esempio di un'e-mail di phishing con l'impiego del nome e del cognome nell'appellativo

Che un'intestazione nominale mirata, una storia plausibile e dunque un social engineering professionale svolgano un ruolo importante è dimostrato dai casi in cui, prima di un attacco, la banca dati dei clienti di una società è stata compromessa da hacker e quindi copiata. Ciò avviene generalmente tramite un'*iniezione SQL*. Segue quindi un'e-mail mirata, a nome dell'azienda, con il link a un sito Web imitato alla perfezione e l'invito a registrarvi il proprio numero di carta di credito per un qualunque motivo. Poiché la vittima probabilmente è già in contatto con la vera azienda e la giustificazione appare plausibile, vi sono buone probabilità che cada nella trappola. L'azienda coinvolta non può quindi fare altro che informare immediatamente il cliente di questo tentativo di frode.

4.5.2 Phishing dopo un *defacement* – e a volte anche il contrario

Negli ultimi tempi MELANI ha riscontrato sempre più spesso anche una relazione tra i defacement e i tentativi di phishing. Affinché i criminali possano creare un sito di phishing, devono dapprima acquistare un dominio o compromettere un sito Web già esistente sfruttando delle falle di sicurezza. Anche nel caso dei defacement vengono sfruttate falle di sicurezza dei siti Web per poterne poi modificare i contenuti e pubblicarvi dichiarazioni di carattere personale, religioso o politico. I siti Web deturpati vengono inoltre spesso pubblicati su siti accessibili a tutti come zone-h.org[19]. Per gli autori di phishing è dunque semplice trovare e sfruttare siti Web con falle di sicurezza conosciute e piazzarvi le proprie pagine di phishing. La situazione opposta, ossia il defacement di una pagina di phishing già esistente, è invece molto meno probabile, in primo luogo perché non esistono liste pubbliche di pagine di phishing e in secondo luogo perché queste pagine, una volta scoperte, vengono tolte dalla rete il più rapidamente possibile.

Nel maggio del 2015 MELANI ha osservato per la prima volta un procedimento di questo tipo: dapprima è stato reso noto un attacco di phishing contro un istituto finanziario svizzero. Com'è consuetudine in questi casi, la pagina è stata analizzata e quindi segnalata al provider responsabile affinché potesse disattivarla ma, ancora prima che il provider potesse reagire e cancellare la pagina ingannevole, l'attacco di phishing era già stato sabotato da un «hacktivist». Coprendo la pagina con un messaggio contro la xenofobia, l'«hacktivist» ha probabilmente impedito, inavvertitamente, che potenziali vittime potessero rivelare i loro dati sulla pagina di phishing.

4.5.3 Moduli di dichiarazione d'imposta falsificati

Nel primo semestre numerose aziende della regione di Ginevra hanno ricevuto un'e-mail con un modulo apparentemente proveniente dalle autorità fiscali ginevrine. Il modulo, sul quale dovevano essere dichiarati gli utili immobiliari e altri dettagli relativi all'impresa, doveva essere quindi spedito a un indirizzo e-mail assieme all'ultimo conteggio dell'affitto. Il modulo inviato è realmente esistente ma l'indirizzo di spedizione indicato non aveva nulla a che vedere con le autorità fiscali ginevrine e apparteneva invece a un truffatore.

Un caso analogo è stato osservato anche nel Canton Vaud[20].

A quale scopo possono essere sfruttati abusivamente questi dati una volta che il truffatore ne entra in possesso? In questo caso sembra essersi trattato più che altro di un'operazione preparatoria in vista dei cosiddetti «president scam», con cui gli hacker raccolgono in via

[19] Zone-h.org è un archivio di siti Web deturpati

[20] http://www.24heures.ch/vaud-regions/arnaqueurs-utilisent-adresse-fisc-vaudois/story/10817017 (stato: 31 agosto 2015)

preliminare informazioni sull'azienda per farsi un'idea precisa dell'organizzazione e del contesto del loro bersaglio. Queste informazioni vengono in parte raccolte tramite una ricerca attiva come quella qui descritta (forse mettere: in parte su fonti aperte, google…). Solo in seguito ha inizio l'attacco vero e proprio: di regola viene inviata un'e-mail a un collaboratore del reparto finanziario, apparentemente proveniente da un membro dei quadri. L'e-mail inviata riguarda generalmente operazioni finanziarie riservate in corso. I truffatori sottolineano il carattere straordinario e la riservatezza del compito ma anche l'urgenza imposta dalla situazione. In diversi casi i truffatori cercano di conferire ancora più credibilità allo scenario con telefonate effettuate in parallelo.

Il Canton Ginevra ha attivato un messaggio di avvertimento sul proprio sito Web.[21]

Le principali regole di condotta legate alle e-mail aiutano a tutelarsi contro il phishing e altri tipi di truffe.

Diffidate delle e-mail che vi vengono inviate spontaneamente: siate critici non soltanto nei confronti delle e-mail provenienti da persone a voi sconosciute, ma anche di quelle che vi giungono da mittenti conosciuti. Le aziende particolarmente meritevoli di fiducia vengono sfruttate volentieri come falsi mittenti.

- Siate scettici se ricevete e-mail che esigono un'azione da parte vostra e minacciano conseguenze in caso contrario (perdita di denaro, denuncia o procedimento legale, blocco del conto o della carta, mancata opportunità, infortunio).
- Quando ricevete un'e-mail sospetta non cliccate su alcun allegato né seguite alcun link; in caso contrario rischiate di essere infettati da un malware. In caso di dubbio chiedete al presunto mittente, utilizzando i dati di contatto forniti sul sito Web, di che cosa si tratta esattamente e se l'e-mail proviene davvero da loro.
- La regola base di non rivelare informazioni interne in caso di prese di contatto dubbie o strane e di non accettare alcun invito a farlo è più attuale che mai a fronte dei casi rilevati negli ultimi tempi.

Regola valida soprattutto per le aziende:

- tutti i processi che riguardano il traffico dei pagamenti dovrebbero essere chiaramente disciplinati all'interno dell'azienda ed essere rispettati in ogni caso dai collaboratori.
- MELANI raccomanda in particolare una sensibilizzazione dei collaboratori, specialmente di quelli in posizioni chiave, nei confronti di questi casi.
- In caso di prese di contatto e inviti insoliti si raccomanda di chiedere conferma per telefono all'interno dell'azienda per verificare la veridicità dell'incarico.
- Un promemoria sulla sicurezza informatica per le PMI è disponibile sul sito Web di MELANI al seguente indirizzo: https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

[21] http://ge.ch/impots/courrier-lectronique-frauduleux (stato: 31 agosto 2015)

4.6 Crimeware

Il crimeware è una forma di malware sviluppata da criminali economici che dal punto di vista criminologico rientra nel campo della criminalità informatica e giuridicamente si colloca nel settore delle truffe su Internet. In materia di crimeware sono sempre molto diffusi i trojan di e-banking, come dimostra la statistica riportata di seguito. Gran parte dei sistemi infettati in Svizzera, comunicati a MELANI, è costituita da trojan di e-banking come ad esempio «Torpig», «Dyre», «Tinba», «Gozi» o «ZeuS».

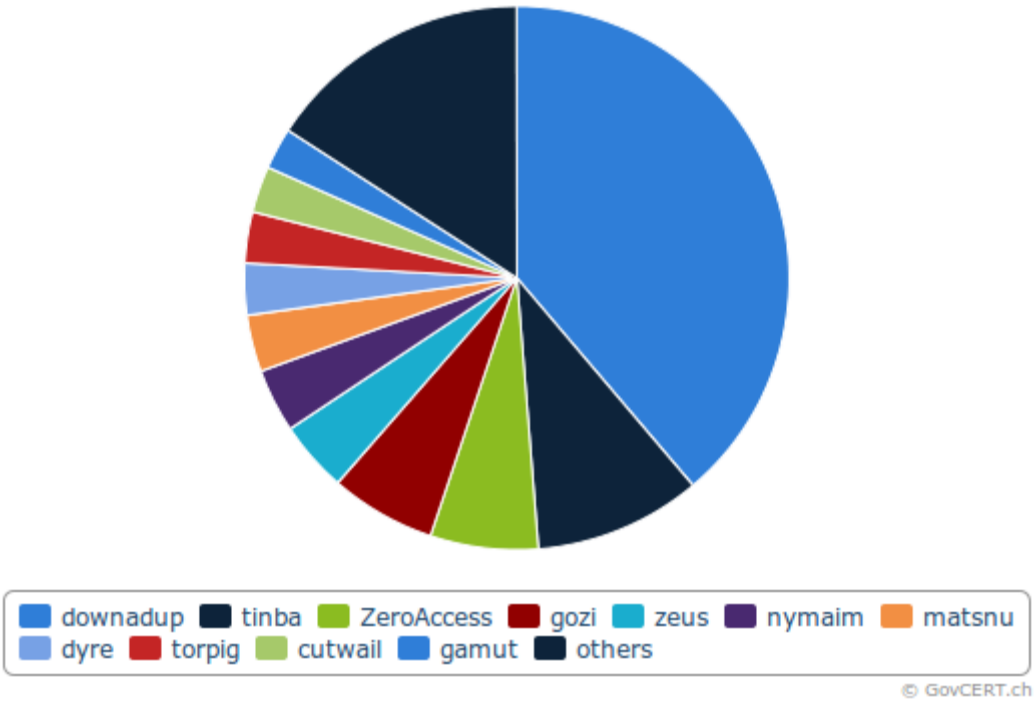


Figura 4: Distribuzione del malware noto a MELANI in Svizzera. Il giorno di riferimento è il 30 giugno 2015. Dati attuali sono reperibili seguendo il collegamento: Cfr. anche: http://www.govcert.admin.ch/statistics/dronemap/

In termini di distribuzione geografica sono soprattutto i Cantoni di Zurigo e del Vallese a presentare una percentuale di infezioni superiore rispetto ad altri Cantoni (tenuto conto del numero di abitanti).

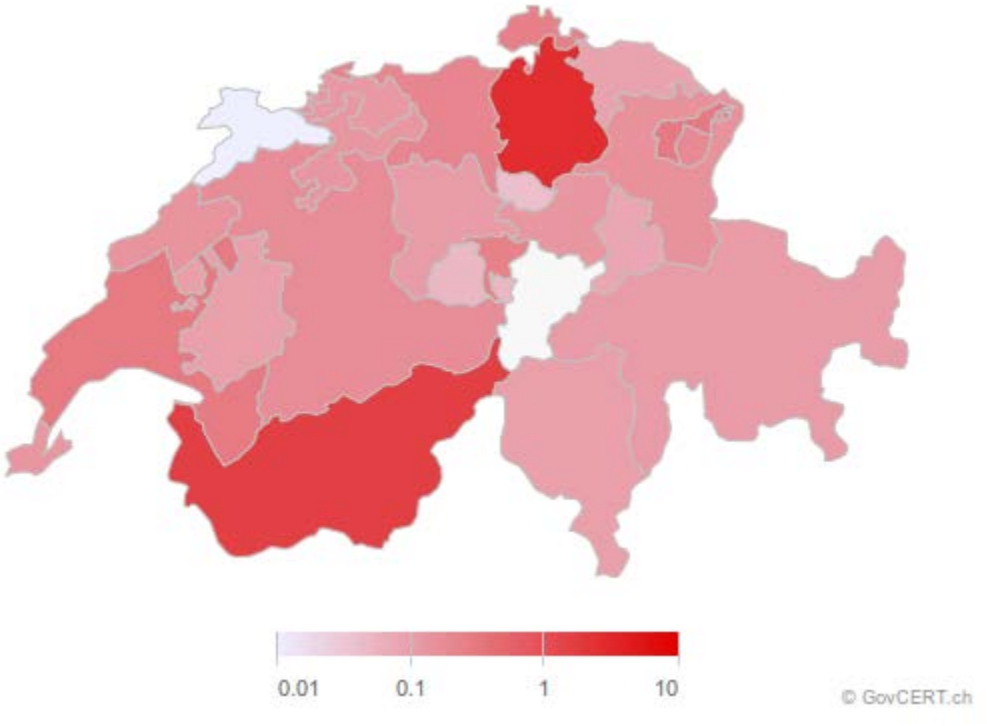


Figura 5: Numero di infezioni per Cantone tenuto conto del numero di abitanti. Il giorno di riferimento è il 30 giugno 2015. Dati attuali sono reperibili seguendo il collegamento: Vedi anche: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1.1 Downadup

L'aspetto preoccupante delle infezioni di Downadup (noto anche come Conficker) è che questo worm esiste già da più di otto anni e continua evidentemente a essere molto diffuso. Downadup si diffonde tramite una lacuna di sicurezza rilevata nel 2008 nel sistema operativo Windows che può essere sfruttata via Internet e installata con un qualsiasi codice nocivo su un computer estraneo. Il numero tuttora elevato di infezioni potrebbe essere giustificato dal fatto che molti utenti di Internet in Svizzera utilizzano ancora una versione meno recente di Windows (Windows XP) e non sottopongono il loro sistema operativo a un patching regolare. Un'altra possibile spiegazione è che in Svizzera esistono tuttora diversi Internet Service Provider (ISP) che non elaborano i messaggi relativi ai clienti infettati (p.es. per mancanza di risorse, di mezzi tecnici adeguati o di know-how).

4.6.1.2 Dyre

Nella prima metà del 2015 si è diffuso in Svizzera soprattutto il malware Dyre (noto anche con il nome di Dyreza). Si tratta di un trojan di e-banking che si diffonde via e-mail. A questo scopo i criminali preparano e-mail spacciandole normalmente per messaggi fax, fatture o altri documenti analoghi che contengono un malware in allegato (normalmente un file .exe eseguibile in un archivio ZIP). Se nei primi mesi Dyre mirava soprattutto alle PMI svizzere[22] e ha portato anche al furto di un importo a sette cifre da un'azienda friburghese, dal maggio

[22] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking-trojaner-hat-schweizer-kmus-im-visier.html (stato: 31 agosto 2015)

del 2015 Dyre ha attaccato diffusamente anche utenti privati[23]. Nei momenti di punta sono state annunciate a MELANI fino a 2000 infezioni dovute a Dyre.

