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
https://www.melani.admin.ch/

SICUREZZA DELLE INFORMAZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2017/II (luglio – dicembre)

26 APRILE 2018

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

1 Indice

2 Editoriale

Werner Meier
Delegato per l'approvvigionamento economico

Care lettrici, cari lettori,

la digitalizzazione offre enormi opportunità al nostro Paese, ma al contempo riserva imponenti sfide. La gestione e l'ottimizzazione dei processi in ambito economico, ricorrendo alle tecnologie dell'informazione e della telecomunicazione (TIC), hanno possibilità di successo duraturo soltanto se le TIC sono sempre disponibili, affidabili e capaci di resistere ai disturbi e agli attacchi. In sostanza, la digitalizzazione è impensabile senza la sicurezza delle TIC.

Il Consiglio federale attribuisce una notevole importanza alla digitalizzazione, come dimostra la strategia «Svizzera digitale» nell'ambito della quale ha annoverato la sicurezza tra i quattro obiettivi prioritari. Anche il Comitato consultivo costituito nell'estate del 2017 dal DEFR e dal DATEC per attuare la strategia ha posto la «Cybersicurezza» tra le tematiche su cui focalizzarsi.

Conformemente al suo mandato costituzionale, l'Approvvigionamento economico del Paese (AEP) deve assicurare l'approvvigionamento della Svizzera in beni e servizi vitali nel caso di crisi. Per l'AEP le TIC non sono soltanto vitali di per sé, ma rivestono un'importanza fondamentale, ad esempio come risorsa per il funzionamento dell'approvvigionamento del nostro Paese in energia elettrica o servizi logistici. Con la riveduta legge sull'approvvigionamento del Paese, l'AEP dispone di una moderna base giuridica per raggiungere il suo obiettivo e la cooperazione dei quadri del settore privato gli assicura le necessarie competenze specifiche.

Negli ultimi mesi l'AEP ha elaborato uno Standard minimo generale TIC, che nel quadro della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) contribuisce ad aumentare la resilienza. Sulla base del «Framework Core» del National Institute for Standards and Technology (NIST) statunitense, vengono descritte 106 misure che servono ai gestori di infrastrutture critiche di approvvigionamento per proteggere le loro risorse TIC. Lo Standard minimo generale TIC sarà presentato prossimamente al pubblico e potrà essere utilizzato liberamente. L'Associazione delle aziende elettriche svizzere (AES) se ne serve già per crearne l'equivalente nel settore dell'energia elettrica. Lo standard, al quale l'AEP ha prestato un notevole contributo, assurgerà a strumento di autodisciplina per questo ramo economico. Attualmente sono in fase di elaborazione standard minimi TIC anche per le acque di scarico nonché per l'approvvigionamento idrico, di gas e olio minerale.

L'AEP, dunque, non solo contribuisce alla digitalizzazione della Svizzera, bensì promuove anche la resilienza delle infrastrutture critiche di approvvigionamento in caso di interruzioni, disturbi e attacchi. La conferma della sua inconfutabile necessità giungerà dal presente rapporto semestrale della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI. Vi auguro una piacevole lettura.

Werner Meier
Delegato per l'approvvigionamento economico

3 Tema principale: le fughe di dati

Nel mondo digitale vengono generati e memorizzati ogni giorno milioni di dati contenenti informazioni personali, che sia esibendo la carta fedeltà alla cassa del supermercato, pagando con la carta di debito o di credito, negli acquisti online, controllando le mail o durante una visita medica. Questo elenco potrebbe proseguire all'infinito. Anche navigando in Internet ogni individuo lascia quotidianamente molte tracce.

Se finiscono nelle mani sbagliate, questi dati possono servire a commettere abusi. Purtroppo la fuga di dati è un fenomeno sempre più frequente e si è puntualmente verificato anche nel secondo semestre dello scorso anno: nel mese di ottobre del 2017 Yahoo!, società che offre servizi su Internet, ha reso noto che dal 2013 la fuga di oltre tre miliardi di dati ha apparentemente interessato tutti gli utenti e non solo una parte di essi, come inizialmente ipotizzato[1]. Questa rappresenta la più grande fuga di dati della storia. Un'indicazione impressionante giunge anche dal portale «have I been pwned»[2], dove ognuno può controllare se il suo indirizzo di posta elettronica è mai stato interessato da una fuga di dati. Il totale di tutte le password rubate raggiunge attualmente l'incredibile cifra di quasi cinque miliardi.

Nei mesi scorsi neppure la Svizzera è rimasta immune alle fughe di dati. Swisscom, ad esempio, ha reso noto che nel mese di ottobre del 2017 oltre 800 000 dati di clienti hanno subito un accesso abusivo. Nel novembre 2017 Galaxus/Digitec aveva il sospetto che dati dei clienti fossero giunti in possesso di truffatori e anche l'assicuratore malattie Groupe Mutuel ha pubblicamente ammesso una fuga di dati nel mese di dicembre del 2017. Sempre in dicembre sono stati segnalati a MELANI 70 000 dati di accesso trafugati, che successivamente hanno potuto essere attribuiti alla società svizzera «DVD-Shop».

Nel frattempo sui portali specializzati emergono sistematicamente dati rubati tra cui password, dati delle carte di credito o altri dati personali. In numerosi casi, tuttavia, è difficile verificarne la provenienza, il tempo da cui sono in circolazione e la qualità. Per molti di questi dati rubati è presumibile che il furto non sia stato neppure notato.

3.1 Definizione

Le fuoriuscite di dati costituiscono incidenti legati alla sicurezza: persone non autorizzate si impossessano di dati personali, segreti d'ufficio o altri dati, non riservati a loro. La nozione di «fuoriuscita di dati» è molto ampia e comprende oltre al furto di dati e allo spionaggio anche guasti, a causa dei quali die dati vengono resi accessibili involontariamente. La tipologia di dati colpiti non si limita dunque alle password e ai dati delle carte di credito, ma si estende anche a quelli che concernono la sfera sanitaria e finanziaria per esempio.

3.2 Estorsione, raccolta di dati e intenti politici

Un metodo cui i criminali ricorrono spesso per guadagnare denaro con i dati trafugati è il ricatto della società dalla quale i dati sono stati prelevati. In Svizzera uno dei primi casi del genere

---

1 http://www.sueddeutsche.de/digital/yahoo-hackerangriff-bei-yahoo-traf-alle-drei-milliarden-konten-1.3693671 (stato: 31.01.2018).

2 https://haveibeenpwned.com/ (stato: 31.01.2018).

risale al 2014, quando un gruppo che si faceva chiamare «Rex Mundi» ha ricattato una società della Svizzera francese minacciandola di pubblicare i suoi dati. L'estorsione può colpire non solo la società ma anche i suoi clienti.

Un altro modo di utilizzare i dati trafugati consiste nell'avvalersene per sferrare attacchi mirati. Gli attori che si muovono nel mercato nero si sono specializzati nel raccogliere il maggior numero possibile di indicazioni su una vittima, utilizzando non solo fonti accessibili a chiunque, ma anche informazioni che provengono da furti di dati. Gli hacker che riescono, con l'aiuto dei diversi dati, a crearsi un'immagine precisa della vittima riusciranno a compiere attacchi molto mirati. Nel periodo in rassegna, ad esempio, è stata rilevata la diffusione di mail contenenti un software nocivo nelle quali, oltre all'appellativo con nome e cognome del destinatario, figurava anche il suo numero di telefono e/o il suo indirizzo postale. Tutti i dati erano stati trafugati e venivano utilizzati per convincere la vittima dell'autenticità della mail.

I furti di dati dettati da intenti politici meritano di essere trattati separatamente. Il caso più famoso è la pubblicazione dei cosiddetti «file di Snowden». Emulando Snowden, molti altri protagonisti hanno cercato da allora di scuotere l'opinione pubblica o cambiare la società. Basti pensare alla pubblicazione dei «Panama-Paper» e dei «Paradise-Paper», con i quali sono state portate alla luce le pratiche attuate da diversi politici e personaggi di spicco sui mercati finanziari di tutto il mondo.

3.3 Ripercussioni

Ma quali sono i reali effetti delle violazioni dei dati sulle vittime, quali danni causano loro? La risposta a questa domanda non è univoca, poiché ognuno attribuisce un valore diverso ai suoi dati. Per alcuni privati è indifferente se e quali dati vengono rilevati e che cosa se ne fa, mentre altri cercano di limitare il più possibile il volume di dati sulla propria persona. Questi ultimi attribuiscono dunque un peso molto maggiore al danno personale subito.

Anche le modalità con cui i dati sono trafugati hanno una loro importanza e possono essere sistematicamente suddivise in due gruppi: i dati che possono essere reimpostati senza problemi e quelli che rimangono validi durante il corso di una vita intera. Le password e i dati delle carte di credito sono facilmente sostituibili e causano alle vittime solo danni limitati nel tempo. I dati riguardanti il proprio stato di salute, gli orientamenti personali o la situazione finanziaria non possono essere semplicemente «resettati» e provocano danni a più lungo termine. Gli hacker sono in grado di mettere in difficoltà una vittima anche a distanza di anni dal furto di dati. Come aggravante si aggiunge il fatto che in molti casi la vittima non è consapevole dei dati trafugati, di conseguenza non può difendersi né tutelarsi.

Nel caso delle imprese, la fuoriuscita involontaria di dati non provoca solo lavoro e spese, ma anche un danno alla reputazione. In tal caso la comunicazione con i clienti assume una rilevanza fondamentale ed è per questo che per un'impresa è straordinariamente importante prepararsi correttamente all'eventualità di una fuga di dati. Ciò implica pianificare le emergenze, preparare la comunicazione e definire chiare responsabilità. In caso di fughe di dati, MELANI raccomanda generalmente di adottare una linea di massima trasparenza nei confronti dei clienti. È importante informarli al più presto per limitare le conseguenze dannose. Il segreto sta nell'adottare uno stile di comunicazione sobrio e pacato.

3.4 Informazione delle persone interessate

Quando un'impresa subisce un furto di dati, sorge ben presto la questione dell'informazione ai clienti. L'impresa coinvolta è nella posizione migliore per occuparsi di questa comunicazione. È infatti la sola ad avere la visione d'insieme sui clienti interessati e sul tipo e la quantità di dati rubati, inoltre è in grado di raccomandare misure appropriate, tra cui la reimpostazione delle password. In una simile eventualità occorre impedire alle persone non autorizzate di accedere a informazioni sulle vittime. L'assicuratore malattie «Groupe Mutuel», ad esempio, ha chiesto una copia di un documento d'identità a coloro che domandavano se erano rimasti coinvolti.

Informare le persone interessate costituisce una sfida ancora più ardua se l'origine dei dati rubati è sconosciuta. Portali tra cui «Pastebin» pubblicano ripetutamente combinazioni di nomi di utenti e password la cui provenienza non può essere stabilita con certezza. In passato MELANI ha già ricevuto più volte elenchi di dati rubati. In questi casi ha messo a disposizione un'applicazione online con la quale gli utenti di Internet potevano scoprire se fossero stati colpiti. Spesso l'origine dei dati può essere ricostruita a posteriori in base alle reazioni della collettività. Secondo il parere di MELANI una volta attribuita l'origine, è compito dell'azienda informare i clienti e l'opinione pubblica della fuga di dati.

3.5 Protezione dei dati

La protezione dei dati personali è disciplinata nella legge federale sulla protezione dei dati (DSG) che ha lo scopo di proteggere la personalità e i diritti fondamentali delle persone fisiche e giuridiche i cui dati sono oggetto di trattamento. La legge distingue tra dati personali e dati personali degni di particolare protezione. La seconda categoria comprende le opinioni e le attività religiose, filosofiche, politiche o sindacali, la salute, la sfera intima o l'appartenenza a una razza, le misure d'assistenza sociale e i procedimenti o le sanzioni amministrativi e penali. Il loro trattamento è subordinato al consenso esplicito della persona interessata. La legge sulla protezione dei dati tiene adeguatamente conto anche dell'aspetto della sicurezza e stabilisce che i dati personali devono essere protetti contro ogni trattamento non autorizzato mediante provvedimenti tecnici ed organizzativi appropriati.

La revisione totale della legge sulla protezione dei dati è in corso. Si presume che essa recepirà diverse novità del regolamento generale dell'Unione europea sulla protezione dei dati la cui applicazione è obbligatoria per tutti gli Stati membri dell'UE dal 25 maggio 2018 dopo un periodo transitorio di due anni. Di conseguenza riguarda pure tutte le imprese elvetiche con o senza una succursale nell'Unione europea che offrono beni o servizi a persone che si trovano nell'UE (questa condizione dovrebbe essere soddisfatta già con le offerte su un sito web o un e-shop), o che trattano dati personali appartenenti a cittadini di Paesi membri dell'UE, oppure che analizzano il comportamento di persone che si trovano nell'UE. In sintesi, le principali modifiche apportate con le nuove disposizioni sono: diritto all'oblio; trattamento dei dati solo previo consenso esplicito dell'interessato; diritto alla portabilità dei dati (a un altro fornitore di servizi); diritto dell'interessato di essere informato in caso di violazione della protezione dei propri dati e, infine, un intervento più duro in caso di violazioni del regolamento. Quest'ultimo significa che a un'azienda possono essere inflitte sanzioni amministrative pecuniarie fino al 4 per cento del suo fatturato totale mondiale annuo dell'esercizio precedente.

In particolare l'ultima prescrizione modificherà profondamente la gestione dei casi di violazione dei dati e porrà un maggiore accento sull'aspetto della sicurezza delle banche dati e dell'elaborazione dei dati. D'altro canto motiverà ancora di più i cybercriminali a trarre profitto

dai dati trafugati. Un ricatto per una somma inferiore a quella della sanzione pecuniaria potrebbe indurre l'una o l'altra azienda ad accogliere l'offerta più vantaggiosa.

3.6 Cause e protezione

Le fughe di dati hanno molteplici cause che spaziano dal furto di dati da parte dei collaboratori alla manutenzione dimenticata o carente dei server fino alla scarsa protezione dei backup.[3]

3.6.1 In guardia contro i cimiteri di dati

L'essere umano tende a registrare da qualche parte tutti i dati raccolti, anche se da tempo hanno perso la loro utilità o validità. Ad esempio, nell'elenco telefonico di un cellulare figurano contatti che non sono più validi da tanto. Questi dati «dimenticati» contribuiscono a ingigantire inutilmente la portata di una violazione di dati. In particolare nella migrazione di un server occorre vigilare affinché i dati siano infine cancellati dai vecchi sistemi. È altresì opportuno attribuire una vita a ogni serie di dati per verificarne periodicamente la validità. Inoltre, dovrebbero essere consultati e memorizzati solo i dati realmente necessari. Da un lato questo requisito è sancito dalla legge sulla protezione dei dati (art. 4 cpv. 2 LPD, principio della proporzionalità), dall'altro un volume esiguo di dati memorizzati riduce notevolmente l'effetto di una fuga di dati.

3.6.2 Proteggere l'accesso / Ridurre il traffico

Sarebbe opportuno limitare il più possibile gli accessi dall'esterno che devono essere comunque particolarmente protetti e monitorati. Ogni azienda deve valutare con attenzione chi ha bisogno di accedere a quali dati e come questo accesso possa essere protetto. Ad esempio i punti di accesso non utilizzati dovrebbero venir chiusi. Il ricorso a un secondo fattore di autenticazione viene caldamente consigliato in caso di accessi dall'esterno. Per un impiego diffuso si sono affermate le procedure di autenticazione OTP («One Time Password»), tra cui «Google Authenticator», un'app ampiamente utilizzata da installare sullo smartphone. Anche il traffico in uscita dovrebbe essere limitato ai collegamenti necessari. Numerosi attacchi si basano sullo scaricamento di codice da internet da parte del computer sotto attacco. Ciò accade spesso automaticamente. Proibire traffico in uscita aumenta perciò in modo considerevole il grado di difficoltà per l'aggressore.

Generalmente e indipendentemente da ciò, che si tratti di un formulario di contatto senza importanza o di un'importante applicazione d'ufficio, i dati inseriti dall'utilizzatore dovrebbero venir inoltrati il più velocemente possibile a un Backend System che non sia raggiungibile direttamente da internet.

Tutti i software dei server e le applicazioni devono essere costantemente aggiornati. Se per una determinata falla la patch non esiste o non può essere installata, sono da adottare adeguati provvedimenti che riducano i rischi. È consigliabile ricorrere a un «Web Application Firewall», la versione specializzata di un firewall che controlla gli accessi alle risorse di un sistema, filtrando tutto il traffico. Esistono molteplici prodotti commerciali e open source che possono migliorare la protezione di un'applicazione accessibile via Internet. La maggior parte

[3] Le minacce più diffuse sono documentate in una classifica top 10 del progetto OWASP (Open Web Application Security Project). Questa classifica viene attualizzata regolarmente. https://www.owasp.org/

di questi prodotti propongono anche delle regole da osservare contro le vulnerabilità più diffuse (OWASP Top 10).

3.6.3 Scarsa sicurezza per i backup

I backup sono una sorta di assicurazione sulla vita di ogni impresa, tuttavia devono soddisfare gli stessi standard di sicurezza dei dati produttivi. Anche i dati archiviati su supporti esterni dovrebbero essere salvati cifrati.

3.6.4 Password non protette

Se tra i dati rubati figurano delle password, esse non dovrebbero essere facili da decriptare. Ciò presuppone l'utilizzo di una funzione «hash»[4] e di un cosiddetto «salt» (equivalente inglese di un «pizzico di sale»). Un «salt» serve per aggiungere alla password una stringa di caratteri random che solo il sistema conosce prima di sottoporla alla funzione «hash». È opportuno utilizzare «salt» più lunghi possibile, che vengono generati alla creazione di una password. È altrettanto importante utilizzare una funzione «hash» lenta, poiché il calcolo dell'«hash» della password diventa così molto complicato e viene eseguito lentamente. Agli utenti regolari non disturba molto se la procedura di login dura qualche millesimo di secondo in più, mentre per gli hacker, che devono effettuare il calcolo milioni di volte, il tempo necessario all'elaborazione dei dati aumenta drasticamente.

3.6.5 Furti compiuti da insider

Anche i dati sono trafugati da dipendenti ancora attivi o ex-collaboratori, che sono insoddisfatti dell'azienda e vogliono arrecarle danno o che intendono procurarsi un vantaggio personale. Tale fenomeno può essere contrastato creando un clima di serena e schietta collaborazione e consentendo di discutere apertamente i problemi. È altresì importante provvedere affinché i collaboratori possano accedere soltanto ai dati di cui hanno bisogno per svolgere il loro lavoro. Agli ex-collaboratori deve essere immediatamente impedito qualunque accesso, il che presuppone una chiara politica della disponibilità dei dati.