Se doveste già aver ricevuto e-mail di questo tipo e aver aperto il file allegato, vi raccomandiamo di verificare il vostro sistema con un programma antivirus o uno strumento di rimozione malware. Una guida sull'argomento è disponibile su:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/guida-per-l_eliminazione-di-software-nocivi.html

MELANI ha pubblicato un promemoria allo scopo di aiutare le PMI a migliorare la sicurezza informatica nella propria rete aziendale. Il promemoria è disponibile su:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/promemoria-sulla-sicurezza-informatica-per-le-pmi.html

Trovate inoltre un programma in dieci punti per aumentare la sicurezza informatica sul portale PMI della Confederazione:

http://www.kmu.admin.ch/kmu-betreiben/03710/03712/03715/index.html?lang=it

4.6.1.3 Retefe

Il malware Retefe è tuttora attivo in Svizzera. MELANI ha parlato per la prima volta di Retefe due anni fa. Il malware si diffonde esclusivamente via e-mail, generalmente spacciandosi per una fattura di famose piattaforme di vendita online come ad esempio Zalando o Ricardo.

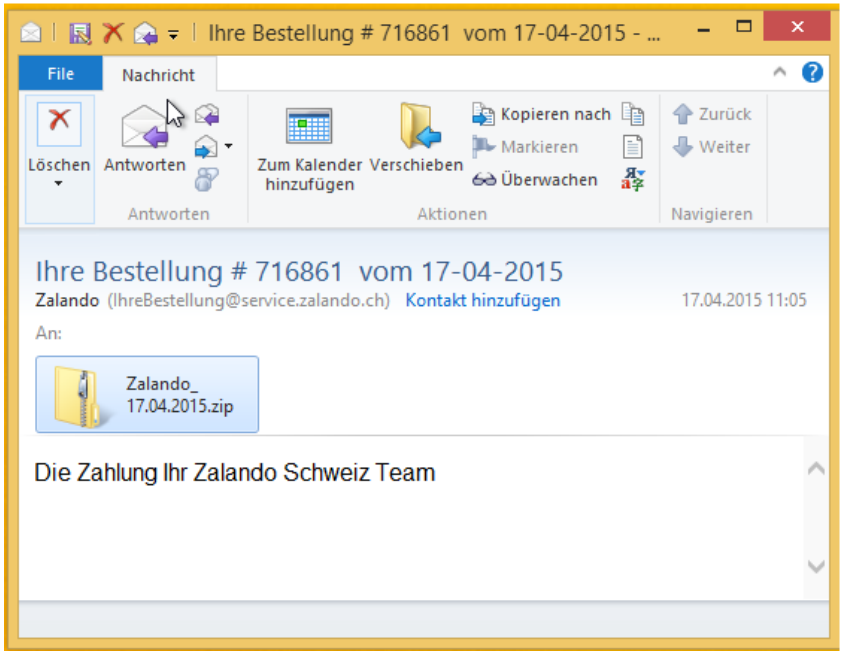


Figura 6: Esempio di un'e-mail falsificata che diffonde il malware Retefe

Se il destinatario dell'e-mail esegue il file contenuto nell'allegato, infetta con Retefe il suo Computer Windows. Se l'infezione ha successo, Retefe modifica le impostazioni di Internet

[23] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/information_dyre_2.html (stato: 31 agosto 2015)

Explorer in modo che determinati siti Web (in particolare i portali di e-banking di alcuni istituti finanziari svizzeri) vengano deviati all'estero tramite un proxy server. Retefe installa inoltre un certificato CA maligno nella memoria dei certificati di Windows. Retefe è così in grado di rilasciare certificati per qualsiasi istituto finanziario e a spacciarsi per quest'ultimo.

Se una vittima effettua il login da un computer infettato con Retefe nel presunto portale di e-banking, gli viene fornito un QR code. Questo codice conduce a un URL maligno che invita la vittima a scaricare e ad installare un App per "aumentare la sicurezza" dietro alla quale si nasconde in realtà un malware Android (un cosiddetto trojan SMS). Se la vittima installa l'app Android pubblicizzata, tutti gli SMS inviati dalla banca per l'autenticazione a due fattori vengono inoltrati agli hacker su un web server all'estero. Questi sono quindi in grado di eseguire il login nell'e-banking della vittima e anche di effettuare pagamenti.

Qualora utilizziate uno smartphone o un tablet Android, assicuratevi di installare unicamente app provenienti dal Google Play Store ufficiale. Non installate mai app provenienti da fonti terze, neppure se venite invitati a farlo. Assicuratevi inoltre che sul vostro dispositivo Android siano state attivate le seguenti impostazioni:

Impostazioni -> Sicurezza -> Origini sconosciute -> DISATTIVATO

Impostazioni Google -> Sicurezza -> Analizza dispositivo per minacce alla sicurezza -> ATTIVATO

Per ulteriori informazioni su Retefe consultate il blog GovCERT.ch (in inglese):

http://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

4.6.1.4 Tinba

Nel primo semestre del 2015 anche Tinba (noto anche con il nome di «Tiny Banker») ha tenuto occupati gli utenti Internet svizzeri ed in alcuni momenti è stata, assieme a Downadup, l'infezione più spesso comunicata a MELANI in Svizzera. Tinba è un altro trojan di e-banking che mira a colpire alcuni istituti finanziari svizzeri. Diversamente da Dyre o Retefe, Tinba è però un «toolkit» che può essere acquistato su forum specializzati su Internet per qualche migliaio di franchi. I criminali attivi su Internet acquistano il software e possono quindi utilizzarlo a loro piacere. Oltre alle campagne Tinba note in Svizzera si rilevano anche alcune dozzine di altre campagne Tinba a livello mondiale che hanno a loro volta come bersaglio gli istituti finanziari di tutto il globo.

4.6.1.5 Trojan di crittografia – Cryptowall 3.0, Teslascript e un autore colpito dai rimorsi

Nel primo semestre del 2015 sono stati notificati nuovamente diversi casi in cui erano stati crittografati dati attraverso un trojan di crittografia. In questi casi si trattava generalmente di Cryptowall 3.0; sono stati tuttavia notificati a MELANI anche diversi casi legati al ransomware Teslacrypt. Le vittime sono generalmente privati, ma sono noti anche casi aziendali. Chi non ha a disposizione un backup aggiornato perde tutti i propri dati o una parte di essi. A questo proposito è emblematico il caso attorno al ransomware Locker. In precedenza il malware si era diffuso su diversi computer ed era in attesa di passare all'attacco e crittografare dati, cosa poi effettivamente avvenuta all'inizio di giugno. Poco dopo, tuttavia, l'autore non si è

soltanto palesato, scusandosi, ma ha anche impartito al malware il comando di decodifica, pubblicando contemporaneamente anche la relativa chiave.[24]

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.

4.7 Misure preventive

Per poter fare fronte alle diverse minacce esistenti sono essenziali le misure preventive. Queste misure possono essere di natura tecnica, organizzativa e anche penale. Anche la sensibilizzazione della popolazione costituisce un importante pilastro nella lotta contro gli attacchi cibernetici. Così, la maggior parte di questi attacchi sfrutta l'ignoranza e la disponibilità delle vittime, cercando di coglierle di sorpresa. Un'altra importante misura contro gli attacchi cibernetici è la diffusione di una cultura della notifica, sia all'interno di un'azienda che in generale tra la popolazione. Solo se i collaboratori hanno la sensazione di essere presi sul serio in caso di denuncia di un caso continueranno infatti a effettuare queste segnalazioni. Per questo MELANI ha creato il portale «antiphishing.ch» sul quale è possibile segnalare le e-mail e i siti web sospettate di essere finalizzate al furto di dati d'accesso o relativi alle carte di credito.

4.7.1 Antiphishing.ch

Per canalizzare meglio e analizzare in modo più efficiente le comunicazioni di pagine di *phishing*, nell'estate del 2015 MELANI ha lanciato il portale antiphishing.ch. La segnalazione di siti Web di *phishing* può avvenire tramite il modulo disponibile sul Web. Sul portale di notifica è inoltre indicato un indirizzo e-mail al quale possono essere inoltrate le e-mail di *phishing*. Il portale di notifica è accessibile all'indirizzo https://www.antiphishing.ch.

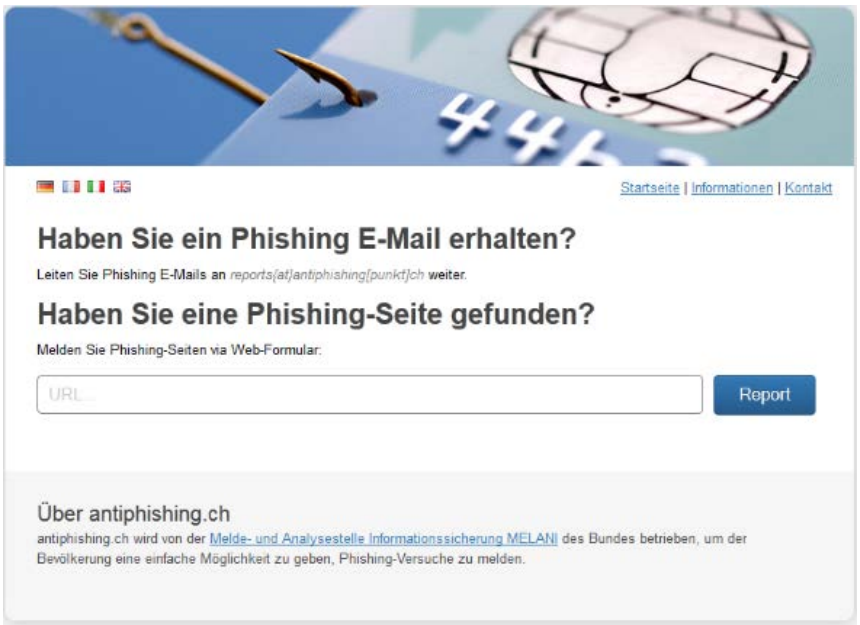


Figura 7: Schermata del nuovo sito Web antiphishing.ch, dove i cittadini possono segnalare le pagine di phishing

[24] http://www.heise.de/security/meldung/Krypto-Trojaner-ueberlegt-es-sich-anders-und-entschluesselt-alles-wieder-2678669.html (stato: 31 agosto 2015)

Le segnalazioni di phishing pervenute vengono sottoposte a un esame automatico preliminare. Sulla base dei risultati di questo esame preliminare, le segnalazioni vengono quindi accuratamente esaminate manualmente prima di essere comunicate ai produttori di software di sicurezza informatica, ai web browser, agli hosting provider ecc. nonché, su richiesta, anche agli istituti finanziari coinvolti e i gestori di servizi internet, per ottenere così la massima protezione.

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 Attacco al Bundestag tedesco da parte di hacker

Il 15 maggio 2015 è stato reso pubblico che la rete del Bundestag tedesco, «Parlakom», aveva subito un attacco mirato e che gli hacker avevano copiato dati per un totale di 16 gigabyte.[25] Sembra che in questo caso gli hacker cercassero password di sistema, documenti Word ed e-mail salvati localmente. Secondo il quotidiano «die Welt» pare che l'infezione iniziale sia partita, come accade molto spesso, da e-mail contenenti un link appositamente preparato a questo scopo.[26,27] Secondo un verbale della *Kommission des Ältestenrates per den Einsatz neuer Informations- und Kommunikationstechniken und –medien (IuK)* del Bundestag[28], l'8 maggio 2015 sarebbe stata notata una «comunicazione insolita» tra sistemi di server. Su un server dell'amministrazione del Bundestag sarebbe stato rilevato un sovraccarico dovuto a una quantità insolita di dati. Questo server avrebbe inoltre presentato collegamenti non previsti con l'ufficio di un deputato. Quattro giorni dopo, durante un'ulteriore indagine, sarebbe emerso che due computer erano in contatto con server potenzialmente pericolosi, cosiddetti *Command & Control server*. Pare si trattasse degli stessi sistemi che già qualche giorno prima avevano dato nell'occhio. Sebbene fossero apparentemente coinvolti solo pochi apparecchi finali, gli hacker sarebbero riusciti a penetrare in profondità nel sistema, dove avrebbero potuto muoversi liberamente e dove potrebbero tornare ad agire in qualsiasi momento.

Nell'ulteriore corso della vicenda sembra sia stato difficile debellare gli hacker dalla rete. Come possibile misura è stata presa in considerazione la ricostruzione di parti della rete. Per questo motivo, il 20 agosto 2015 la rete del Bundestag è stata disattivata per quattro giorni allo scopo di eliminare le conseguenze dell'intrusione cibernetica. Questa misura decisiva dimostra la portata dell'evento, ma non costituisce naturalmente una garanzia contro future infezioni.

Il procuratore generale federale tedesco sta valutando se in questo caso esista un sospetto iniziale di reato penale che rientri nella sfera di competenza della procura generale federale. Il programma di spionaggio utilizzato per l'attacco sembra essere stato individuato. Sono state fatte ipotesi sul fatto che possa essersi trattato del complesso di malware «Sofacy/APT28».[29] La struttura del programma sembra somigliare a quella di un malware già osservato nel 2014 durante un attacco cibernetico a una rete di dati tedesca.