4 La situazione a livello nazionale

4.1 Spionaggio

4.1.1 Nuovo attacco ai sistemi interni della Confederazione

Nel mese di luglio del 2017 è stato scoperto il software di spionaggio «Turla» su alcuni server del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS). Il malware non è certo uno sconosciuto all'interno dell'amministrazione federale. Proprio il software di spionaggio «Turla» ha attaccato, nel dicembre del 2015, il gruppo tecnologico RUAG responsabile, tra l'altro, di salvaguardare l'equipaggiamento dell'esercito. In quell'occasione gli hacker sono riusciti a sottrarre oltre 20 gigabyte di dati. In questo caso il malware è stato scoperto già nella sua fase iniziale, quindi prima che riuscisse a rubare dati

[4] Hash è una funzione matematica che consente di ottenere una sequenza di caratteri di lunghezza fissa (valore hash) partendo da una sequenza di caratteri di qualunque lunghezza (in questo caso una password).

importanti oppure a colpire altri sistemi collegati alla rete. Ciò è avvenuto sebbene l'hacker abbia potenziato la sua infrastruttura e i suoi strumenti e aumentato il grado di complessità della procedura. I competenti uffici federali sono riusciti a svolgere le necessarie verifiche in tempo utile e ad adottare provvedimenti appropriati. L'ottima collaborazione tra gli uffici federali ha consentito di raccogliere informazioni sui metodi di attacco e sugli indicatori tecnici. Lo scambio di questi indicatori a livello nazionale e internazionale è un elemento centrale per scoprire attacchi in corso o futuri. Il Consiglio federale, i membri della Delegazione Sicurezza del Consiglio federale e le presidenze delle commissioni competenti sono stati prontamente informati, come solitamente avviene in tali circostanze. Inoltre, il DDPS ha sporto denuncia penale contro ignoti presso il Ministero pubblico della Confederazione per l'attacco informatico a danno dei suoi server[5].

4.2 Sistemi industriali di controllo

I giornali riportano sistematicamente notizie di sistemi industriali di controllo (Industrial control system ICS) accessibili da Internet, quindi a rischio, tra cui sistemi di controllo degli impianti industriali, pompe di centrali idroelettriche[6] o installazioni mediche[7]. Questi sistemi sono a rischio perché, ad esempio, è emersa una falla in una delle componenti utilizzate oppure perché esse non sono state configurate in modo sufficientemente sicuro.

Quando emergono questi casi, i gestori delle infrastrutture colpite sono spesso criticati poiché non eseguono gli aggiornamenti con la necessaria tempestività. Ma i ritardi o l'impossibilità di installare patch di sicurezza hanno anche i loro motivi, ad esempio l'aggiornamento di una componente può compromettere la certificazione dell'intero sistema. Sarebbe dunque molto più importante che l'ambiente di sistema e la rete alla quale sono collegati questi apparecchi fossero costruiti e gestiti in modo talmente solido che le vulnerabilità possono emergere senza compromettere le funzioni chiave[8]. Anche nella lista di controllo «Misure di protezione dei sistemi di controllo industriali (ICS)» elaborata da MELANI risulta che la gestione degli aggiornamenti rappresenta soltanto una di undici misure. Le altre dieci concorrono a contenere i rischi in modo diverso: ad esempio, una robusta architettura di rete garantisce che nell'area di rete contenente l'apparecchio vulnerabile si trovino idealmente soltanto sistemi preposti a comunicare con l'apparecchio vulnerabile. Le transizioni da un'area di rete all'altra dovrebbero essere ridotte allo stretto indispensabile e ben monitorate. Ai collaboratori devono essere sempre attribuiti soltanto i diritti assolutamente necessari allo svolgimento dei compiti stabiliti. La ricostruzione centralizzata degli eventi informatici consente inoltre di controllare che tutti i sistemi funzionino come previsto. Tuttavia, qualora fosse registrato un attacco a dispetto di tutti i provvedimenti adottati, giunge in aiuto il processo di «Security Incident Management». Se la reazione a un incidente di sicurezza è definita ed è stata esercitata con tutte le istanze coinvolte, il potenziale danno può essere ridotto al minimo.

---

5 https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-68135.html (stato: 31.01.2018).

6 http://www.spiegel.de/netzwelt/web/so-bedrohen-hacker-wasserversorgung-stromnetz-und-kliniken-a-1181325.html (stato: 31.01.2018).

7 https://nakedsecurity.sophos.com/2018/02/01/hospital-mri-and-ct-scanners-at-risk-of-cyberattack/ (stato: 31.01.2018).

8 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (stato: 31.01.2018).

Nella letteratura specialistica la compensazione tra un rischio inevitabile e una o più strategie di difesa è designata «difesa di profondità»[9]. Un esempio schematico di un'infrastruttura di rete ICS è riportato nella figura 1.

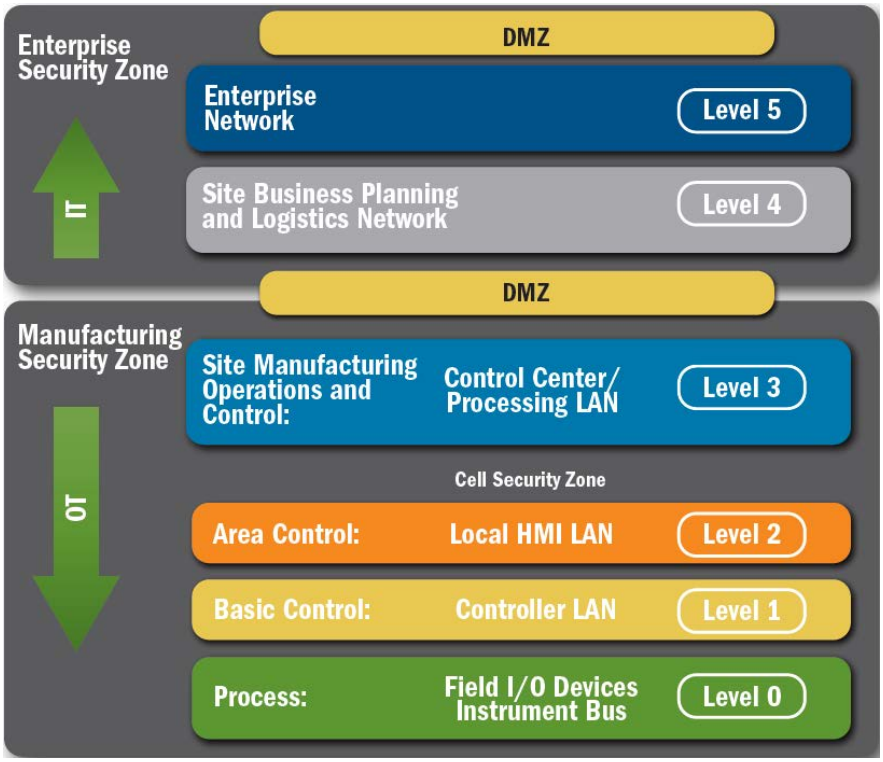

Figura 1: architettura di rete dell'US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[9]

Sebbene queste raccomandazioni siano tutte scontate e semplici da attuare se considerate isolatamente, spesso mancano le risorse disponibili per metterle in pratica in sistemi complessi. In molti casi anche la conclusione puntuale del progetto o la semplicità di gestione dei processi sono anteposte alla sicurezza. Al fine di sfruttare al meglio delle risorse limitate è indispensabile attuare una gestione dei rischi globale, nella quale i rischi residui sono individuati e assunti dalla direzione.

9 https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP (stato: 31.01.2018).

Raccomandazione

Se scoprite sistemi di gestione in Internet accessibili dall'esterno o protetti in modo inadeguato, trasmetteteci i dati necessari per darci modo di informare il gestore.

Formulario d'annuncio MELANI

https://www.melani.admin.ch/melani/it/home/meldeformular/formular.html

Lista di controllo delle misure di protezione dei sistemi industriali di controllo:

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

4.2.1 Hacker da batticuore

Un pacemaker è un piccolissimo computer alimentato a batteria, dotato del necessario sistema di rilevamento, dell'elettronica di valutazione e degli elementi di attuazione sotto forma di generatore di impulsi. In tal modo i battici cardiaci possono essere monitorati e, in caso di emergenza, stimolati elettricamente. Molti di questi piccoli salvavita hanno anche un trasmettitore a radiofrequenza che consente di analizzare i valori cardiaci e modificare la configurazione senza ulteriori interventi chirurgici.

Il 29 agosto 2017 l'ICS-CERT focalizzato sui sistemi di controllo del Dipartimento della sicurezza interna statunitense (Department of Homeland Security, DHS) ha segnalato[10] vulnerabilità su diversi modelli di pacemaker della società Abbott Laboratories. Le falle scoperte dalla MedSec Holdings Ltd consentono la manipolazione dei dati che sono scambiati con l'apparecchio impiantato tramite il trasmettitore. L'apparecchio trasmittente dell'hacker dovrebbe essere posto direttamente sul corpo del paziente, così come avviene per una visita di routine dal medico, ma potrebbe eseguire tutti i processi di lettura e di scrittura. Il motivo sta nel fatto che l'autenticazione dell'apparecchio di programmazione si differenzia dallo standard previsto. Secondo una pubblicazione[11] dell'ente governativo statunitense che si occupa della regolamentazione dei prodotti alimentari e farmaceutici (Food and Drug Administration, FDA) e disciplina anche i dispositivi medici, un attacco del genere, in grado di sfruttare le falle esistenti, non si è ancora verificato.

Nel frattempo l'azienda produttrice ha pubblicato aggiornamenti[12] per i dispositivi in questione che possono essere installati presso il medico curante. In Svizzera i pazienti che hanno dovuto

10 https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01 (stato: 31.01.2018).

11 https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (stato: 31.01.2018).

12 https://www.sjm.com/~/media/galaxy/patients/heart-vascular/arrhythmias/resources-support/cybersecurity/pacemaker-firmware-update-patient-guide-aug2017-us.pdf (stato: 31.01.2018).

sottoporsi a questa procedura sono stati circa 5000[13] e rappresentano quasi un settimo di tutti i portatori di pacemaker in Svizzera.

4.3 Attacchi (DDoS, Defacement, Drive-By)

In Svizzera i cittadini, le organizzazioni e le aziende continuano a essere il bersaglio di diversi tipi di attacchi.

4.3.1 Estorsione in ambito DDoS a nome di gruppi celebri

L'estorsione è attualmente uno dei metodi privilegiati dai cyber-criminali che mirano a realizzare un rapido guadagno finanziario. Oltre agli attacchi dei cosiddetti «ransomware», malware che cifrano file a scopo di estorsione, e alla minaccia di pubblicare dati rubati, nel repertorio degli hacker si annoverano anche gli attacchi DDoS. Sebbene molti di loro non abbiano affatto la capacità di sferrare un attacco di questo tipo, se ne servono a scopo di intimidazione per intimorire le potenziali vittime.

Spesso gli hacker scelgono nomi di gruppi già noti per aver compiuto attacchi in passato. Si accontentano di inviare una mail di avvertimento senza preoccuparsi di mettere effettivamente a segno l'attacco. Sperano così che la vittima prescelta inserisca il loro nome in un motore di ricerca e, impressionata dalle malefatte compiute dal gruppo originario, paghi il riscatto.

Anche il gruppo di ricattatori DDoS «Fancy Bear», salito alla ribalta per la prima volta nell'estate del 2017 e attivo anche in Svizzera nel mese di novembre, è ricorso a questo metodo. Stranamente il nome non identifica un gruppo che opera in ambito DDoS, bensì appartiene al gruppo di spionaggio più famoso del mondo. Dietro «Fancy Bear», o il più noto pseudonimo «Sofacy», si presume si celi uno Stato il cui repertorio annovera anche «zero-day exploit», ossia attacchi compiuti con codici che sfruttano le vulnerabilità di un sistema e lasciano ai produttori del sistema zero giorni per correre ai ripari. Dal momento che sinora «Sofacy» non era mai stato collegato a estorsioni in ambito DDoS, si presume che si tratti di un gruppo che utilizza il nome di «Fancy Bear», con l'intenzione di approfittare della sua notorietà nella speranza di ottenere maggiori guadagni.

4.4 Social engineering e phishing

Il presupposto di un buon attacco è un racconto credibile che induca la potenziale vittima a compiere una determinata azione. I cosiddetti attacchi di social engineering funzionano meglio se l'utente malintenzionato riesce a raccogliere numerose informazioni concernenti la potenziale vittima. I truffatori utilizzano sia fonti accessibili a chiunque, sia informazioni provenienti da furti di dati. I dati rubati vengono esaminati, collegati ad altri dati rubati o di pubblico dominio, preparati e rivenduti ad altri criminali.

4.4.1 Phishing

Anche nel secondo semestre del 2017 sono state inviate numerose e-mail di phishing. Il contenuto delle mail non cambia molto: alcuni chiedono i dati della carta di credito per poterli

[13] https://www.blick.ch/news/wirtschaft/sicherheitluecke-bei-herzschrittmachern-5000-schweizer-in-gefahr-id7255939.html (stato: 31.01.2018).

«verificare», altri domandano di cliccare su un link per collegarsi a un certo sito e di inserire la password al fine di usufruire di servizi Internet. In questi messaggi di phishing si fa regolarmente un uso abusivo dei loghi di aziende conosciute o del servizio interessato per conferire una parvenza di ufficialità all'e-mail.

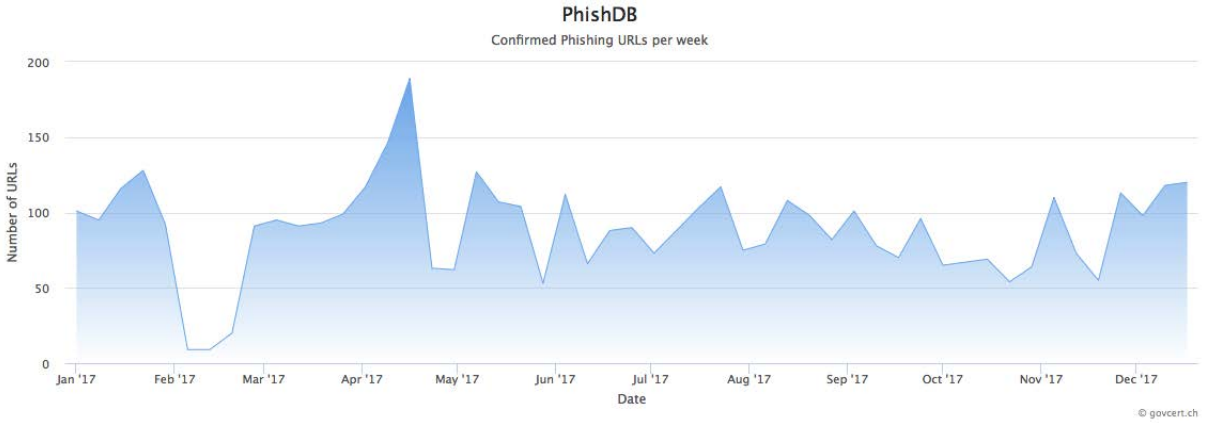

Figura 2 Siti segnalati e confermati di phishing ogni settimana su antiphishing.ch nell'anno 2017

Nel 2017 sono stati segnalati 4587 casi di inequivocabili pagine web di phishing tramite antiphishing.ch, il portale gestito da MELANI. Nella figura 2 sono riprodotti i siti di phishing segnalati settimanalmente, il cui numero varia nel corso del anno. I motivi delle oscillazioni sono disparati: alcune sono dovute a periodi di vacanze, in cui vi sono meno segnalazioni, mentre altre sono dovute al fatto che i criminali spostano regolarmente la loro attenzione da un Paese all'altro.

4.4.2 La truffa delle fatture online – sostituzione delle fatture nell'account di posta elettronica

Oltre agli attacchi compiuti sui dati delle carte di credito, i criminali prendono di mira soprattutto i dati di accesso agli account di posta elettronica. Dal momento che ogni servizio online offre la possibilità di reimpostare la password, l'indirizzo mail degli utenti è ormai diventato il perno e l'asse portante praticamente di tutti i servizi di Internet. Tuttavia, l'account di posta elettronica offre molto di più ai criminali, che oggi si prendono il tempo di passare meticolosamente al setaccio lo scambio di e-mail di un conto manomesso alla ricerca di materiale utilizzabile. Un metodo, che nel secondo semestre del 2017 è stato ripetutamente segnalato a MELANI, è quello di esaminare attentamente l'account alla ricerca di fatture elettroniche. Se i truffatori trovano una fattura attuale, la copiano dalla posta in entrata, dove poi la cancellano. A questo punto hanno tutto il tempo di manipolare la fattura in formato PDF allegata alla mail. Più esattamente, modificano i dati del conto bancario dell'emittente della fattura e inseriscono il loro numero IBAN. Il documento «rivisitato» viene quindi rinviato all'account di posta elettronica. Ai malviventi basta falsificare il mittente indicando l'indirizzo mail della società che ha emesso la fattura. Così la manipolazione è quasi impossibile da individuare.

Raccomandazione

Ad ogni bonifico appaiono le informazioni sul conto del beneficiario. Nel migliore dei casi figura il nome o, almeno, l'istituto bancario del beneficiario. La plausibilità di queste informazioni dovrebbe essere sempre verificata. Fortunatamente i criminali non dispongono di così tanti intermediari finanziari da far figurare sempre un conto idoneo, quindi può succedere che il denaro debba essere trasferito all'estero sebbene la fattura sia stata emessa da una società svizzera. Al più tardi a questo punto le vittime dovrebbero insospettirsi.

4.4.3 Phishing di Office 365 - la chiave di accesso all'ufficio

Dal mese di giugno del 2017 circolano le mail di phishing cosiddette «Office 365». Con oltre 100 milioni di utenti ogni mese, non stupisce che l'account di Office 365 sia diventato un bersaglio popolare tra gli hacker[14]. L'attacco di phishing comincia con un tradizionale messaggio di posta elettronica nel quale si comunica, ad esempio, che lo spazio massimo di memoria è stato superato e, per risolvere il problema, occorre effettuare il login. Ovviamente il link indicato conduce a un sito fraudolento. Gli hacker che entrano in possesso dei dati di accesso a Office 365 possono agire in diversi modi. La situazione più frequente è l'impostazione di una regola di reindirizzamento nell'account di posta elettronica in questione. Così tutte le mail in entrata e in uscita sono inviate a un account predefinito dai malviventi che, quindi, riescono a leggerle. Obiettivi preziosi di questa truffa sono gli account di posta elettronica delle aziende. Le informazioni acquisite possono essere a loro volta utilizzate per colpire altri collaboratori. Dal momento che l'hacker ha accesso anche all'elenco telefonico, può rivolgersi in modo molto mirato a singoli collaboratori all'interno dell'azienda. Gli hacker inviano mail intercettate precedentemente e le manipolano, ad esempio chiedendo ai collaboratori di scaricare un documento. Per avviare il download deve essere nuovamente immessa la password di Office 365 (su un sito contraffatto). In tal modo gli hacker si insinuano poco a poco all'interno della società presa di mira per arrivare alle vittime prescelte.

Una volta che hanno raggiunto la persona stabilita, con i dati trafugati in precedenza attuano una truffa del CEO molto mirata. Non è escluso neppure che ricattino la società con i messaggi di posta elettronica intercettati o che rivendano i dati rubati ad altri malviventi. Questo metodo può essere utilizzato anche per lo spionaggio economico.