---

25 http://www.spiegel.de/politik/deutschland/cyberangriff-auf-bundestag-abgeordneten-e-mails-erbeutet-a-1039388.html (stato: 31 agosto 2015)

26 http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html (stato: 31 agosto 2015)

27 https://www.tagesschau.de/inland/bundestag-cyberattacke-105.html (stato: 31 agosto 2015)

28 http://www.bild.de/politik/inland/bundestag/spielte-cyber-angriff-laut-geheimprotokoll-herunter-41314062.bild.html (stato: 31 agosto 2015)

29 http://www.focus.de/politik/deutschland/bundestag-cyber-angriff-auf-bundestag-dauert-schon-laenger-als-bekannt_id_4761526.html (stato: 31 agosto 2015)

5.1.2 Carbanak – la rapina in banca elettronica

Finora le rapine su conti online erano limitate ai clienti finali. In questi casi il computer del cliente veniva infettato con un *malware* di e-banking che assumeva quindi il controllo della sessione di e-banking. Nel febbraio del 2015, tuttavia, sono divenute di pubblico dominio rapine elettroniche di una qualità del tutto nuova. Sotto il nome di «Carbanak», nell'arco di due anni, sono stati manipolati in grande stile diversi sistemi bancari. Il carico di lavoro connesso con questo attacco è simile a quello degli attacchi di spionaggio mirati come quelli osservati finora negli Stati Uniti. In questo contesto si è cercato dapprima di infettare i computer di alcuni impiegati di banca. A questo scopo è stato utilizzato il metodo classico dell'allegato dannoso contenuto in un'e-mail mirata. Successivamente gli hacker hanno cercato computer di postazioni di lavoro di collaboratori tramite i quali venivano gestiti bonifici e distributori automatici di contanti collegati alla rete. I rapinatori sono rimasti nella rete per un periodo compreso tra due e quattro mesi per scoprire come avrebbero potuto sfruttare a proprio vantaggio le procedure bancarie interne.[30] Dopo aver raccolto queste informazioni, gli hacker si sono finti impiegati di banca trasferendosi del denaro oppure hanno manipolato i distributori automatici di contanti in modo che distribuissero denaro in un dato momento. Un complice attendeva quindi al distributore interessato per raccogliere il denaro. Perché i trasferimenti effettuati non venissero notati, i saldi dei conti rapinati venivano dapprima aumentati per poi essere nuovamente alleggeriti dello stesso identico importo. Il saldo complessivo presso la vittima rimaneva dunque invariato e la truffa non veniva riconosciuta tanto rapidamente dalla vittima.

Secondo Kaspersky gli hacker avrebbero infettato almeno 100 banche in 30 paesi, la maggior parte delle quali in Russia. Il denaro sottratto giustifica le fatiche compiute dagli hacker e durate fino a due anni. Da ogni singola banca sono stati rubati fino a 10 milioni di dollari.

5.1.3 Schede SIM apparentemente nelle mire della NSA e dei GCHQ

Nel corso di questo semestre sono stati rivelati nuovi fatti basati su documenti di Snowden. Al centro dell'attenzione c'erano le *schede SIM*, ossia le schede che vengono inserite in un telefono cellulare e servono a identificare l'utente nella rete. Secondo il giornale «The Intercept», un'unità comune dei Government Communications Headquarters (GCHQ) britannici e della NSA denominata «Mobile Handset exploitation Team (MHET)» avrebbe compromesso le reti interne dei grandi produttori di schede SIM e di apparecchi finali nonché di molti operatori di rete. Nel mirino è finito soprattutto il produttore di schede SIM «Gemalto». Quest'ultimo ha poi reso noto di aver osservato, rispettivamente scoperto nel 2010 e nel 2011, raffinati attacchi nella propria rete che avrebbero potuto costituire indizi di attività della NSA e dei GCHQ. Nel luglio del 2010 sarebbero state inoltre inviate e-mail mirate dirette a collaboratori[31]. Al centro dell'interesse c'era soprattutto lo scambio di chiavi tra operatori di telefonia mobile e altri fornitori. Nella maggior parte dei casi questo scambio era già crittografato nel 2010. Tutti gli attacchi sembrano tuttavia aver riguardato solo l'automazione d'ufficio e non le reti produttive. Non è chiaro se questi attacchi siano effettivamente riconducibili alla NSA. Gemalto ha escluso un furto consistente di codici di

30 http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide (stato: 31 agosto 2015)

31 http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx (stato: 31 agosto 2015)

crittografia di schede SIM. Per uno specialista di crittografia sarebbe proprio questo lo scenario peggiore.

5.1.4 Spionaggio nello sport professionistico

Non sorprende più di tanto che lo spionaggio informatico riguardi anche il mondo dello sport professionistico, dato che anche in questo caso sono in gioco ingenti somme di denaro. Ciò vale in particolare per l'US Baseball League. Da anni in questo sport i «Saint Louis Cardinals» si sfidano sul campo con gli «Houston Astros». Alcuni collaboratori dei Cardinals sembrano però aver deciso di non disputare più le partite soltanto sul campo da baseball, bensì anche nel cyberspazio. Invece di raccogliere unicamente punti, si sono dedicati alla raccolta di informazioni, come quelle sulle statistiche degli allenamenti dei giocatori, le statistiche di gioco, e le norme contrattuali o su possibili acquisti futuri di giocatori, sulle strategie ecc. che possono rivelarsi naturalmente altrettanto preziose.

Il retroscena di questa vicenda sembra essere costituito dal trasferimento del general manager Luhnow dai Cardinals agli Astros nel 2011. Si dice che Luhnow concentri la propria attenzione sulle analisi statistiche. Quando lavorava ancora per i Cardinals, reclutava giovani talenti che trovava grazie a una banca dati e a una sorta di screening elettronico dei giocatori, contribuendo così al successo della squadra. Dopo il suo passaggio agli Astros, ha riproposto gli stessi metodi ed è riuscito a imporli. I Cardinals hanno dichiarato pubblicamente di aver temuto che Luhnow avesse messo a disposizione della squadra avversaria delle informazioni su di loro.

In un mondo sempre più interconnesso e digitalizzato anche lo sport è soggetto a pressioni verso la modernizzazione. Sempre più spesso fanno il loro ingresso nello sport analisi e statistiche e, con esse, anche l'impiego di grandi volumi di dati che possono costituire interessanti obiettivi di attività di spionaggio. Nel baseball, in particolare, le previsioni sulle prestazioni dei giocatori sono largamente diffuse, poiché il numero limitato di variabili legate ai singoli soggetti rende più semplice formulare pronostici ed effettuare misurazioni. Nel calcio e nell'hockey su ghiaccio questi metodi sono meno frequenti, poiché questi sport non vedono contrapposti singoli giocatori, bensì due squadre, e il numero di variabili in gioco è superiore. Nonostante questo, anche la squadra di calcio del «Manchester City» ha lanciato nel 2012 un concorso per incoraggiare giovani analisti a sviluppare metodi applicabili a questo sport.

5.2 Flussi di dati in uscita

5.2.1 Oltre 21 milioni di dati sottratti all'Ufficio di gestione del personale del governo degli Stati uniti

Nell'aprile del 2015 l'«Office of Personnel Management OPM» (approssimativamente paragonabile all'Ufficio federale del personale) ha scoperto che erano stati copiati dati personali di 4.2 milioni di dipendenti federali attuali e passati. Il furto riguardava informazioni quali il nome, la data di nascita, l'indirizzo e il numero di assicurazione sociale. Durante le indagini sull'accaduto, l'OPM ha tuttavia scoperto un ulteriore e ancora più consistente furto di dati, riguardante anche informazioni sul background di dipendenti federali e partner contrattuali passati, presenti e futuri. Questo caso più recente riguarda molto probabilmente 21.5 milioni di dati individuali e informazioni raccolte nell'ambito di controlli di sicurezza[32]. In

[32] https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/ (stato: 31 agosto 2015)

questo contesto, 19.7 dati proverrebbero da persone che si sono candidate per un posto di lavoro e 1.8 milioni da persone che sono in contatto con candidati a un posto di lavoro, ad esempio coniugi o conviventi. Alcune parti dei dati rubati contengono tra l'altro gli esiti di colloqui di lavoro raccolti dagli inquirenti, informazioni sullo stato di salute mentale e sulla storia finanziaria. Sono stati inoltre copiati anche 1,1 milioni di impronte digitali. Nel 2014 l'ufficio di vigilanza interna dell'OPM aveva raccomandato di chiudere undici dei suoi 47 sistemi TIC, poiché non possedevano alcun certificato di sicurezza valido. L'OPM non aveva dato seguito alla raccomandazione. Non è chiaro se l'hackeraggio abbia riguardato eventualmente uno di questi sistemi TIC. Questo attacco – il più grande mai operato a una rete di computer del governo americano, è costato il posto di lavoro alla direttrice dell'OPM.

Gli inquirenti USA ritengono che dietro agli attacchi all'amministrazione federale statunitense ci sia un gruppo cinese. Come previsto, la Cina ha immediatamente smentito una un'implicazione in questi attacchi.

Gli uffici del personale sono particolarmente interessanti per i cacciatori di dati, soprattutto se tutti i dati di tutti i collaboratori dell'amministrazione sono riuniti in un unico ufficio o sono amministrati in un unico luogo. Poiché al loro interno viene elaborato un numero elevato di documenti di diverse provenienze, si crea anche un ulteriore pericolo potenziale proveniente dai malware, che possono infiltrarsi in diversi modi.

5.2.2 AdultfriendFinder, British Airways e assicurazione malattie – deflussi di dati nei settori più svariati

Buona parte dei servizi di ricerca di un partner si è ormai trasferita sul Web. Le conquiste di Internet e le possibilità offerte dai social media non si fermano neppure davanti a questo settore e semplificano la ricerca di un partner idoneo. Se però il portale utilizzato diventa il bersaglio di criminali cibernetici e i dati degli utenti, comprese le loro preferenze sessuali, finiscono con l'essere resi pubblici in rete, il tanto apprezzato anonimato non è più garantito. Un simile passo falso è capitato al sito di incontri «Adultfriendfinder»[33] nel maggio di quest'anno. Circa quattro milioni di dati di utenti, grazie ai quali è possibile identificare con poco sforzo le persone che si celano dietro agli pseudonimi, sono finiti su un forum specializzato e accessibile a tutti. Questo caso è stato addirittura superato lo scorso luglio dall'attacco al portale per persone impegnate in cerca di un'avventura «Ashley Madison»[34], sfociato nella pubblicazione dei login di 32 milioni di utenti.

Ma nel primo semestre sono stati resi noti anche flussi di dati in uscita decisamente più critici. Alla British Airways sono stati infatti sottratti dati di clienti aderenti al programma per frequent flyer[35]. Questi dati consentono ad esempio di stilare un profilo degli spostamenti delle persone interessate.

La questione si fa ancora più delicata quando sono dati fiscali sensibili a finire nelle mani sbagliate, com'è accaduto lo scorso maggio presso l'autorità fiscale americana IRS[36].

33 http://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web (stato: 31 agosto 2015).

34 http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (stato: 31 agosto 2015).

35 http://www.theregister.co.uk/2015/03/29/british_airways_frequent_flyers_hacked/ (stato: 31 agosto 2015)

36 http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application (stato: 31 agosto 2015)

Tramite ricerche di «social engineering» gli hacker sono riusciti a scardinare un processo di autenticazione dell'IRS e a estrarre così i dati dei contribuenti a loro nome.

Tra i dati più sensibili figurano anche quelli dei pazienti. Nessuno desidera che dati relativi alle proprie visite mediche e malattie diventino di pubblico dominio. Purtroppo, però, anche questi dati personali particolarmente meritevoli di tutela non sono sempre protetti da sguardi indiscreti. Nel mese di febbraio la seconda più grande compagnia di assicurazioni malattia americana, Anthem[37], ha subito un furto nella propria banca dati, che comprende 80 milioni di clienti. A marzo un'altra compagnia di assicurazioni malattia, la «Premera Health Care»[38], è stata vittima di un furto di dati dello stesso tipo.

Per gli operatori, questo significa che i criminali informatici motivati non si fermano davanti a nessuno. Si raccomanda pertanto caldamente di adottare tutte le misure possibili per evitare di cadere vittima di un furto di dati. Una buona sintesi dell'argomento è contenuta nel nostro promemoria sulla sicurezza informatica per le PMI:

https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

5.3 Sistemi industriali di controllo

Dopo che negli ultimi anni gli esperti di sicurezza delle TIC hanno scoperto i sistemi industriali di controllo e i sistemi SCADA come campo di ricerca e di collaudo, essi si dedicando ora, in misura crescente, anche alle componenti integrate nelle auto, nei treni, nelle navi e negli aerei. L'interconnessione di differenti apparecchi e la tendenza verso un collegamento costante a Internet non si arrestano infatti neppure di fronte ai mezzi di trasporto. Compagnie aeree, operatori ferroviari e armatori intendono offrire ai loro passeggeri un accesso a Internet e anche le auto sono sempre più spesso collegabili alla rete.

A questo proposito occorre distinguere due aspetti: l'accesso all'offerta di informazioni e proposte d'intrattenimento su Internet da un lato e l'impiego dell'elettronica e della tecnologia dell'informazione per il controllo operativo del mezzo di trasporto e/o a supporto del conducente dall'altro.

Mentre nel primo caso l'accesso al World Wide Web è implicito, nel secondo caso occorre effettuare una seconda distinzione tra applicazioni che devono poter reperire informazioni dall'esterno (ad esempio dati GPS, comunicazioni meteo o informazioni sulle code) e sistemi prettamente interni: nel caso di un auto, ad esempio, la spia del serbatoio, il sistema di monitoraggio della pressione dei pneumatici o la fotocamera posteriore ma anche sistemi di assistenza che mantengono costante la distanza dal veicolo antistante attraverso l'interazione di sensori e attuatori, che frenano e accelerano nel traffico a singhiozzo e che parcheggiano autonomamente.

[37] http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (stato: 31 agosto 2015)

[38] http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (stato: 31 agosto 2015)

5.3.1 La sicurezza nel settore automobilistico

Mettersi in contatto con le auto per via elettronica non è possibile solo da quando queste sono collegate a Internet tramite la rete di telefonia mobile: alcuni malintenzionati hanno già saputo sfruttare a proprio vantaggio le chiusure elettroniche delle portiere, sia copiando il segnale inviato dalla chiave per aprire la portiera (questo rischio è stato nel frattempo riconosciuto ed eliminato dalla maggior parte dei produttori) che disturbando il segnale affinché la portiera non ricevesse il segnale di chiusura.