Raccomandazione

Se una società lavora nella cloud di Office 365, con i dati di accesso rubati gli hacker possono mettere le mani su tutti i documenti della società. Oggigiorno è estremamente pericoloso proteggere questi dati solo con il nome utente e la password. Ove possibile, conviene dunque attivare sempre l'autenticazione a due fattori.

È opportuno sensibilizzare i collaboratori affinché i processi definiti dall'impresa e le misure di precauzione siano sempre rispettati. In caso di bonifici, ad esempio, è consigliabile osservare il principio del duplice controllo con la firma collettiva.

[14] https://betanews.com/2017/08/30/office-365-phishing/ (stato: 31.01.2018).

4.5 Vulnerabilità

4.5.1 Verificare anche gli ordini dei clienti effettuati allo sportello elettronico

Nel 2017 il sistema di gestione dei pagamenti «Smartvista» del gruppo svizzero BPC ha rilevato una falla di sicurezza che ha potuto essere sfruttata per una SQL Injection[15]. Formulando delle richieste specifiche al momento opportuno sull'interfaccia di transazione «Smart Vista» su cui gli utenti eseguono le operazioni, un hacker potrebbe arrivare a un elenco di tutti gli utenti con le rispettive password attingendo alle banche dati soggiacenti. Un comunicato di BPC ha reso noto che nel mese di maggio del 2017 la società è stata informata della falla dal ricercatore Aaron Herndon della compagnia per la sicurezza Rapid7. Il 19 luglio dello stesso anno la società ha rilasciato un aggiornamento che eliminasse il problema.

4.6 Fuoriuscita di dati

Così come illustrato nel tema principale del presente rapporto, anche nel secondo semestre del 2017 la Svizzera ha registrato numerose fughe di dati. Nel capitolo che segue riepiloghiamo gli incidenti conosciuti avvenuti in Svizzera.

4.6.1 Emersi 70 000 dati di accesso all'online shop di DVD

All'inizio di dicembre del 2017 è stato segnalato a MELANI un elenco di dati di accesso consistenti di login e password. Dalla verifica effettuata è emerso che si trattava di 70 000 dati d'accesso trafugati in Svizzera, ma in quel momento non era ancora chiara la loro provenienza. MELANI ha quindi deciso di inserire i dati nel suo check tool[16] per consentire a chiunque di verificare se il proprio nome utente fosse interessato. In base alle reazioni ricevute MELANI è infine riuscita a identificare il webshop colpito. Si trattava di «dvd-shop.ch», immediatamente informato da MELANI. Il gestore ha quindi reimpostato tutte le password e disattivato il webshop. Secondo il gestore del sito, i dati rubati non sono recenti. I clienti colpiti sono stati informati direttamente da lui.

Raccomandazione

MELANI consiglia di scegliere password sufficientemente lunghe in modo che siano difficili da ricostruire. Per ogni negozio/servizio dovrebbe essere scelta una password diversa. Quando viene offerta la possibilità, è opportuno attivare un secondo fattore per il login.

4.6.2 Gli assicuratori malattie svizzeri vittime dei furti di dati

La cassa malati Groupe Mutuel ha reso noto in un comunicato stampa che il 19 dicembre 2017 alcuni hacker si sono infiltrati sotto falsa identità nella piattaforma IT esterna «ePremium Health», lanciata nel 2012, con l'intenzione di rubare dati. La piattaforma serve alla rete di vendita del Groupe Mutuel per predisporre offerte e richieste di copertura assicurativa. In base

15 https://blog.rapid7.com/2017/10/11/r7-2017-08-bpc-smartvista-sql-injection-vulnerability/ (stato: 31.01.2018).

16 https://www.checktool.ch Per effettuare il controllo è sufficiente inserire l'indirizzo mail o il nome utente. Questi dati non sono trasmessi a MELANI sotto forma di testo in chiaro né memorizzati. (stato: 31.01.2018)

ai dati dell'assicuratore malattie il furto non ha interessato polizze assicurative, rapporti medici, conteggi dei premi, conteggi della partecipazione alle spese e simili. Il sistema IT interno del Groupe Mutuel, nel quale erano memorizzati i dati di circa 1,4 milioni di clienti, non è mai stato in pericolo. Dopo il cyberattacco il Groupe Mutuel ha sporto denuncia penale contro ignoti. La polizia cantonale del Vallese è riuscita a identificare rapidamente i presunti colpevoli e ha arrestato il primo di loro già il 28 dicembre 2017. Il giorno dopo la polizia cantonale turgoviese ha fermato un secondo sospettato. Si tratta di un cittadino svizzero di 29 anni e di un cittadino macedone di 30 anni. Entrambi sono stati messi in detenzione preventiva. Secondo la polizia, l'indagine prosegue[17].

Nel mese di febbraio del 2018 Groupe Mutuel ha pubblicato un modulo con il quale le potenziali vittime potevano appurare se erano state interessate dalla fuga di dati. Sono a rischio soprattutto le persone e le imprese che dal 2012 a oggi hanno chiesto a un intermediario o a un broker un'offerta per una polizza assicurativa del Groupe Mutuel[18].

4.6.3 Dati relativi alle malattie presso una società di gestione crediti – fuga di dati da EOS

Alla fine di dicembre del 2017 la «Süddeutsche Zeitung»[19] ha pubblicato la notizia di una fuga di dati dalla filiale svizzera della società di gestione crediti EOS. Il gruppo EOS opera in ben 26 Paesi e comprende 55 imprese singole. Nell'incidente in questione sono stati probabilmente trafugati dati per circa tre gigabyte. Oltre a nomi, indirizzi e importi dovuti, il furto ha riguardato anche altri dati sensibili, tra cui le informazioni concernenti lo stato di salute con indicazioni delle malattie pregresse e i dettagli dei trattamenti. I dati trafugati comprendono anche documenti d'identità e numerosi conteggi delle carte di credito. Le serie di dati risalgono al 2002.

Apparentemente i medici hanno caricato o potuto caricare tutte le informazioni concernenti lo stato di salute dei pazienti su un portale di EOS. Non è noto a quale fine e a quali condizioni ciò sia avvenuto. Sicuramente dati sensibili come quelli sullo stato di salute non sono indispensabili per il compito che una società di gestione crediti è chiamata a svolgere.

Presumibilmente la fuga di dati è cominciata già nel mese di aprile del 2017 con un attacco mirato che ha sfruttato la falla di sicurezza «Apache Struts». Secondo EOS, all'epoca erano stati individuati i primi segnali di un attacco che, tuttavia, non hanno mai potuto essere verificati. Nonostante ciò, il server colpito è stato completamente riconfigurato. Non è noto se i dati siano effettivamente collegati a questo incidente oppure se si sia verificata un'altra falla.

4.6.4 Flusso di dati anche alla Digitec

Il 6 novembre 2017 Digitec ha ammesso l'eventualità che i dati provenissero da una vecchia banca dati. Allo stato attuale delle conoscenze risulta che i dati dei clienti potenzialmente colpiti

---

17 https://www.polizeiwallis.ch/medienmitteilungen/martinach-hackerangriff-auf-eine-versicherungsgesellschaft/ stato: 31.01.2018).

18 https://www.groupemutuel.ch/it/clients-prives/page/cyberattaque.html (stato: 31.01.2018).

19 http://www.sueddeutsche.de/digital/it-sicherheit-schwerwiegendes-datenleck-legt-zehntausende-schuldnerdaten-offen-1.3805589 (stato: 31.01.2018).

vadano dal 2001 fino alla metà del 2014 al massimo. Nel frattempo la presunta falla di sicurezza sarebbe stata risolta e il nuovo online shop Digitec non sembrerebbe colpito. Quando esattamente abbia avuto luogo il flusso di dati, non è ad oggi noto.[20]

4.7 Crimeware

Il crimeware è una forma di malware che dal punto di vista criminologico rientra nel campo della criminalità informatica e giuridicamente rientra nel settore del danneggiamento di dati e dell'abuso di un impianto per l'elaborazione di dati. Anche nel secondo semestre del 2017 sono state rilevate numerose infezioni riconducibili ad attacchi di crimeware. La statistica nella figura 3 riproduce dati di singoli server a cui si connettono computer infetti. Ci sono altri malware che hanno pure un rilievo importante ma non compaiono nella statistica (per esempio il crimeware Retefe). Così come avvenuto negli anni precedenti, la maggior parte delle infezioni sono imputabili al malware «Downadup» (noto anche come «Conficker»), un worm che esiste già da più di dieci anni e si diffonde tramite una falla di sicurezza rilevata nei sistemi operativi Windows nel 2008 e perciò colmata da tempo. Al secondo posto si colloca «gamarue»[21], conosciuto anche con il nome di «andromeda», un software di download che può scaricare altri malware. Al terzo e al quarto posto troviamo i malware «spambot» e «cutwail», che si sono specializzati nell'invio di spam e malware. La rete bot «Mirai», resa celebre dall'attacco al fornitore di servizi Internet «Dyn», che infetta apparecchiature dell'Internet delle cose è scesa dal quarto al settimo posto. Al nono posto si colloca il primo trojan «Gozi» che colpisce chi opera con l'e-banking.