Nel frattempo le auto si stanno trasformando sempre più in veri e propri computer su ruote: così, spesso in officina il primo passo consiste nel collegare un computer portatile diagnostico all'auto per rilevarne le condizioni. Tramite una simile interfaccia è possibile accedere in modo completo all'elettronica dell'auto – è previsto che sia così e non costituisce una falla di sicurezza in sé (*it's not a bug, it's a feature*). Nonostante queste interfacce costituiscano un vettore di attacco, esse richiedono tipicamente un accesso fisico all'auto. Diversi sistemi comunicano invece tra loro anche senza fili: è il caso, ad esempio, dei sensori della pressione dei pneumatici che trasmettono i valori misurati o del telefono cellulare collegato via *Bluetooth* con l'elettronica dell'auto per consentire l'utilizzo dell'impianto vivavoce integrato. Su vari veicoli viene inoltre installato un collegamento di telefonia mobile per poter inviare e ricevere informazioni via Internet. Questo collegamento non serve soltanto per la manutenzione, ma ha anche allo scopo di consentire, eventualmente, al produttore di rilevare la posizione del veicolo, di aprire le portiere tramite accesso remoto (quando il guidatore ha dimenticato le chiavi del veicolo) o anche di attivare l'immobilizzatore se è stato denunciato il furto dell'auto. Queste funzioni implicano un collegamento delle TIC con l'elettronica del veicolo, che diviene di conseguenza accessibile anche per questa via.

Appare scontato che su di un veicolo i sistemi di intrattenimento debbano essere separati in modo netto dall'elettronica operativa e che l'elettronica operativa debba essere protetta in modo da non poter essere manipolata direttamente dall'esterno né tramite apparecchi per la manutenzione compromessi. Tuttavia i produttori non rispettano sempre questa regola, come hanno recentemente dimostrato alcuni ricercatori in diverse occasioni e nel caso di diverse marche automobilistiche.

In molti casi le diverse componenti non sono sufficientemente schermate tra loro. Ciò porta a hackeraggi astuti quali la manipolazione dei sistemi di assistenza tramite malware precedentemente instillato tramite CD dall'autoradio o addirittura attraverso il *Radio Data System (RDS) VHF*. [39] Se possono essere lanciati comandi a sistemi di assistenza – tramite un malware o un collegamento diretto senza fili – diviene eventualmente possibile accelerare, frenare o guidare il veicolo. Anche la contraffazione dei valori rilevati dai sensori consente di provocare reazioni inappropriate dei sistemi di assistenza.

Qualsiasi comunicazione senza fili all'interno dell'auto deve essere crittografata affinché non possa essere facilmente intercettata e registrata. Le diverse componenti dovrebbero inoltre autenticarsi a vicenda. Con queste misure, immettere comandi arbitrari o valori errati dei sensori diventa decisamente più difficile. Occorre inoltre garantire che le componenti che devono comunicare via Internet non possano essere sfruttate illecitamente come porte d'accesso all'elettronica dell'auto.

[39] http://www.bbc.com/news/technology-33622298 (stato: 31 agosto 2015).

5.3.2 Reboot del Boeing 787 Dreamliner

Talvolta la panacea adottata quando l'applicazione per l'ufficio rifiuta di fare ciò che desidera il collaboratore sembra essere efficace anche nel caso degli aerei: il riavvio del computer non si rivela provvidenziale solo nel caso del computer per uso privato o aziendale, bensì in alcuni casi persino sul Dreamliner della Boeing.[40]

Anche sul Dreamliner è installato molto software. Nell'ambito di test di laboratorio interni alla Boeing, durante i controlli del software di comando dei generatori responsabili della produzione di corrente elettrica, è stato osservato che dopo 248 giorni questi passano in modalità «fail safe» a causa di un sovraccarico del contatore. Per l'aereo ciò comporta un'interruzione di corrente. La soluzione più semplice consiste dunque nel riavviare il software di comando del Dreamliner.

I passeggeri non devono preoccuparsene, per fortuna, poiché il riavvio viene effettuato durante ogni manutenzione di routine e il sovraccarico del contatore può essere così evitato con successo.

5.3.3 Sistemi di intrattenimento e informazione in aereo

Il ricercatore americano Chris Roberts, attivo nel settore della sicurezza delle TIC, afferma di aver rilevato delle falle nei sistemi di intrattenimento dei passeggeri (IFE) dei modelli di aerei Boeing 757-200, Boeing 737-800, Boeing 737-900 ed Airbus A-320 che permetterebbero di accedere ad sistemi critici dell'elettronica di bordo. Il 13 febbraio 2015 Roberts ha informato spontaneamente l'US Federal Bureau of Investigation (FBI) in merito ai risultati ottenuti, nella speranza che le falle di sicurezza venissero eliminate. Il 15 aprile è stato arrestato dall'FBI dopo aver accennato al fatto di essere in grado di manipolare il controllo delle maschere d'ossigeno. Gli apparecchi che aveva con sé sono stati sequestrati.

Dalla richiesta di un mandato di perquisizione[41] del 17 aprile 2015 per il caso Roberts si evince che Chris Roberts aveva con sé diversi utensili che gli avrebbero consentito di effettuare test di penetrazione negli ambienti di rete più svariati. Da Roberts sono stati inoltre messi al sicuro schemi di cablaggio e dell'ulteriore documentazione tecnica sui sistemi di navigazione aerea e d'informazione. Alcuni specialisti di avionica hanno confermato che i comandi di controllo nei rispettivi protocolli esistono davvero. Quando dopo l'arresto all'aeroporto di Syracuse sono stati esaminati i sedili dell'aereo sui quali era seduto Roberts, è stato riscontrato che aveva cercato di rimuovere i rivestimenti dei *seat electronic box* dei due sedili davanti. Roberts dichiarò di aver ottenuto così accesso al sistema IFE con connettori modificati ai cavi Ethernet portati con sé e di essere quindi riuscito ad avere accesso, con metodi di *penetration testing*, ad ulteriori sistemi di bordo.

Nel caso specifico di Roberts appena descritto è da ritenere che quest'ultimo abbia quanto meno cercato di penetrare nei sistemi IFE ed eventualmente anche in altre parti della rete. In presenza di misure di sicurezza insufficienti avrebbe posseduto le competenze specialistiche necessarie e gli strumenti idonei per svolgere una simile operazione. Il successo di questo modo di agire non può essere pertanto completamente escluso. È tuttavia anche plausibile che abbia cercato di gonfiare i fatti per farsi pubblicità.

---

40 https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-10066.pdf (stato: 31 agosto 2015)

41 http://www.wired.com/wp-content/uploads/2015/05/Chris-Roberts-Application-for-Search-Warrant.pdf (stato: 31 agosto 2015)

5.3.4 Blackout – sospettato ma non confermato il movente cibernetico

Spesso scopriamo quanto una cosa ci sia necessaria solo quando essa cessa di funzionare: è ciò che devono aver pensato, lo scorso 27 marzo, molti olandesi. Dopo un blackout su vasta scala, infatti, semafori, mezzi di trasporto pubblici e antenne di telefonia mobile hanno smesso di funzionare. I supermercati sono stati costretti a chiudere perché le casse elettroniche ed i dispositivi antifurto non funzionavano più. Gli ascensori hanno dovuto essere evacuati e le scuole chiuse.[42] All'aeroporto di Schiphol sono stati cancellati dei voli. Sebbene singole voci affermassero che dietro al blackout ci fosse un attacco da parte di hacker, la vera causa è da attribuire a un sovraccarico in una stazione di trasformazione in un sobborgo di Amsterdam. In passato è stato più volte dimostrato che un difetto in un punto centrale dell'erogazione di corrente può provocare una reazione a catena.

Le speculazioni relative a un attacco da parte di hacker si sono rinfocolate quando il 31 marzo 2015, poco dopo i fatti di Amsterdam, un altro blackout ha messo in ginocchio ampie zone della Turchia: la corrente è saltata nelle città di Istanbul, Ankara e Izmir. Nel complesso, il blackout sembra aver interessato 30 delle 81 province turche. Altre fonti parlano addirittura di 80 province colpite. Solo dopo dieci ore il ministero dell'energia turco ha annunciato di aver ripristinato ovunque l'approvvigionamento elettrico. Nelle due metropoli di Istanbul e Ankara alcune aziende private si erano premunite in vista di simili eventualità dotandosi di generatori di emergenza. Per questo, nelle due città le conseguenze del blackout sono state limitate. Esso ha però avuto gravi conseguenze per i trasporti pubblici, ad esempio sulla metropolitana che passa sotto il Mar di Marmara. Anche in questo caso non è stato possibile confermare le voci relative a un attacco da parte di hacker. Il blackout sembra essere stato infatti provocato dall'interruzione nel funzionamento di diverse centrali e dalle conseguenti fluttuazioni della tensione.

5.3.5 Stazioni di benzina statunitensi attaccabili via Internet

Una corsa sulla «Route 66» ed ecco che l'indicatore di livello del serbatoio punta verso il basso. La piccola stazione di benzina distante dall'abitato offre speranza, ma la pompa di benzina è vuota. Una prospettiva molto sgradevole. Eppure, non necessariamente la pompa di benzina è realmente vuota. Infatti, nel caso delle stazioni di benzina statunitensi gestite da remoto, per via della loro posizione dislocata, sono stati riscontrati problemi di sicurezza legati agli indicatori di livello automatizzati[43]: il 3%dei circa 150 000 indicatori di livello delle pompe di benzina controllate via Internet erano accessibili senza alcuna protezione e soprattutto liberamente configurabili. Attraverso la modifica delle impostazioni sarebbe dunque possibile far credere che una stazione di benzina con le pompe vuote disponga ancora di riserve a sufficienza, inducendo così i responsabili a non provvedere al rifornimento. Per mezzo di comandi specifici le pompe di benzina potrebbero inoltre essere messe fuori servizio senza problemi.

---

42 http://nos.nl/artikel/2027141-noord-holland-heeft-weer-stroom.html (stato: 31 agosto 2015)

43 https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges (stato: 31 agosto 2015)

Quando è assolutamente necessario, l'accesso remoto deve essere soggetto a una procedura di protezione adeguata. Il seguente documento di MELANI fornisce diverse raccomandazioni al riguardo:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/misure-di-protezione-dei-sistemi-industriali-di-controllo--ics-.html

5.4 Attacchi (DDoS, *defacement*)

5.4.1 Schermo nero su TV5 Monde

Tra i numerosi attacchi avvenuti nei primi sei mesi del 2015, quello che lo scorso 8 aprile ha colpito la catena televisiva francofona TV5 Monde ha indubbiamente lasciato il segno tra la popolazione. È infatti la prima volta che un'emittente televisiva viene colpita così aggressivamente, non soltanto attraverso il proprio sito Internet ma, soprattutto – ed è questo che caratterizza la natura inedita dell'attacco – tramite l'immobilizzazione del suo apparato di produzione.

5.4.1.1 Dinamica dell'attacco

L'8 aprile 2015 l'emittente televisiva TV5 Monde ha subito un attacco diversificato che ha colpito vari impianti di produzione e piattaforme. L'aspetto più spettacolare ha riguardato l'infrastruttura di diffusione dei programmi e ha costretto l'emittente a cessarne la diffusione a partire dalle 22. Solo tre ore più tardi essa ha potuto riprendere possesso dell'antenna, dapprima trasmettendo programmi preregistrati. In parallelo a ciò, la catena ha perso il controllo dei propri account di Facebook e Twitter, che le sono stati sottratti per diffondere messaggi di sostegno al jihad. È stato inoltre deturpato il sito Web dell'emittente. Infine, secondo informazioni provenienti da fonti aperte, l'attacco avrebbe consentito di colpire e rendere inagibile la comunicazione via e-mail all'interno dell'azienda. L'attacco è stato tempestivamente rivendicato da un gruppo che si fa chiamare «Cyber Caliphate» e dichiara fedeltà allo Stato Islamico. L'esatta identità di questo attore e del mandante dell'attacco si è tuttavia rivelata meno chiara in seguito, ricordandoci quanto sia tuttora spinoso il processo di attribuzione delle responsabilità di un attacco (cfr. più in basso).

5.4.1.2 Presunta vulnerabilità dell'apparato di produzione

L'assunzione del controllo degli account di social network è un tipo di incidente osservato di frequente, in particolare nell'ambito di attacchi volti a diffondere un messaggio di sostegno al jihad. La capacità di attaccare l'apparato di produzione di una grande emittente televisiva costituisce invece un elemento innovativo. Più precisamente, è l'infrastruttura che serve a diffondere i programmi dell'antenna (*encoder* e *multiplexer*) a essere stata attaccata. Questo fatto solleva naturalmente la questione dell'esposizione a pericoli informatici di questo tipo di infrastruttura. A meno di un accesso fisico agli apparecchi, che consente ad esempio di propagare un'infezione attraverso una chiavetta USB, l'attacco presuppone infatti un accesso remoto. Secondo informazioni provenienti da fonti aperte, diversi sistemi dell'emittente erano visibili via Internet, aumentando così la superficie d'attacco. La seconda questione che emerge da questo tipo di attacchi riguarda la separazione tra il sistema di burotica e il sistema di produzione. Non sono noti dettagli su questo aspetto, ma alcuni esperti hanno formulato l'ipotesi dell'esistenza di carenze a questo livello. È vero anche che, in alcuni casi, è il sistema di burotica a essere infettato per primo, per cui, in mancanza di un'efficace compartimentazione, il sistema di produzione può essere a sua volta colpito.

Indipendentemente dalle misure adottate prima dell'attacco, l'incidente che ha coinvolto TV5 Monde ci ricorda che qualsiasi sistema industriale di controllo deve essere protetto.