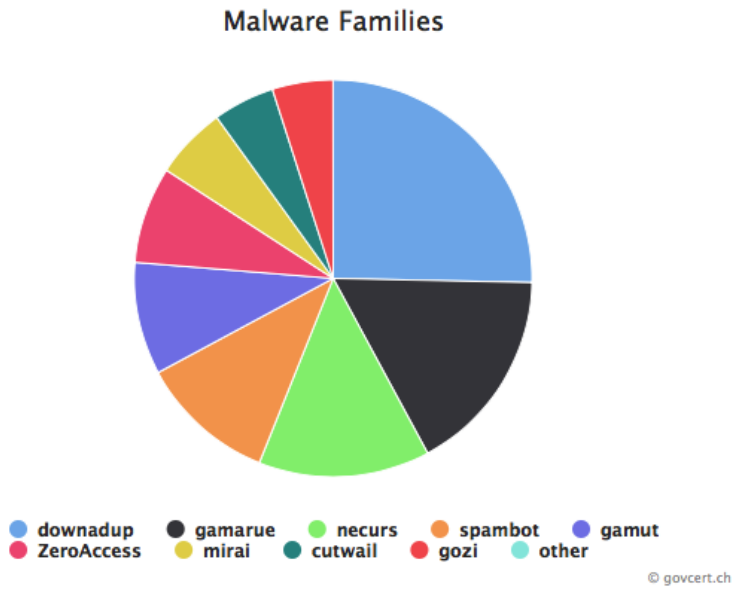

Figura 3: Distribuzione dei malware in Svizzera noti a MELANI. La data di riferimento è il 31 dicembre 2017. I dati aggiornati sono pubblicati nel sito: http://www.govcert.admin.ch/statistics/dronemap/

[20] https://www.digitec.ch/de/page/statement-zum-digitec-leck-6265 (stato: 31.01.2018).

[21] https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/Schadsoftware/Andromeda_Gamarue.html (stato: 31.01.2018).

4.7.1 Ransomware

Anche nel periodo in rassegna, sono stati segnalati a MELANI numerosi casi di ransomware (ossia di trojan che cifrano documenti a scopo di estorsione). Per difendersi è di vitale importanza eseguire un backup funzionante su un supporto esterno che non possa essere attaccato dal ransomware. Ancora meglio sarebbe impedire al ransomware di arrivare a questo punto adottando le opportune misure preventive. La cifratura, e quindi la perdita temporanea di dati, rappresenta infatti solo una parte del problema. Occorre anche considerare che nel tempo occorrente per il caricamento del backup gran parte dell'azienda può essere paralizzata. Siccome oggi la maggior parte delle aziende è dipendente da TIC funzionanti, un'interruzione può comportare considerevoli perdite finanziarie. Per le infrastrutture critiche, un'interruzione dell'attività potrebbe avere conseguenze ancora più gravi.

Raccomandazione

Pagina informativa di MELANI sui ransomware

https://www.melani.admin.ch/melani/it/home/themen/Ransomware.html

4.7.2 Trojan in azione nell'e-banking – «Retefe» tuttora molto diffuso

Diversi trojan che agiscono a livello di e-banking sono più o meno attivi in Svizzera. Tra questi si trova, ad esempio, il malware «Dridex», che ha la capacità di ampliare le sue funzioni per compiere attacchi mirati ai clienti commerciali. A tal fine «Dridex» perlustra un sistema infetto alla ricerca di software per l'e-banking offline[22]. Il trojan «Gozi ISFB» si diffonde sia tramite le infezioni nei siti web sia con allegati infetti alle mail. Nel 2017 «Trickbot» ha esteso l'elenco dei suoi bersagli anche agli istituti bancari elvetici. «Trickbot» è concepito con una struttura modulare e viene potenziato con funzioni sempre nuove. «Emotet», originariamente un gruppo di malware utilizzato per colpire a livello dell'e-banking, viene utilizzato dai criminali anche per la diffusione di altri malwere ad esempio ransomware e per la sua diffusione ricorre soprattutto a fatture contraffatte.

Ma un dei software nocivi più aggressivo in Svizzera rimane «Retefe». In passato ha colpito esclusivamente in Austria, Svezia, Giappone, Gran Bretagna e Svizzera. MELANI ha trattato «Retefe» già in un suo rapporto semestrale di tre anni fa. A differenza di altri malware, che si diffondono infettando siti web, «Retefe» si propaga esclusivamente tramite mail. In passato ciò avveniva soprattutto con le fatture contraffatte di online shop, ad esempio Zalando o Ricardo, mentre le versioni più recenti si spacciano in primo luogo per gli uffici della Confederazione o parastatali, come l'Amministrazione delle contribuzioni o la Posta.

[22] Rapporto semestrale 2016/2, cap. 4.6.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2016-2.html (stato: 31.01.2018).

Se l’infezione ha successo, Retefe modifica le impostazioni del browser in modo che determinati siti web (in particolare i portali di e-banking di alcuni istituti finanziari svizzeri) vengano deviati tramite un proxy server. Inoltre «Retefe» installa un certificato sul computer con il quale può a sua volta rilasciare certificati per qualsiasi istituto finanziario e spacciarsi come tale. Il malware evita la visualizzazione del messaggio di errore del certificato che desterebbe sospetti nella vittima. 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.

Nel semestre passato i malviventi hanno ampliato il loro modus operandi cercando di entrare in possesso di lettere con i cosiddetti dati di attivazione. Solitamente queste lettere sono inviate dalla banca ai clienti per posta e contengono un mosaico che deve essere scannerizzato con un’apposita app la prima volta che si effettua il login nell’e-banking con un dispositivo. A questo punto il dispositivo viene autorizzato dalla banca per il metodo di autenticazione mobile. Mediante pratiche di social engineering, gli hacker hanno cercato di arrivare ai dati di attivazione chiedendo alla vittima di scannerizzare o fotografare la lettera e di trasmetterla ai truffatori.

Nel mese di settembre scorso, al malware si è aggiunto l’exploit di «EternalBlue». Si tratta della falla che in maggio è stata sfruttata per compiere il pesante attacco con il trojan di crittografia «WannaCry», all’origine di danni su scala globale. Con l’implementazione di «EternalBlue» è possibile che «Retefe» voglia mirare alla diffusione soprattutto nelle reti aziendali. Se un collaboratore apre inavvertitamente un allegato infetto, il malware può contaminare il computer nel quale la società esegue i suoi pagamenti e-banking. Naturalmente questa pratica funziona solo se la falla non è ancora stata colmata.

Nel periodo in esame MELANI ha ripetutamente ricevuto nuove segnalazioni di mail infettate con «Retefe» nel cui oggetto figuravano sia l’appellativo corretto sia l’esatto numero di telefono del destinatario. Nella maggior parte dei casi i criminali si spacciavano per collaboratori dell’Amministrazione federale delle contribuzioni (AFC), fingendo di avere domande sulla dichiarazione d’imposta. In realtà c’erano elementi a sufficienza per destare dubbio nei riceventi. Presumibilmente, l’indicazione del proprio numero di telefono ha tuttavia indotto alcuni destinatari ad aprire l’allegato.

Von: Eidgenossische Steuerverwaltung ESTV [redacted]
Gesendet: Mittwoch, 21. Februar 2018 11:32
An: [redacted]
Betreff: Fragen zu der Steuererklarung (die Nummer 043 [redacted] ist unzuganglich)

Sehr geehrte(r) Herr/Frau [redacted]

Mein Name ist [redacted], ich bin Finanzinspektor und bin zuständig für Ihren Bezirk.

Es gibt einige Fragen zu Ihrer Einkommensteuererklärung.

Dieses Dokument beinhaltet die Liste von Fragen über Ihre Steuererklärung, sowie auch meine Kontaktnummer.

Freundliche Grüsse

[redacted]

Das Gemeindesteueramt

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Figura 4: Esempio di una mail fraudolenta con il malware «Retefe» e il numero di telefono riportato nell'oggetto

Inizialmente non era chiaro come gli hacker potessero collegare i dati dell'indirizzo mail, il nome e il cognome e, soprattutto, il numero di telefono. Tuttavia MELANI ha ricevuto diverse segnalazioni dai cittadini che le combinazioni di dati potessero provenire da un furto.

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 Medio Oriente nel mirino

Le campagne di spionaggio informatico si possono suddividere in due categorie: quelle motivate da ragioni economiche e quelle che mirano alle informazioni strategiche, militari e/o politiche. Di seguito sono esposte alcune campagne. Ad esempio le tensioni politiche in Medio Oriente e la rilevanza di quei Paesi nel settore della produzione gas-petrolifera, fanno di questa regione un bersaglio appetibile per il cyber-spionaggio.

5.1.2 Esempio APT33

«Non sono solo gli avversari politici ed economici a possedere dati interessanti, ma anche le informazioni dei partner possono essere preziose». Potrebbe essere questo lo slogan della campagna di spionaggio informatico «APT33»[23] che la società di sicurezza statunitense

[23] https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html (stato: 31.01.2018).

FireEye attribuisce a un servizio iraniano. APT33 è attivo almeno dal 2013 e ha colpito soprattutto obiettivi sauditi, statunitensi e sudcoreani del settore militare, dell'aviazione civile e dell'energia. Pare che da metà 2016 all'inizio 2017 APT33 abbia violato un'azienda aerospaziale americana e un'organizzazione saudita operante anch'essa nel settore dell'aviazione. APT33 ha diffuso i suoi malware tramite e-mail mascherate da offerte di lavoro. L'indirizzo del mittente delle e-mail conteneva nomi di dominio simili a quelli registrati da società aerospaziali saudite e occidentali, che collaborano con l'Arabia Saudita sia in ambito civile che militare. Secondo la società di sicurezza FireEye i menzionati attacchi miravano a ottenere informazioni militari dell'aeronautica militare saudita per incrementare il know-how delle forze aeree iraniane e utilizzare le notizie acquisite nelle decisioni militari e strategiche di Teheran.

La campagna di spionaggio ha colpito nello stesso periodo anche una raffineria sudcoreana. Nel maggio 2017, ai collaboratori di un'azienda saudita e di un'azienda sudcoreana, entrambe operanti nel settore petrolifero, sono state inviate e-mail mascherate da offerte di lavoro che contenevano un programma di spionaggio e che apparentemente provenivano da una società petrolifera saudita.

Pare che FireEye abbia identificato una persona, probabilmente un ex-membro del governo iraniano, collegata a questi fatti. Alcuni dei malware utilizzati contenevano inoltre parole in farsi, la lingua ufficiale dell'Iran. Anche gli orari e i giorni in cui sono stati sferrati questi attacchi e l'utilizzo di malware specifici che si trovano su siti di hacker iraniani, sembrano confermare il sospetto di un'orchestrazione da parte iraniana.

Anche «Shamoon», la più famosa campagna informatica finora sferrata da attori presumibilmente iraniani, che a partire dal 2012 ha bersagliato organizzazioni nel Golfo Persico, si concentrava sul settore petrolchimico.

5.1.3 «Copy Kittens» - sviluppo tecnico e strategico[24]

Il 29 marzo 2017, l'Ufficio federale tedesco per la sicurezza informatica (BSI) ha comunicato che il sito web del quotidiano «Jerusalem Post» era stato violato e manomesso per diffondere programmi dannosi. L'infezione del sito sarebbe probabilmente all'origine di non meglio specificate anomalie riscontrate nel traffico web del parlamento federale a partire da gennaio 2017.[25] In quello stesso mese la società di cyber-intelligence israeliana ClearSky aveva confermato l'infezione del «Jerusalem Post» e reso pubbliche anche infezioni di altri siti israeliani, compreso quello del ministero della salute palestinese, attribuendone la paternità al gruppo di spionaggio «CopyKittens».[26] I siti violati da ottobre 2016 alla fine di gennaio 2017 contenevano un javascript, che scaricava, da un dominio appositamente registrato dagli hacker, uno strumento di *penetration testing* specifico per browser. Il codice javascript non veniva trasmessi ad ogni visitatore del sito, ma solo a vittime appositamente selezionate.

«CopyKittens» è un gruppo di spie informatiche attivo almeno dal 2013, il cui nome si ispira alla prassi di copiare frammenti di codice di forum online e utilizzarli per i loro cyber-attacchi. Nel mirino del gruppo sono finiti soprattutto Israele, Arabia Saudita, Turchia, Stati Uniti,

---

24 http://www.clearskysec.com/tulip/ (stato: 31.01.2018).

25 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Cyber-Angriff_auf_den_Bundestag_Stellungnahme_29032017.html (stato: 31.01.2018).

26 http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf (stato: 31.01.2018).

Giordania e Germania, ma anche funzionari dell'ONU. Tra gli obiettivi dal gruppo figurano istituzioni statali e scientifiche, imprese dell'industria della difesa, fornitori del ministero della difesa e grandi aziende informatiche.

La campagna si diffonde, oltre che con gli attacchi Watering Hole sopra descritti, anche tramite e-mail mirate con allegati o link dannosi. Come esempio di link si può citare un'e-mail destinata ai collaboratori di numerose organizzazioni governative. L'e-mail era stata inviata a fine aprile 2017 da un account di posta manomesso. Il titolo dell'allegato infetto rimandava a relazioni internazionali tra l'Iran, la Corea del Nord e la Russia. In altri due casi il gruppo ha violato l'account di posta di persone vicine all'obiettivo reale dell'attacco. Gli scambi di messaggi del legittimo titolare venivano utilizzati in modo fraudolento per inviare un'e-mail con un link a un sito registrato appositamente per questo scopo.

Il gruppo gestisce e amministra già dal 2013 falsi profili Facebook, tramite i quali tenta di instaurare così un clima di fiducia con le potenziali vittime, raccogliendo informazioni su di loro per altri attacchi. I falsi profili venivano utilizzati anche per diffondere link a un sito infetto. Per risultare più credibili, questi profili pubblicavano anche materiale innocuo e il numero di amici era tale da non destare sospetti.

Conclusione

Nel 2015 «Copy Kittens» era ritenuto solo un virus con potenziale dannoso medio. Ma gli attacchi recentemente scoperti dimostrano che il gruppo si è in apparenza perfezionato tecnicamente e strategicamente e oltre ai malware acquistati in rete utilizza anche programmi sviluppati in proprio.

5.1.4 Il gruppo OilRig sviluppa nuovi sistemi di attacco[27]

In passato, le campagne di spionaggio del gruppo «OilRig» puntavano su aziende pubbliche e private in Nord America ed Europa, concentrandosi in particolare sulla produzione di petrolio e gas e sul loro commercio in Medio Oriente. Nel semestre in esame OilRig ha aggiunto al suo arsenale un nuovo trojan che prende di mira il Medio Oriente. Tra luglio e agosto 2017 sono stati lanciati in diversi attacchi due nuovi strumenti: il backdoor «ISMAgent» e un injector per la sua installazione. L'injector possiede una struttura complessa e contiene tecnologie che ne complicano ulteriormente l'individuazione sui computer infettati.

Il 23 agosto 2017 OilRig ha attaccato un servizio governativo interno degli Emirati Arabi Uniti tramite un'e-mail mirata di phishing con due allegati ZIP e una immagine nel corpo della mail. L'immagine veniva scaricata da un server esterno e serviva probabilmente per assicurarsi che il destinatario aprisse la mail. L'attacco utilizzava anche altri interessanti espedienti tecnici. L'indirizzo del mittente non era falsificato, anche se il mittente risultava essere un indirizzo interno della società. Probabilmente «OilRig» si era impossessato dei dati di autenticazione di un account di posta legittimo all'interno del dominio stesso, da cui poteva poi inviare la mail infetta. Entrambi i file ZIP contenevano un documento Word. Nel primo era nascosta la macro dannosa tramite cui l'injector installava la backdoor. A tal fine gli hacker si sono serviti di tecniche di social engineering per indurre i destinatari ad acconsentire all'esecuzione della

[27] https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/ (stato: 31.01.2018).

macro. Il secondo documento cercava di sfruttare una falla nella sicurezza di Microsoft Word[28], per la quale era stato rilasciato da poco l'aggiornamento. Il gruppo cerca di sfruttare sia lacune tecniche sia debolezze umane.

Dopo essere penetrati nel sistema, gli hacker utilizzano programmi reperibili sul mercato nero, come ad esempio «Mimikatz», per procurarsi i dati di autenticazione dell'azienda e muoversi tra i computer della rete aziendale. Secondo la società di network security «Palo Alto», il gruppo mette in atto anche cosiddetti attacchi Supply Chain[29]: questo metodo consiste nell'attaccare l'obiettivo non direttamente, ma per vie traverse tramite un fornitore di servizi dell'azienda. Avendo questi accesso alla rete della vittima predestinata o fornendole software e hardware, l'attacco può essere sferrato indirettamente. Dato che di solito ogni azienda si avvale di più fornitori di servizi, con questo metodo l'hacker dispone di una «scelta» più ampia di possibilità (e falle) per realizzare i suoi scopi. Questo metodo viene utilizzato sempre più spesso, come descritto anche nel capitolo «Attacchi internazionali» del rapporto semestrale 1/2017[30]: stando alle previsioni annuali di Kaspersky sulle minacce nel 2018, questa minaccia dovrebbe acutizzarsi ulteriormente nel corso dell'anno[31].

Conclusione

La Svizzera non rientra tra gli obiettivi del gruppo OilRig, ma sul suo territorio sono presenti numerosi fornitori di prodotti e servizi specifici del settore petrolchimico e gli attacchi sono dunque ipotizzabili anche qui.

5.1.5 Spazi pubblicitari su Facebook acquistati per scopi propagandistici da una presunta società russa [32]

Nell'ultimo rapporto semestrale è stato trattato il tema dell'intrusione di Stati terzi nelle elezioni presidenziali statunitensi tramite attacchi informatici mirati. Gli obiettivi non erano solo i sistemi di conteggio delle schede elettorali (a riguardo di ciò non ci sono segnalazioni di manipolazioni avvenute con successo) e la corrispondenza e-mail del partito democratico: i servizi segreti americani hanno dichiarato che parallelamente venivano diffuse campagne di disinformazione soprattutto tramite i social network. Recentemente una campagna di propaganda svolta su Facebook durante le elezioni presidenziali negli Stati Uniti è stata messa in relazione a una presunta società russa, l'«Internet Research Agency», che pare abbia acquistato spazi pubblicitari su Facebook per diffondere posizioni politiche del governo russo. Più di 3300

---

28 CVE-2017-0199 Microsoft Word Office/WordPad Remote Code Execution Vulnerability

29 https://researchcenter.paloaltonetworks.com/2017/12/unit42-introducing-the-adversary-playbook-first-up-oilrig/ (stato: 31.01.2018).

30 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2017-1.html (stato: 31.01.2018).

31 https://www.kaspersky.com/about/press-releases/2017_kaspersky-labs-threat-predictions-for-2018 (stato: 31.01.2018).

32 https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.936611ed98fb (stato: 31.01.2018).

inserzioni pubblicitarie possono essere ricondotte a questa campagna russa.[33] Sono stati diffusi e pubblicizzati oltre 470 profili falsi. I nomi dei due candidati alla presidenza USA sono stati nominati sporadicamente in alcuni post, ma principalmente sono stati propagati contenuti politici su temi delicati come ad esempio le unioni omosessuali, l'immigrazione e il diritto al possesso di armi. Alcuni post invece non avevano proprio lo scopo di propagare controversie ideologiche, ma soltanto quello di gettare nel panico e nel caos la rete. Il giornale «Washington Post» cita ad esempio una fake news relativa a una fuga di sostanze chimiche in Louisiana. La propaganda è stata gestita in modo mirato, cioè i contenuti erano visibili solo a persone di determinate regioni.