Quando è assolutamente necessario, l'accesso remoto deve essere soggetto a una procedura di protezione adeguata. Il seguente documento di MELANI fornisce diverse raccomandazioni al riguardo:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/misure-di-protezione-dei-sistemi-industriali-di-controllo--ics-.html

5.4.1.3 Il difficile lavoro di attribuzione

All'indomani degli attacchi nessun commentatore ha messo in dubbio l'attribuzione della responsabilità a un gruppo islamista attivo su Internet. È stato discusso unicamente il coinvolgimento dello Stato islamico. Solo nel mese di giugno, però, nuovi elementi hanno indirizzato i commenti relativi all'attribuzione della responsabilità dei fatti in un'altra direzione. In primo luogo gli autori erano penetrati nella rete già all'inizio dell'anno. In seguito essi avevano dunque potuto esplorare con calma e muoversi lateralmente per individuare i sistemi interessanti. Questa prima informazione costituisce un indizio del livello relativamente elevato di professionalizzazione dell'hacker. Ma, soprattutto, alcune rivelazioni giornalistiche, a loro volta basate su analisi delle società di servizi di sicurezza Trend Micro e FireEye, suggeriscono una nuova pista, quella di un legame tra questo attacco e una campagna di spionaggio cibernetico presumibilmente russa, di origine statale, nota con il nome di «Sofacy» (e conosciuta anche come Pawn Storm e APT28). Questi parallelismi si basano su diversi indicatori rilevati sulle reti di TV5 Monde che potrebbero far parte dell'infrastruttura di Sofacy. La presenza di Sofacy sulle reti di TV5 Monde sembra certa; invece, il legame tra questa campagna e l'attacco del aprile del 2015 che ha causato in particolare l'interruzione dei programmi rimane soggetta a diverse interpretazioni. Una prima ipotesi è quella di un attacco di fatto sferrato dal gruppo intorno a Sofacy, che avrebbe tentato di dirottare la responsabilità nella direzione errata della pista islamista («false flag»). Il principale punto debole di questa interpretazione è che questo tipo di attacchi non è in linea con i metodi e le finalità di Sofacy, una campagna di spionaggio estremamente furtiva. Inoltre, l'interesse potenziale di un presunto attore statale russo per questo tipo di operazione è poco evidente, anche se a suo tempo erano note tensioni tra la Francia e la Russia sul piano diplomatico.[44]. In base a una seconda ipotesi, Sofacy sarebbe stato implementato da gruppi simpatizzanti del jihad. Questa spiegazione non è tuttavia avvallata da alcun elemento concreto e richiederebbe una spiegazione delle modalità di acquisizione del malware da parte dei gruppi in questione. La terza ipotesi, a nostro giudizio la più verosimile, è quella di due operazioni parallele non collegate tra loro. Un interesse di un attore statale russo per media quali TV5 è in effetti assolutamente plausibile. Come d'abitudine, però, la volontà dell'autore della campagna sarebbe in questo caso quella di penetrare nella rete per acquisirvi, nel corso del tempo, informazioni sensibili. In parallelo a ciò, un'operazione cibernetica condotta da un altro attore e avente quale obiettivo principale quello di divulgare un messaggio di sostengo al jihad avrebbe causato invece i danni evidenti riscontrati in gennaio.

[44] Le frizioni derivano dall'accordo per la vendita di due navi da guerra francesi terminato con l'annullamento della stessa.

5.4.1.4 I media, un bersaglio privilegiato

Nel suo rapporto semestrale 2014/1[45], MELANI aveva già sottolineato come i media costituissero obiettivi particolarmente ambiti – e vulnerabili – per gli attacchi informatici. L'attacco contro TV5 conferma questa tendenza che non riguarda unicamente la stampa scritta. I media sono interessanti perché trattano un gran numero di informazioni talvolta sensibili ma anche perché possono offrire una cassa di risonanza più ampia a un attore che desidera divulgare un messaggio di propaganda o diffondere informazioni falsificate. D'altronde alcuni elementi legati all'attività di un mezzo d'informazione sono poco compatibili con le esigenze di sicurezza, che dovrebbero essere giustamente particolarmente elevate. Basti pensare, ad esempio, alla necessità di poter passare rapidamente dalla ricezione al trattamento e quindi alla pubblicazione di un'informazione. D'altro canto a volte può risultare difficile istituire dei protocolli di comunicazione protetti in presenza di una molteplicità di corrispondenti, talvolta indipendenti, mobili e ubicati in molti luoghi diversi. Occorre infine sottolineare che gli attori che mirano a questo tipo di obiettivo dispongono spesso di molte più risorse da destinare all'attacco di quante ne abbiano a disposizione i media per difendersi.

A fronte della vasta gamma di rischi a cui sono soggetti i media (p.es. DDoS, spionaggio, sabotaggio), conviene loro integrare procedure di sicurezza sia preventive che reattive. L'azienda deve essere in grado in particolare di rilevare le intrusioni o altri eventi anomali e di adottare misure di emergenza adeguate ai diversi scenari.

5.4.2 Attacco cibernetico: cancellati voli di Polish Airlines

Gli attacchi cibernetici a mezzi di trasporto quali le ferrovie o gli aerei suscitano particolare interesse e anche alcuni timori. Lo scorso 21 giugno 2015, una notizia di questo tipo ha fatto scalpore, facendo temere in un primo momento un pesante attacco. Un attacco da parte di hacker al sistema informatico della compagnia aerea «Polish Airlines (LOT)» avrebbe infatti costretto quest'ultima a cancellare diversi voli, poiché avrebbe reso impossibile generare i piani di volo attraverso il sistema colpito. I piani di volo contengono, ad esempio, dati sull'aeroporto di decollo e di atterraggio, nonché sulla rotta aerea. L'attacco avrebbe interessato complessivamente 1400 passeggeri di voli aerei. Questi dati vengono utilizzati tra l'altro dai controllori del traffico aereo per mantenere gli aerei su una rotta aerea sicura. Se questi dati non possono essere trasmessi o stampati, gli aerei non possono neppure decollare. Non sono state tuttavia fornite indicazioni relative ai retroscena.[46]

Il giorno seguente il portavoce ha indicato come motivo un sovraccarico della rete che sarebbe stato causato da un attacco di negazione del servizio. Non è stato riferito se quest'attacco fosse o meno mirato. Restano poco chiare, inoltre, la natura e le proporzioni dell'attacco. Di norma i sistemi critici che necessitano un collegamento a Internet devono essere protetti, in particolare contro gli *attacchi DDoS*. Il CEO della LOT Sebastian Mikosz ha spiegato che si tratta di un problema generale riguardante tutto il settore e che è prevedibile che le stesse cose possano accadere in qualsiasi momento e ovunque.

---

[45] MELANI Rapporto semestrale 2014/1, capitolo 5.2: https://www.melani.admin.ch/melani/it/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-1.html (stato: 31 agosto 2015)

[46] http://www.reuters.com/article/2015/06/22/us-poland-lot-cybercrime-idUSKBN0P21DC20150622 (stato: 31 agosto 2015)

Ruben Santamarta, consulente di sicurezza presso IOActive, ha notato dal canto suo che potrebbe trattarsi di un'inversione di tendenza nel settore delle linee aeree e che questo settore sarebbe ora appetibile anche agli occhi dei criminali cibernetici. In effetti negli ultimi mesi si rileva un maggiore interesse per i sistemi di sicurezza nell'aviazione. Lo dimostra ad esempio il caso illustrato al capitolo 5.3.3, riguardante un tentativo di infiltrazione nel settore critico del controllo dell'aeromobile passando attraverso il sistema di intrattenimento e informazione.

Negli ultimi tempi si osserva una crescente attenzione degli esperti di sicurezza IT per i mezzi e per i sistemi di trasporto. Tuttavia, ad essa potrebbe forse essere collegato anche un interesse da parte dei criminali cibernetici. In generale occorre sempre distinguere tra sistemi che devono essere necessariamente collegati a Internet e sistemi che non sono collegati a Internet per motivi di sicurezza. Rientrano nella prima categoria ad esempio i sistemi di contabilizzazione nonché tutti i sistemi che comportano uno scambio tra diversi servizi. Qui i modelli operativi classici, come l'estorsione *DDoS* o il furto di dati degli utenti con successivo ricatto, funzionano esattamente come in ogni altro settore. A questo proposito è da prevedere che in futuro anche questi sistemi finiscano con l'essere (come in tutti gli altri settori) bersaglio dei criminali cibernetici. Appare tuttavia esagerato parlare di un'inversione di tendenza nell'aviazione con riferimento al caso in oggetto.

5.4.3 Attacchi cibernetici nella scia di Charlie Hebdo

L'attacco alla redazione parigina di Charlie Hebdo nel gennaio del 2015 ha avuto conseguenze anche per Internet, conseguenze che non sono tuttavia in alcun modo paragonabili a quelle di un attacco fisico. Sebbene il numero di attacchi virtuali, stimato in alcuni momenti attorno a 25 000, sia elevato, non lo è però altrettanto la loro qualità. Nella maggior parte dei casi si tratta di cosiddetti *defacement* (deturpamenti), in cui vengono sfruttate falle di sicurezza dei siti Web per pubblicarvi slogan politici o religiosi. In questi casi sono state pubblicate frasi come «Morte alla Francia» o «Morte a Charlie Hebdo». La maggior parte degli attacchi è stata operata da gruppi denominati «Middle East Cyber Army», «Fallaga team» e «Cyber Caliphate». Gli attacchi sono stati operati in modo poco concertato, anzi piuttosto arbitrario; ciò corrisponde al modo di agire abitualmente adottato in questo tipo di attacchi. Sono state colpite ad esempio scuole, università, chiese e aziende. Le vittime non vengono scelte in modo mirato. Gli autori cercano piuttosto sistemi vulnerabili le cui falle di sicurezza vengono quindi sfruttate in modo sistematico. Sono soprattutto gli hacker spinti da motivi religiosi a servirsi di questo tipo di metodi. Mentre, in condizioni normali, gli attacchi sono distribuiti in tutto il mondo, in caso di particolari avvenimenti le forze vengono concentrate consistentemente contro chi viene ritenuto colpevole di aver provocato la rabbia degli aggressori. Le conseguenze di questi attacchi sono state osservate anche nella Svizzera romanda (cfr. n. 3.4.2).

Una cellula belga di Anonymous è intervenuta a sua volta nel conflitto e annunciando di voler seguire in una controiniziativa tutte le attività jihadiste online con l'intenzione di bloccare i rispettivi account su Twitter, YouTube e Facebook.

5.4.4 Hacker bloccano il sito Web dell'esercito statunitense

Nel giugno del 2015 le forze armate statunitensi si sono viste confrontate con un attacco alla propria infrastruttura Web. In questo contesto sul sito Web pubblico www.army.mil sono stati diffusi messaggi di propaganda e il sito ha dovuto essere tolto temporaneamente dalla rete. Poiché sul sito non erano salvati dati riservati o personali, non è stato possibile neppure

rubarli. La «Syrien Electronic Army» ha rivendicato l'attacco via Twitter. Il gruppo era già stato notato diverse volte in precedenza per i suoi attacchi, rivolti soprattutto contro diversi media[47]. Non si tratta qui principalmente di un furto di dati, bensì di disinformazione e pubblicazione di dichiarazioni politiche. Il Pentagono ha sottolineato che si sarebbe trattato di semplice vandalismo cibernetico.

Già nel mese di gennaio presunti affiliati allo Stato islamico (SI) si erano temporaneamente impossessati degli account di Twitter e Youtube del comando centrale delle forze armate statunitensi (CENTCOM). Durante il momento di follia durato 30 minuti, sull'account di Twitter è stato visualizzato il testo «Cyber Caliphate» e sono state diffuse immagini di propaganda. Anche in questo caso si è trattato più che altro di un semplice attacco e gli hacker si sarebbero impadroniti dei dati d'accesso tramite e-mail di *phishing* mirate (cosiddetto *spear phishing*). Youtube e Twitter offrono ormai metodi di autenticazione a due fattori che rendono difficoltoso realizzare simili attacchi. Sembra tuttavia che questi metodi non fossero ancora in uso al momento degli attacchi nel caso degli account colpiti.

5.4.5 Superfish/Lenovo

Il produttore di computer e notebook Lenovo dotava i propri notebook di default di un software preinstallato denominato «Superfish». Secondo un'indagine condotta da fornitori di servizi di sicurezza per le TIC, si tratta di un *adware* che nel momento in cui viene attivata una ricerca Google integra tra l'altro nel web browser proiezioni di messaggi pubblicitari di terzi.

Nel febbraio del 2015 è stato reso noto che Superfish installa un proprio certificato CA nella memoria dei certificati di Windows. Ciò consente a Superfish di spacciarsi per un qualsiasi sito Web (ad esempio Google) e di integrare, anche nel caso di collegamenti crittografati con HTTPS, opportuni annunci pubblicitari. Poiché la chiave segreta del certificato CA installato da Superfish è contenuta nel programma del software, può essere estratta con tecniche specifiche. Ciò consente agli hacker di emettere certificati per qualsiasi pagina Web, che viene quindi classificata come affidabile dagli apparecchi Lenovo.

Superfish rende dunque vulnerabili gli apparecchi sui quali è preinstallato, ad esempio nei confronti di attacchi del tipo «*Man-In-The-Middle*». In questo modo gli hacker potrebbero teoricamente spacciarsi per una banca e rubare informazioni di login (nome utente, password, token) della vittima per commettere poi una frode di e-banking.

La presa di posizione ufficiale di Lenovo in merito alla problematica legata a Superfish è pubblicata sul sito Web di Lenovo[48].

---

47 Rapporto semestrale MELANI 2013/1, capitolo 4.4: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-1.html (stato: 31 agosto 2015)
Rapporto semestrale MELANI 2013/2, capitolo 4.8: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html (stato: 31 agosto 2015)

48 http://forums.lenovo.com/t5/Lenovo-P-Y-and-Z-series/Removal-Instructions-for-VisualDiscovery-Superfish-application/ta-p/2029206 (stato: 31 agosto 2015)

MELANI raccomanda agli utenti di apparecchi Lenovo di verificare se sul proprio apparecchio risulta installato Superfish ed eventualmente di disinstallare il software. Sul seguente sito Web è possibile verificare se il proprio apparecchio è interessato dalla problematica legata a Superfish.

Superfish, Komodia, PrivDog vulnerability test (inglese)

https://filippo.io/Badfish/

Lenovo ha inoltre messo a disposizione un tool che consente di eliminare Superfish (disinstallazione):

https://support.lenovo.com/us/en/product_security/superfish_uninstall

MELANI raccomanda, per quanto riguarda i computer utilizzati per scopi sensibili, di formattare i nuovi computer e notebook prima della messa in esercizio e di reinstallare quindi il sistema operativo. Questo provvedimento consente di evitare che un software preinstallato superfluo ed eventualmente indesiderato (ad esempio un *adware*) possa interferire con il funzionamento dell'apparecchio o inoltrare dati sensibili a terzi senza che l'utente ne sia a conoscenza.

5.4.6 Exploit kit

Un *exploit kit* è uno strumento che consente agli hacker di sfruttare falle presenti sugli apparecchi finali, sia direttamente nel browser che in programmi di supporto quali Flash, Acrobat Reader o Java.

L'*exploit kit* permette di realizzare in questo contesto un'elevata divisione del lavoro all'intero di aggruppamenti criminali, poiché in genere è strutturato in modo da poter essere gestito anche da chi non possiede conoscenze delle TIC. Di regola si tratta di un'interfaccia Web che mette a disposizione le necessarie funzionalità, quali ad esempio la selezione degli exploit, statistiche degli apparecchi infettati nonché altre possibilità di configurazione.

Di regola il modo di procedere adottato dai diversi gruppi di autori è quasi identico:

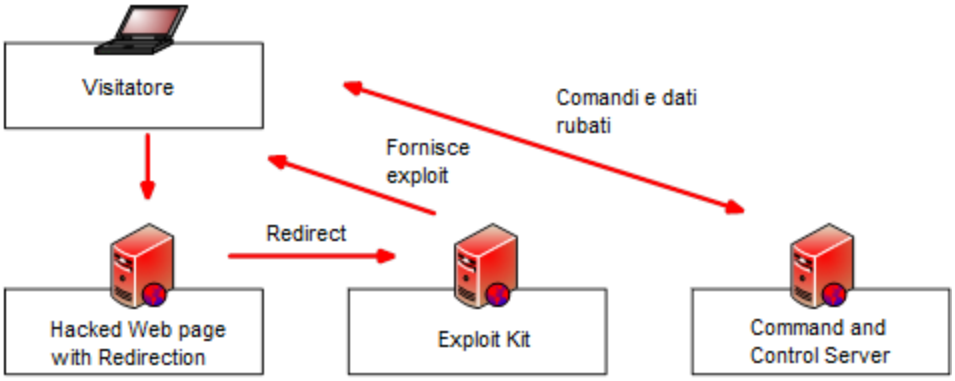


Figura 8:Rappresentazione schematica del funzionamento di un exploit kit

L'hacker reindirizza il maggior numero possibile di vittime potenziali verso il suo exploit kit. Può farlo in diversi modi:

- assumendo il controllo di siti Web realizzati con un CMS vulnerabile e inserendovi un collegamento nascosto al server con l'*exploit kit*. Per questo motivo è essenziale che

tutti gli operatori di un sito Web proteggano il loro CMS e lo tengano sempre aggiornato;[49,50]

- piazzando della pubblicità che indirizza i visitatori verso l'*exploit kit*. Ciò può avvenire tramite l'acquisto di opportuni banner o l'assunzione del controllo di web server vulnerabili;
- acquistando il traffico che gli occorre presso un altro fornitore di servizi. Un sistema di questo tipo è detto *Traffic Distribution System (TDS)*. Non tutti gli operatori di questi sistemi sono criminali: spesso i flussi di visitatori vengono controllati anche in un contesto di legalità.

L'*exploit kit* stesso verifica spesso l'apparecchio finale con *JavaScript* per quanto riguarda i plugin installati e le relative versioni allo scopo di individuare una falla idonea e di poter attaccare con un exploit. Esistono numerosi *exploit kit* con diverse capacità. Gli *exploit kit* più conosciuti sono Angler, Neutrino, Rig, Nuclear e Magnitude. È interessante osservare con quale velocità i singoli *exploit kit* dispongono di exploit idonei alla comparsa di nuove falle. Non tutti gli *exploit kit* dispongono degli stessi exploit; la variabilità è piuttosto ampia in questo contesto.[51] Capita inoltre sempre più spesso che gli *exploit kit* stessi siano provvisti di *0-day exploit*.[52]

Gli *exploit kit* non vengono tuttavia utilizzati soltanto da criminali «comuni», bensì in parte anche da hacker ingaggiati da stati per attività di spionaggio.

5.4.7 Log Jam e lacune FREAK

Nel periodo in analisi sono emerse due falle di una certa entità che possono mettere a rischio la sicurezza dei collegamenti crittografati: «FREAK» e «LogJam». A fare da sfondo a queste due falle è in questo caso il fatto che in passato esistevano delle restrizioni alle esportazioni degli USA per i prodotti crittografici. Nel *source code* delle biblioteche di crittografia sono ancora disponibili le *funzioni di fallback* necessarie a questo scopo che possono essere sfruttate per questa categoria di attacchi.

FREAK (Factoring Attack on *RSA*-EXPORT Keys) consente di accettare chiavi deboli che consentono la decrittografia nel caso di determinati browser. Questo presuppone tuttavia che un browser vulnerabile si colleghi a *cipher* deboli su un server. L'attacco ha interessato una grande quantità di browser e programmi dal lato dei client.[53]

LogJam è un attacco affine a FREAK diretto a collegamenti crittografati con cui il grado di crittografia del collegamento può essere ridotto in misura tale da rendere quest'ultimo decrittografabile. In questi casi i numeri primi utilizzati nel *key exchange* con *Diffie-Hellman* vengono ridotti in modo da rendere possibile la decrittografia.[54]

---

[49] Cfr. anche la lista di controllo di MELANI: Misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti (CMS): https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/misure-per-contribuire-alla-sicurezza-dei-sistemi-di-gestione-de.html

[50] Cfr. anche il capitolo 2 del rapporto semestrale attuale.

[51] http://contagiodump.blogspot.ch/2010/06/overview-of-exploit-packs-update.html (stato: 31 agosto 2015)

[52] http://malware.dontneedcoffee.com/ (stato: 31 agosto 2015)

[53] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204 (stato: 31 agosto 2015)

[54] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000 (stato: 31 agosto 2015)

5.5 Misure preventive

5.5.1 Nuovo Patch Management di Microsoft

Mentre si discute di un Patch Management regolare per i sistemi operativi dei telefoni cellulari, Microsoft intende abolire il tradizionale *patchday* per gli utenti di Windows 10 e introdurre aggiornamenti continuativi. Il *patchday* è stato introdotto soprattutto a fronte delle esigenze degli amministratori nelle grandi aziende, affinché potessero pianificare e testare meglio l'installazione degli aggiornamenti ed evitare così che dopo l'installazione alcuni sistemi critici non funzionassero più.

Microsoft, con il nome di "Windows Update for Business", intende fornire alle aziende una soluzione a questi problemi per mezzo di cosiddetti *distribution ring*. Con questa soluzione una rete viene suddivisa in più anelli. A seconda dell'anello, alcuni sistemi sono sottoposti all'aggiornamento prima degli altri. Solo in un secondo tempo gli aggiornamenti vengono quindi distribuiti anche agli altri computer. Inoltre in questo modo gli aggiornamenti possono essere installati in base ai rischi. I computer che presentano un rischio d'infezione più elevato ricevono l'aggiornamento più rapidamente, gli altri qualche tempo dopo. Gli amministratori possono inoltre stabilire delle finestre di manutenzione in cui installare o meno gli aggiornamenti. Nel caso sistemi critici per le aziende Microsoft intende tuttavia mantenere in essere il *patchday* per ora.[55]

5.6 Altri temi

5.6.1 Furti semplici ma dalle notevoli conseguenze

Lo *smartphone* rappresenta ormai uno strumento imprescindibile della società moderna che consente di ascoltare musica, leggere le e-mail, gestire appuntamenti o misurare prestazioni sportive. Affidiamo ormai quasi tutti i nostri dati allo smartphone. È chiaro che così facendo esso diventa un bersaglio appetibile per criminali di tutti i tipi. Nel caso degli apparecchi elettronici, in particolare, si pensa in primo luogo a metodi d'attacco elettronici, sia che si tratti del furto di dati tramite un *malware* che di tentativi di ricatto operati, ad esempio, tramite *ransomware*. Nel giugno del 2015 su alcuni media tedeschi circolavano messaggi di monito che invitavano a non trascurare neppure i metodi di ricatto tradizionali. In Germania si registra un aumento dei furti di smartphone e laptop a scopo di ricatto tra i manager e gli uomini d'affari. Il calo dei prezzi degli smartphone e le misure di sicurezza sempre più difficili da aggirare rendono il furto vero e proprio di questi apparecchi sempre meno interessante ma, se su di essi sono presenti dati molto preziosi per una persona o per la sua azienda o i suoi clienti, un furto di questo tipo può facilmente risultare conveniente dal punto di vista economico.

Ha fatto notizia il furto di cui è caduto vittima Dieter Kempf, una personalità leader nel mondo dell'informatica. Il direttore generale della società fornitrice di servizi Datev e presidente dell'associazione tedesca dell'IT BITKOM si stava recando al 14° congresso tedesco dell'informatica, nell'ambito del quale avrebbe dovuto moderare una tavola rotonda sul tema della «comunicazione mobile sicura». Quando il stava per salire sul treno, tre persone si sono avvicinate e gli hanno sottratto il notebook e un Blackberry. La descrizione dei fatti coincide con quella fatta da altre vittime: i ladri agiscono in piccoli gruppi, generalmente nelle

[55] http://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/ (stato: 31 agosto 2015)

ore di punta, sui treni o nelle stazioni, e derubano persone che hanno l'aria di essere uomini d'affari.

Non si tratta in questo caso di criminali cibernetici che si procurano fisicamente un accesso ai dati, quanto piuttosto di comuni borseggiatori che hanno capito di poter trarre profitto da questo modus operandi. Una vera e propria ondata di rapine appare tuttavia poco probabile, perché i ladri devono agire sul posto e corrono grandi rischi nell'avvicinare la vittima. In ogni caso l'esempio mostra in modo emblematico che gli strumenti IKT e i dati riservati sono esposti a molti rischi.

Le seguenti misure aiutano a tutelarsi contro questo tipo di ricatto:

- Assicuratevi che le misure di sicurezza del vostro *smartphone* siano attivate correttamente (p.es. inserimento del PIN e blocco automatico del display).
- Non salvate informazioni aziendali riservate sui vostri apparecchi privati.
- Non lasciate mai incustoditi gli apparecchi che contengono dati riservati.
- Assicurate regolarmente i vostri tati (Backup / Cloud-Sync) così da non rischiare di perdere, insieme a un apparecchio elettronico anche tutti i dati che vi sono registrati.
- misure di sicurezza contro i furti (ad es.. „find my iPhone")
- Assicurazione nel caso di furto di apparecchiature e di dati

6 Tendenze e prospettive

6.1 Quando i dati hanno una doppia vita

La problematica della raccolta di dati personali e della successiva catena di elaborazione di questi dati è già stata affrontata nell'ultimo rapporto semestrale.[56] Spesso in questo contesto viene indicato come problema principale il possibile abuso dei dati da parte di aziende e privati. Poco tematizzato è invece il modo in cui i singoli individui possono procedere se un'amministrazione pubblica o un'autorità di vigilanza commette errori, come nel caso illustrato di seguito. Mancano consigli riguardo alle misure che gli interessati possono intraprendere per rendere retroattive le informazioni errate e soprattutto per prevenirle.

Le cose si fanno problematiche ad esempio nel caso di due persone con lo stesso nome e la stessa data di nascita che vivono in Svizzera. Queste persone sono soggette a diversi intoppi a cui è collegato un rischio giustificato di confusione. In un articolo intitolato «Verwechslung – Der doppelte Moser» Il «Beobachter», una rivista svizzera dei consumatori, ha riferito di un caso concreto di questo tipo. L'accaduto dimostra in modo emblematico come possono essere risolti i problemi nel singolo caso, ma anche come il diretto interessato sia costretto senza colpa a richiedere ripetutamente una rettifica. Le persone citate, Peter Moser di Ipsach e Peter Moser di Winterthur, sono nate lo stesso giorno e vengono confuse dall'AVS e anche da altre aziende o autorità.[57]

Lo scorso semestre MELANI è stata informata di un caso analogo. Il caso riguardava un cittadino svizzero che aveva un omonimo con la stessa data di nascita. La persona annunciatasi a MELANI, indicata di seguito come l'informatore[58], si distingue dall'altra unicamente per il secondo nome di battesimo. La serie di confusioni è iniziata con un'iscrizione nel casellario giudiziale ricevuta dall'informatore, ma in realtà destinata al suo omonimo. È spiacevole doversi difendere contro un decreto d'accusa con cui non si ha nulla a che fare. Altri scambi si sono verificati presso le casse malati, le autorità fiscali e le amministrazioni comunali in seguito a cambiamenti di domicilio. Persino l'organo di mediazione, informato del problema, ha confuso l'informatore con il suo omonimo nel fornire una risposta. In tutti i casi l'onere della prova era a carico della vittima, sebbene l'errore fosse stato commesso ogni volta dall'azienda o dall'autorità in questione. In altri casi l'informatore è riuscito per poco a impedire confusioni che avrebbero portato a un divieto d'entrata in alcuni Paesi o a un'attribuzione errata di dati biometrici all'ufficio passaporti intervenendo attivamente presso i servizi interessati. Se la vittima non fosse intervenuta, il sistema avrebbe nuovamente fallito.

Nell'ottica degli interessati, il problema centrale è costituito dal fatto che i problemi descritti sopra sono sempre riconducibili al medesimo errore, lo scambio di identità. I diretti interessati sono tuttavia costretti a rivolgersi in ogni singolo caso al servizio competente per il settore o l'unità amministrativa ecc. Ciò comporta per tutti gli interessati un enorme carico di lavoro di cui non sono in alcun modo responsabili e che viene loro indennizzato solo in rarissimi casi. Essi sono dunque costretti a risolvere ogni problema singolarmente e a più

---

[56] Rapporto semestrale MELANI 2014/2, capitolo 5.1: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (stato: 31 agosto 2015)

[57] http://www.beobachter.ch/justiz-behoerde/buerger-verwaltung/artikel/verwechslung_der-doppelte-moser/ (stato: 31 agosto 2015)

[58] Nome noto alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione

riprese in quanto non esiste un interlocutore centrale che potrebbe assumersi la responsabilità per la causa dell'identificazione errata trasversalmente per tutte le istituzioni coinvolte e farsi carico del coordinamento di tutti gli interessati. A causa della velocità dell'ulteriore elaborazione delle informazioni errate, inoltre, non tutti i sistemi vengono automaticamente aggiornati dopo la rettifica della fonte; ciò implica a sua volta un ulteriore carico di lavoro per gli interessati.

A fronte di accordi imminenti ad esempio nel campo dello scambio automatico di informazioni (SAI), i problemi legati a uno scambio di identità possono estendersi rapidamente a livello internazionale, aggravando così ulteriormente la problematica della rettifica delle attribuzioni errate. Nel negoziare i nuovi accordi e le nuove leggi non si dovrebbe dunque porre l'accento soltanto sull'eliminazione degli abusi del sistema da parte di singoli individui, bensì, anche sulla necessità di garantire la qualità del sistema. Dovrebbe inoltre essere garantita la possibilità di correggere facilmente eventuali errori.

6.2 Questione di vita o di morte – le TIC nel settore della sanità

Le pompe da infusione sono strumenti pratici nei trattamenti medici quotidiani che consentono di predisporre automaticamente il giusto dosaggio del farmaco da somministrare per la rispettiva patologia. L'idea che il contenuto del tubo per infusione che sfocia nel corpo possa essere controllato da un esterno è dunque molto inquietante.

Nell'ultimo rapporto semestrale abbiamo analizzato la problematica dell'interconnessione totale di un numero crescente di apparecchi nell'ambito dell'Internet delle cose (*Internet of Things (IoT)*). Questa tendenza non si arresta neppure di fronte agli strumenti medici. Con la loro interconnessione entra tuttavia in gioco anche l'intera gamma di rischi ad essa associata. Billy Rios, ricercatore attivo nel settore della sicurezza, ha rilevato delle lacune nel caso delle pompe da infusione del marchio Hospira.[59] In un primo momento è riuscito unicamente a manipolare i limiti al raggiungimento dei quali l'infermiere responsabile riceve un messaggio di avvertimento. Nel corso di altri esperimenti Rios è riuscito però anche a manipolare il dosaggio da remoto. All'inizio di giugno del 2015 il ricercatore lo ha comunicato alla ditta produttrice e all'autorità di regolamentazione americana competente, la «US Food and Drug Administration (FDA)». La FDA ha emanato un avvertimento ufficiale[60] a fine luglio, in teoria un lasso di tempo sufficiente per verificare nella pratica i risultati della ricerca e testare la falla rilevata. Dal tenore dell'avvertimento emerge inoltre un ulteriore problema: sebbene la FDA raccomandi di staccare le pompe da infusione dalla rete, essa avverte però al contempo che, in tal caso, le banche dati dei dosaggi dovranno essere gestite manualmente. Ciò creerebbe dunque nuove fonti di errore. In molti settori ci si abitua in fretta alle funzionalità supportate dalle TIC. Occorre tassativamente impostare nel miglior modo possibile la sicurezza delle automatizzazioni e definire i livelli di funzionamento ridotto in caso di problemi.

Nella scia della tendenza verso l'Internet delle cose vengono automatizzati e interconnessi componenti e processi sempre nuovi. Oltre alle nuove possibilità e ottimizzazioni che queste applicazioni offrono all'utente, esse pongono tuttavia i responsabili di fronte a nuovi problemi. Un caso esemplificativo è quello del Boeing Dreamliner riportato al numero 5.3.2, per correggere i problemi si preferisce praticare un *workaround* funzionante piuttosto che

[59] http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/ (stato: 31 agosto 2015)

[60] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm (stato: 31 agosto 2015)

modificare la configurazione omologata attraverso una *patch* mirata, poiché quest'ultima potrebbe implicare una ricertificazione dei sistemi.

Non sono solo gli utenti a essere confrontati con nuovi problemi: anche gli organi di regolamentazione dei rispettivi settori devono occuparsi sempre più spesso delle tematiche legate alle TIC. Nel caso dei prodotti medici, la direttiva «93/42/CEE» decide in merito all'autorizzazione del prodotto all'interno dell'Unione europea e anche in Svizzera. Le 65 pagine dedicate alle TIC contengono il termine «software» solo in un unico passaggio specifico: «Per i dispositivi che incorporano un software o costituiscono in sé un software medico, il software è convalidato secondo lo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione dei rischi, della validazione e della verifica.»

A tale riguardo lo stato della tecnica è definito nella norma «EN62304», una norma del 2006 completa dal punto di vista metodologico relativa al ciclo di vita del software dei dispositivi medici. Se viene riscontrata una falla, il problema spesso non risiede soltanto nel dispositivo in questione, bensì anche nella configurazione insufficiente delle reti circostanti.

Chi si sta già occupando intensamente dei nuovi rischi sono gli assicuratori. Per loro, essi implicano naturalmente la possibilità di nuovi modelli operativi. Chi non riesce a controllare in prima persona i rischi legati all'interconnessione intelligente può quanto meno sopperire in altro modo alle possibili conseguenze finanziarie.

7 Politica, ricerca, policy

7.1 Atti parlamentari

Atto parlamentare	Numero	Titolo	Depositato da	Data del deposito	CN/CS	Ufficio	Stato delle deliberazioni & link
Interpellanza	15.3656	Pericolo per la centrale nucleare di Mühleberg a causa della manutenzione a distanza del sistema informatico. Discutibile sorveglianza da parte dell'IFSN	Martina Munz	18.06.2015	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153656
Postulato	15.3359	Per un esercito innovativo	Fathi Derder	20.03.2015	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153359
Postulato	15.3769	Rapporto sul servizio pubblico. Offerta Internet della SSR limitata a una audioteca ed una videoteca	Marco Romano	19.06.2015	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153769
Interpellanza	15.3723	Protezione della gioventù dai rischi dei media. Attuazione delle raccomandazioni degli esperti	Barbara Schmid-Federer	19.06.2015	CN	DFI	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153723
Interpellanza	15.3661	Violazione della concessione SSR. Proibire serie web illegali	Rutz Gregor A.	18.06.2015	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153661
Interpellanza	15.3657	Diritto all'oblio per gli utenti Internet	Martina Munz	18.06.2015	CN	DFGP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153657
Postulato	15.3618	Rapporto sul mandato di servizio pubblico della SSR. Analisi secondo il principio della sussidiarietà	Christian Wasserfallen	18.06.2015	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153618
Interpellanza	15.3615	Servizio pubblico nel settore mediatico	Edith Graf-Litscher	18.06.2015	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153615
Postulato	15.3407	Tutela dei diritti della personalità	Yvonne Feri	05.05.2015	CN	DFGP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153407
Mozione	15.3358	Accelerare l'attuazione di un programma d'investimento nella società digitale	Fathi Derder	20.03.2015	CN	DEFR	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153358
Interpellanza	15.3352	Come sono tassati i grandi gruppi di Internet in Svizzera?	Margret Kiener Nellen	20.03.2015	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153352
Postulato	15.3307	Rapporto sulla società svizzera dell'Internet nel 2030	Edith Graf-Litscher	20.03.2015	CN	DEFR	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153307
Interpel	15.3291	Esportazione di tecnologie di	Pierre-Alain	19.03.2015	CN	DEFR	http://www.parlament.ch/d/suche/seiten/geschaefte.asp

lanza		sorveglianza e di intercettazione. Che cosa ne è dei diritti umani?	Fridez				x?gesch_id=20153291
Interrogazione	15.1027	Quali azioni preventive intende condurre il Consiglio federale per evitare il radicarsi di estremismi violenti in Svizzera??	Christian van Singer	20.03.2015	CN	DFGP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20151027
Postulato	15.3759	Rete di dati sicura e ulteriori progetti IT della protezione della popolazione. Stato attuale, prospettive, fabbisogno di risorse	Ida Glanzmann-Hunkeler	19.06.2015	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153759
Interpellanza	15.3692	L'informatica nell'amministrazione federale. Un pozzo senza fondo?	Sylvia Flückiger-Bäni	18.06.2015	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153692
Interpellanza	15.3137	Esternalizzazione del trattamento di dati fiscali	Philipp Hadorn	16.03.2015	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153137
Interpellanza	15.3448	Come favorire l'introduzione di veicoli a guida autonoma?	Fathi Derder	06.05.2015	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153448
Interpellanza	15.3375	Sottrazione di codici SIM da parte della NSA e del GCHQ presso la società Gemalto	Luc Recordon	20.03.2015	CS	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153375

7.2 Altri temi

7.2.1 Programma nazionale di ricerca «Big Data»

Alla fine di giugno 2015 il Consiglio federale ha lanciato il nuovo Programma nazionale di ricerca (PNR) *Big Data*. Il budget stanziato per il PNR Big Data è di 25 milioni di franchi. Big Data prevede la creazione delle basi per un impiego efficace e appropriato del volume di dati in continua crescita in tutti i settori della società. La durata della ricerca è di cinque anni. I progetti di ricerca promossi hanno lo scopo di fornire basi scientifiche per soluzioni innovative nel campo del *computing* (analisi dei dati, algoritmi, crittografia, servizi di gestione dei dati, sicurezza e controlli d'accesso) con cui proteggere in modo efficace e sicuro grandi volumi di dati. A partire da queste basi si tratterà di analizzare con occhio critico ambiti di applicazione sociali (sanità, infrastrutture pubbliche) ed economici in cui grandi volumi di dati costituiscono già oggi e costituiranno ancor più in futuro una realtà, in particolare sotto il profilo della sicurezza dei dati e dei sistemi nonché in funzione di aspetti regolamentari (protezione dei dati, tutela della sfera privata).

Il gruppo di direzione del progetto del Fondo Nazionale Big Data è stato istituito nell'estate del 2015. I bandi per i singoli progetti e le condizioni di partecipazione per i gruppi di ricerca dovrebbero essere pubblicati nel corso dell'autunno del 2015. Bozze di progetto scientifiche dovranno essere quindi presentate entro tre mesi e una selezione definitiva dei progetti di ricerca avrà luogo presumibilmente nel corso del 2016.

7.2.2 Riorganizzazione dell'assegnazione dei domini

L'Ordinanza sui domini Internet (ODIn) entrata in vigore il 1° gennaio 2015 comporta una vasta riorganizzazione dell'assegnazione dei domini in Svizzera. Finora SWITCH svolgeva sia la funzione di gestore del registro (amministrazione della banca dati dei nomi dei domini, il cosiddetto *registry*) che di centro di registrazione (commercializzazione dei nomi di dominio). Con l'entrata in vigore della nuova ODIn, questa duplicità di ruoli non è più possibile. L'ODIn prevede infatti che il ruolo di Network Information Center (NIC), ossia di organizzazione che amministra centralmente le risorse per la gestione del Domain Name System (DNS) di un Paese, spetti all'UFCOM o a un terzo incaricato dall'UFCOM (art. 8 ODIn). Per poter offrire *Top Level Domain* (ccTLD o gTLD) sul mercato in Svizzera occorre stipulare un contratto di centro di registrazione con l'*ICANN* e il gestore del registro. In tutto il mondo sono ormai autorizzati al TLD 79 centri di registrazione, tra cui 46 aziende svizzere. Il trasferimento dei nomi di dominio .ch da SWITCH ai centri di registrazione è in corso ormai da diverso tempo. Secondo l'ODIn, la competenza per il gTLD .swiss spetta unicamente alla Confederazione (UFCOM); lo scopo è di garantire i vantaggi in particolare per la Svizzera a lungo termine.

Per assicurare un processo di migrazione ordinato e trasparente e preparare l'assegnazione del centro di registrazione, l'UFCOM ha prorogato il suo rapporto di delega con SWITCH fino a metà del 2017 nell'ottica di una soluzione transitoria e secondo quanto stabilito dall'art. 62 ODIn. Il bando per la funzione di gestore del registro è attualmente ancora aperto.

8 Prodotti MELANI pubblicati

Oltre ai rapporti semestrali MELANI mette a disposizione del pubblico un certo numero di prodotti di vario tipo. I seguenti paragrafi offrono una sintesi dei blog, delle newsletter, delle liste di controllo, delle guide e dei promemoria realizzati nel periodo in rassegna.

8.1 Blog GovCERT.ch

8.1.1 Joining the DNSSEC Day in Germany (in inglese)

30.06.2015 - DNSSEC stands for Domain Name System Security Extensions and has been introduced in 1999. The goal of DNSSEC is to implement authenticity and integrity in the DNS by taking advantage of digitally signing DNS records using public-key cryptography. DNSSEC helps you to prevent man-in-the-middle attacks on the DNS layer and DNS cache poisoning. Besides that, DNSSEC also provides a secure ground that allows you making usage of further security mechanisms that rely on DNSSEC, such as DNS-based Authentication of Named Entities (DANE).

➔ http://www.govcert.admin.ch/blog/9/joining-the-dnssec-day-in-germany

8.1.2 Outdate WordPress: Thousands of websites in Switzerland are vulnerable (in inglese)

08.06.2015 - The internet has grown very fast in the past 15 years. Thousands of new websites are going online every day. According to Netcraft, there are currently more than 850'000'000 active websites in the internet (May 2015). One of the reasons why the number of websites has grown that much is the use of content management systems (CMS), for example WordPress, Typo3, Joomla and Durpal. By using a CMS, you can easily publish

content in the internet without needing IT knowledge. While CMS are something great, they are also a valuable target for hackers.

➔ http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable

8.1.3 Increase in DDoS extortion (DD4BC) (in inglese)

08.05.2015 - In the past days MELANI / GovCERT.ch has received several requests regarding a Distributed Denial of Service (DDoS) extortion campaign related to 'DD4BC'. The DD4BC Team (that is how the attackers call themselves) started its DDoS extortion campaigns in 2014. Since earlier this week, the DD4BC Team expanded their operation to Switzerland. MELANI / GovCERT.ch is aware of several high profile targets in Switzerland that have recently received a blackmail from DD4BC and have consequently suffered from DDoS attacks, obviously conducted by DD4BC.

➔ http://www.govcert.admin.ch/blog/6/increase-in-ddos-extortion-dd4bc

8.1.4 e-Banking Trojan Retefe still spreading in Switzerland (in inglese)

01.05.2015 - In July 2014, Trend Micro published a report about a threat called Retefe, an ebanking Trojan that is targeting financial institutions in Switzerland, Austria, Sweden and Japan. In fact, Retefe is already around since November 2013. Back then, MELANI already took appropriate action together with the affected financial institutions and ISPs in Switzerland to mitigate the threat. However, Retefe is still being distributed in recent spam campaigns, targeting Swiss Internet users.

➔ http://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

8.1.5 Critical vulnerability in Magento: Many Swiss websites are still vulnerable (in inglese)

30.04.2015 - In February 2015, Magento (a popular eCommerce software for webshops) released a security patch addressing a critical vulnerability in its product. The vulnerability allows an attacker to send a special prepared HTTP request to any website running a vulnerable version of Magento in order to execute malicious code on the remote webserver (a so called Remote Code Execution RCE vulnerability). More than two months later, MELANI / GovCERT.ch still sees a fairly big amount of websites in Switzerland running an old, vulnerable version of Magento, exposing themselves and its visitors to cyber-attacks from the internet. Hackers can (ab)use the vulnerability to e.g. place malicious code on the victims website to infect its visitors with malware (Drive-By exploits).

➔ http://www.govcert.admin.ch/blog/4/critical-vulnerability-in-magento-many-swiss-websites-are-still-vulnerable

8.2 Newsletter di MELANI

Nel primo semestre del 2015 MELANI ha pubblicato le seguenti newsletter:

8.2.1 Portale di segnalazione contro il phishing

29.07.2015 - Nel corso degli ultimi anni è notevolmente aumentato il numero di richieste relative al phishing che sono state elaborate dalla Centrale d'annuncio e d'analisi per la

sicurezza dell'informazione MELANI. Nella maggioranza dei casi sono state segnalate e-mail e pagine web create a scopo di phishing che prendono di mira clienti di istituti finanziari in Svizzera, ma anche piattaforme Internet di fama internazionale (come ad es. social network, servizi e-mail o fornitori di servizi di pagamento online). Per poter elaborare in maniera più efficiente le numerose segnalazioni di phishing in entrata, la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha attivato un sito Internet sul quale è possibile segnalare pagine sospette di phishing.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/meldeportal_gegen_phishing.html

8.2.2 Attacchi DDoS e estorsione : una combinazione molto attuale

20.05.2015 - Le numerose segnalazioni, giunte a MELANI in queste ultime settimane, testimoniano l'incremento di attacchi DDoS, attuati al fine di estorcere del denaro alle proprie vittime. MELANI consiglia di non cedere al ricatto e pubblica un documento contenente differenti misure di protezione contro gli attacchi DDoS.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/ddos_angriffe_und_erpressung.html

8.2.3 Diffusione a macchia d'olio del trojan bancario «Dyre»

07.05.2015 - Nel febbraio 2015 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI aveva già richiamato l'attenzione sul trojan bancario Dyre, che insidiava le PMI svizzere. Nelle scorse settimane, MELANI, ha ricevuto giornalmente diverse centinaia di segnalazioni di nuove infezioni in Svizzera. Nel frattempo, ad essere colpite non sono più soltanto le PMI, infatti, sempre più utenti privati sono entrati nel mirino dei pirati informatici.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/information_dyre_2.html

8.2.4 Decimo anniversario di MELANI: il 20° rapporto semestrale fornisce una retrospettiva e illustra le minacce attuali nel mondo cibernetico

30.04.2015 - La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI celebra il suo decimo anniversario. Per questo motivo il 20° rapporto semestrale non si focalizza solo sugli eventi più importanti che si sono verificati nella seconda metà del 2014, anno caratterizzato soprattutto da estorsioni e attacchi a sistemi mal protetti. Il rapporto pubblicato in data odierna affronta anche la tematica dell'evoluzione della criminalità su Internet nell'ultimo decennio.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/20_melani_halbjahresbericht.html

8.2.5 Clienti di PMI svizzere nel mirino degli attacchi di phishing

31.03.2015 - Gli attacchi di phishing, tramite i quali i truffatori cercano di accedere a dati sensibili (password, dati di carte di credito ecc.) sono sempre d'attualità. Nella maggior parte dei casi, vengono creati siti web che imitano quelli di imprese conosciute (ad es. banche o emittenti di carte di credito). MELANI interviene ogni giorno per eliminare questi contenuti fraudolenti dal web e proteggere gli utenti. Già da qualche anno, i truffatori non attaccano più soltanto grandi marche note, ma sferrano attacchi di phishing mirati contro imprese più piccole. Sembra che questa tendenza si stia estendendo e diversi casi portati recentemente all'attenzione di MELANI provano persino una maggior sofisticazione degli attacchi. Essi

concernono diversi tipi di PMI con siti web che registrano gli indirizzi e-mail di clienti, ad esempio per l'invio di newsletter.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/clienti-di-pmi-svizzere-nel-mirino-degli-attacchi-di-phishing.html

8.2.6 Le PMI svizzere nel mirino di un trojan bancario

02.02.2015 - Nei giorni scorsi, la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha ricevuto un numero crescente di segnalazioni da parte di PMI svizzere che comunicavano di aver ricevuto per posta elettronica messaggi spam sospetti. I messaggi segnalati provengono in tutta evidenza da sedicenti soci d'affari e tentano di infettare i destinatari delle mail con un trojan bancario. In un caso di cronaca di poco tempo fa, riguardante un'azienda del Canton Friburgo, i pirati informatici sono riusciti con lo stesso trojan a sottrarre un importo a sette cifre.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/le-pmi-svizzere-nel-mirino-di-un-trojan-bancario.html

8.3 Liste di controllo e guide

Nel primo semestre del 2015 MELANI ha pubblicato le seguenti liste di controllo e guide:

8.3.1 Misure contro attacchi DDoS

25.06.2015 - L'acronimo DDoS («Distributed Denial of Service» = negazione del servizio) indica un attacco a sistemi informatici con lo scopo dichiarato di limitarne la disponibilità. Le conseguenze economiche per la vittima possono essere notevoli.
I motivi alla base degli attacchi DDoS sono per lo più legati all'attivismo politico, a tentativi di estorsione o all'intenzione di danneggiare un concorrente. Attualmente MELANI constata un aumento degli attacchi DDoS a fini di estorsione, nei quali viene richiesto un riscatto in criptovalute come bitcoin o litecoin.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/massnahmen-gegen-ddos-attacken.html

8.3.2 Promemoria sulla sicurezza informatica per le PMI

30.01.2015 - Il presente promemoria è rivolto alle PMI svizzere e ha lo scopo di aiutarle a migliorare la sicurezza informatica della loro rete aziendale.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/promemoria-sulla-sicurezza-informatica-per-le-pmi.html

9 Glossario

Termine	Definizione
0-day Exploit	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
Adware	L'adware, una combinazione delle parole advertisement e software, viene sovente utilizzato a scopi pubblicitari, nel senso che le abitudini di navigazione dell'utente sono registrate e sfruttate per offrire prodotti corrispondenti (ad es. tramite link).
Big Data	Quantità di dati troppo grandi o troppo complesse per poter essere analizzate con metodi manuali e classici.
Bitcoin	Sistema di pagamento decentrato disponibile a livello mondiale nonché il nome di un'unità di moneta digitale.
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).
Certificate	Un certificato digitale è in un certo qual senso l'equivalente di una carta d'identità a livello di cyberspazio ed è destinato all'assegnazione di una determinata chiave pubblica a una persona o a un'organizzazione. Tale assegnazione è autenticata dal servizio di certificazione che provvede a tale scopo apponendovi la propria firma digitale.
Cifratura RSA	Abbreviazione di cifratura Rivest-Shamir-Adleman. Procedura di cifratura con chiavi pubbliche, introdotta nel 1978. La cifratura RSA è una procedura asimmetrica.
Cipher	Procedimento di crittografia che consente di convertire un testo normale in un testo segreto o, al contrario, di riconvertire un testo segreto in un testo normale.
Command and 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 Systemen (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).
Crittografia	Termine che definisce originariamente la scienza della codifica di informazioni.
Cross-Site-Scripting (XSS)	Cross-Site-Scripting (XSS) designa una falla di sicurezza che di norma può essere riscontata in applicazioni web. Cross-Site-Scripting permette agli hacker ("cattivi") di inserire codici sorgente in una pagina web, che poi verrà visualizzata da un visitatore.
Defacement	Deturpamento di pagine Web.
Diffie-Hellman Key Exchange	Strumento che permette a due partner di una comunicazione di generare una chiave segreta nota unicamente a loro.
Distributed Denial of Service (DDoS)	Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi, il quale ha lo scopo di rendere un determinato servizio irraggiungibile per l'utente o perlomeno di ostacolarne notevolmente la raggiungibilità.
Elettronica di bordo	Elettronica situata in un oggetto mobile e che contribuisce a supportare la guida di questo oggetto.
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.
FTP	File Transfer Protocol FTP è un protocollo di rete per la trasmissione di dati tramite reti TCP/IP. FTP può ad esempio essere utilizzato per caricare pagine Web su un server Web.
Funzione di fallback	Funzione (livello di funzionamento ridotto) che rappresenta un secondo sistema che in caso di interruzione nel funzionamento del primo sistema impedisce un'interruzione totale nel funzionamento.
Geolocation	Localizzazione della posizione
Global Positioning System	Il Global Positioning System (GPS), ufficialmente NAVSTAR GPS, è un sistema globale di navigazione

(GPS)	satellitare per la determinazione della posizione e la misura del tempo.
Hacktivismo	Hacktivismo è il termine scelto per indicare l'atto di infiltrarsi in un sistema informatico mossi da obiettivi politici o sociali.
Honeypot	In ambito di sicurezza dei computer si designa come honeypot (italiano: vaso di miele) un programma informatico o un server che simula i servizi di rete di un computer, un'intera re-te di computer oppure il comportamento di un utente. Gli honeypot sono utilizzati per ottenere informazioni sui modelli di attacco e sui comportamenti degli aggressori.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) L'ICANN e un'organizzazione senza scopo di lucro con sede nella cittadina costiera californiana di Marina del Rey. ICANN decide in merito ai principi di gestione dei Top Level Domain. Così facendo ICANN coordina gli aspetti tecnici di Internet, senza peraltro stabilire norme di diritto vincolanti. ICANN sottostà al Dipartimento statunitense del commercio (Department of Commerce) e pertanto al Governo americano.
Industria 4.0	Industria 4.0 o la quarta rivoluzione industriale è una designazione che indica comprensivamente la automazione attuale, il collegamento integrale in rete e lo scambio di dati. Industria 4.0 appoggia il concetto e la messa in pratica di "Smart Factories".
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.
Internet of Things (IoT)	Il termine «Internet delle cose» (in inglese «Internet of Things», IoT) descrive il fatto che il computer viene progressivamente sostituito da oggetti intelligenti.
IP-address	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
Javascript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di

	Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo Web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i browser.
Malware	Termine composto dalle parole inglesi «Malicious» e "Software". Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Troia.
Password unica	Una password unica è una parola d'ordine di autentificazione o di autorizzazione. Essa è valida per un solo processo e non può essere utilizzata una seconda volta.
Patchday	Giorno in cui la società Microsoft pubblica gli aggiornamenti del proprio software.
Patch-Management	Organizzazione della distribuzione degli aggiornamenti di software.
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 und Firmenlogos è falsificato.
Plug-In, Plugin	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.
QR Code (o codice QR)	Metodo per annotare informazioni in modo che possano essere reperite e scansionate meccanicamente in modo particolarmente rapido.
Radio Data System (RDS)	Sistema che consente di trasmettere informazioni aggiuntive alla radio.
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.
SIM	La carta SIM (in inglese: Subscriber Identity Module) è una carte chip inserita nel telefono mobile che serve all'identificazione dell'utente.
Sistemi industriali di controllo (ICS)	I sistemi di controllo e di comando constano di una o più apparecchiature che guidano, regolano e/o sorvegliano il comportamento di altre apparecchiature o sistemi. Nella produzione industriale il concetto di «sistemi industriali di controllo» (inglese: Industrial Control Systems, ICS) è corrente.
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Smartphone	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.
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.
SSL/TLS Tunnel	Il tunnel o il, rispettivamente tunneling, designa la conversione e la trasmissione all'interno di una rete di un protocollo di comunicazione, integrato ai fini del trasporto in un altro protocollo di comunicazione. SSL e TLS sono protocolli di comunicazione cifrata in Internet.
Top Level Domains	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separate da un punto. La designazione Level-Domain si riferisce all'ultimo nome di questa successione e costituisce il livello più elevato della risoluzione del no-me. Se ad esempio il

	nome completo di dominio di un computer, rispettivamente di un sito Web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome.
Traffic Distribution System (TDS)	Sistemi che dirigono il traffico Internet sul sito di destinazione vero e proprio quando viene selezionata una pubblicità online. Un sistema di questo tipo viene spesso utilizzato per diffondere un malware.
Web Application Firewall	Procedimento finalizzato a proteggere applicazioni Web dagli attacchi operati tramite l'Hypertext Transfer Protocol.