Già nel gennaio 2017 i servizi segreti americani avevano accusato la Russia[34] di interferire con le elezioni presidenziali. La Russia pare abbia sovvenzionato anche cosiddetti troll, che diffondono notizie false sui social network e influenzano l'opinione pubblica. In seguito a queste accuse il CEO di Facebook, Mark Zuckerberg, ha promesso di dichiarare guerra alle fake news sulla sua piattaforma.

5.2 Furti di dati

Il periodo in rassegna è stato di nuovo caratterizzato da diversi casi di furti consistenti di dati, riportati sulle prime pagine dei media.

5.2.1 Equifax

Tra i casi più spettacolari vi è senza dubbio quello che ha interessato Equifax, una delle principali società statunitensi di valutazione dell'affidabilità creditizia. Il 7 settembre 2017 l'azienda ha annunciato di aver scoperto un'intrusione nelle sue reti, che si era verificata nel mese di luglio. Apparentemente, l'intrusione sarebbe stata causata da una nota falla in Apache Struts, per la quale l'azienda non aveva installato la patch. Questa falla ha potenzialmente messo in pericolo i dati personali di 143 milioni di clienti statunitensi. Oltre al numero di persone colpite, aspetto che rende questo caso particolarmente critico, vi è la quantità di informazioni personali e finanziarie a cui l'azienda ha accesso e che le consentono di calcolare i rischi creditizi. Queste informazioni comprendono, tra l'altro, il numero di previdenza sociale (*social security number, SSN*[35]). L'incidente ha evidenziato le questioni aperte in materia di sicurezza, legate a questo numero univoco, inizialmente previsto per l'identificazione delle persone nell'ambito della previdenza sociale, ma che nel tempo è diventato un identificatore univoco, utilizzato in ambiti diversi come nella sanità, per le imposte o la concessione di crediti. Il furto di questo numero, ancor più se corredato da altre informazioni personali sul suo titolare, offre numerose possibilità per commettere frodi e usurpazioni d'identità.

---

33 http://www.wired.co.uk/article/facebook-twitter-russia-congress-fake-ads-2016-election-trump (stato: 31.01.2018).

34 http://www.zeit.de/politik/ausland/2017-01/hacker-angriff-us-wahl-russland-barack-obama-geheimdienste (stato: 31.01.2018).

35 https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/statistik--register-und-forschung/numero-avs.html (stato: 31.01.2018).

5.2.2 Imprese di revisione e consulenza

Il clamore mediatico era appena calato, quando il 25 settembre 2017 il quotidiano britannico *The Guardian* ha divulgato la notizia di un incidente informatico che aveva colpito nuovamente una grande società americana[36]. Secondo le informazioni fornite dal quotidiano britannico, il servizio di posta elettronica della Deloitte, una delle quattro maggiori società di revisione (*big four*) del mondo, sarebbe stato compromesso dal mese di ottobre o novembre del 2016. Un account amministratore non sufficientemente protetto avrebbe consentito di accedere alle e-mail scambiate tra la Deloitte e i suoi clienti più importanti, salvati sul cloud «Azure» di Microsoft. Il livello di sicurezza dell'azienda molto criticato, ancor più a seguito delle rivelazioni inerenti ad elementi potenzialmente vulnerabili della sua infrastruttura di rete visibili su Internet (ad es. accesso RDP aperto, identificatori del servizio VPN)[37]. Tra le sue molteplici attività, Deloitte fornisce servizi di consulenza nel settore della sicurezza informatica ad aziende che operano in numerosi settori critici. Nel mese di giugno del 2017, Deloitte è stata nominata da Gartner, per il quinto anno consecutivo, prima azienda al mondo fornitrice di servizi di consulenza nel settore della sicurezza informatica.

5.2.3 Ricatto con dati sulle abitudini di guida

Neppure la Silicon Valley è stata risparmiata dai furti di dati. A novembre Uber ha confermato di essere stata vittima di un furto di dati personali di 57 milioni di clienti e autisti. L'azienda era informata sui dettagli dell'incidente dalla fine del 2016. Secondo Bloomberg[38], l'incidente informatico è stato causato dall'utilizzo di una pagina privata sul sito GitHub da parte di ingegneri di Uber. Gli autori dell'attacco informatico hanno potuto recuperare gli identificatori che hanno consentito loro di accedere alle informazioni sensibili memorizzate dall'azienda sul cloud di Amazon, dopo di che hanno chiesto ad Uber un riscatto di 100 000 dollari, apparentemente andato a buon fine, in cambio dei dati e della non divulgazione dell'incidente. Tuttavia, il pagamento del riscatto e la supposta distruzione dei dati non hanno risolto l'incidente: il caso è infatti diventato comunque di dominio pubblico. Per giunta scegliendo di non informare né le autorità né le vittime di essere a conoscenza dei fatti, Uber non ha adempiuto agli obblighi di legge. Diversi procedimenti giudiziari sono attualmente in corso. Non è risaputo se la ditta dopo il primo pagamento del riscatto sia stata nuovamente ricattata.

5.2.4 Supporto informatico perso

Che le fughe di dati non siano sempre causate da falle nella sicurezza o da sistemi mal configurati lo dimostra un caso verificatosi in Gran Bretagna. Nell'ottobre 2017 un passante ha notato per le vie di Londra una chiavetta USB da 2.5 Gigabyte contenente dati cifrati, che riguardavano anche informazioni sensibili sull'aeroporto di Heathrow, come ad esempio informazioni sui punti in cui erano installate telecamere di sorveglianza, vie di fuga e orari delle pattuglie di polizia. Il passante ha consegnato la chiavetta USB a un giornale che poi ha reso pubblico l'accaduto. Resta ancora da chiarire come quella pennetta sia finita per strada.

---

36 https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails (stato: 31.01.2018).

37 https://www.theregister.co.uk/2017/09/26/deloitte_leak_github_and_google/ (stato: 31.01.2018).

38 https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (stato: 31.01.2018).

Conclusione

Ridurre al minimo i rischi informatici è un processo globale che deve comprendere anche misure di sicurezza fisiche. A tal fine occorre regolamentare chiaramente i dati che possono essere memorizzati su supporti esterni e le misure di sicurezza (ad esempio il livello di cifratura) da adottare.

Trovate maggiori informazioni nel tema principale esposto al capitolo 3.

5.3 Sistemi industriali di controllo

5.3.1 «Dragonfly» spia l'infrastruttura dei fornitori di energia

In luglio, il New York Times ha riferito che una centrale elettrica nel Kansas era finita nel mirino degli hacker da maggio 2017[39]. Da allora sono emersi ripetuti cyber-attacchi nel settore energetico negli Stati Uniti e in Europa[40,41]. Anche se gli articoli dei media danno l'impressione che gli attacchi nel settore energetico si stiano moltiplicando e che un nuovo gruppo chiamato «Palmetto Fusion» stia creando scompiglio, è probabile che tutte queste operazioni si possano ricondurre a un unico soggetto attivo dal 2011 denominato «Dragonfly»[42], alias «Havex», «Energetic Bear», «Crouching Yeti» ecc. che tiene sotto attacco il settore energetico negli Stati Uniti e in Europa dal 2013. Dal 2017 questi attacchi, raggruppati sotto la denominazione «Dragonfly 2.0», si sono visibilmente intensificati e migliorando anche dal punto di vista tecnico.

«Dragonfly 2.0» sfrutta le mail di Spear Phishing per i suoi attacchi[43] con allegati o link infetti e siti web appositamente predisposti e modellati in base alla sfera personale delle vittime, i cosiddetti Watering Hole[44]. I siti violati e utilizzati per gli attacchi rimandano alle vittime designate di «Dragonfly»: aziende attive nel settore energetico, operatori del settore energetico, avvocati specializzati nel settore energetico e produttori di soluzioni informatiche per l'industria europea e statunitense. Gli hacker cercano in questo modo di procurarsi i dati di accesso a reti critiche. La società di software statunitense Symantec riferisce nel suo rapporto su «Dragonfly 2.0» oltre che di vittime negli USA e in Turchia, anche di un'azienda attaccata in Svizzera. Finora MELANI non ha potuto verificare questa affermazione. Non è ancora stata identificata nessuna vittima svizzera.[45]

---

39 https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html (stato: 31.01.2018).

40 https://www.wired.com/story/russian-hacking-teams-infrastructure/ (stato: 31.01.2018).

41 https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html (stato: 31.01.2018).

42 https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear (stato: 31.01.2018).

43 http://blog.talosintelligence.com/2017/07/template-injection.html (stato: 31.01.2018).

44 https://www.riskiq.com/blog/labs/energetic-bear/ (stato: 31.01.2018).

45 https://www.watson.ch/Digital/Schweiz/472496967-Droht-ein-Blackout--Hacker-attackieren-Schweizer-Energiesektor (stato: 31.01.2018).

Conclusione

Lo spionaggio delle reti informatiche nel settore energetico può essere destinato a vari scopi. Da un lato gli hacker possono procurarsi l'accesso alle reti per rubare informazioni e ottenere un vantaggio strategico ed economico, dall'altro il controllo esercitato su computer di reti critiche consente all'occorrenza di manomettere o pregiudicare processi.

Attualmente non si hanno notizie di sabotaggi con «Dragonfly» in una sua qualche versione. Tuttavia, non si può escludere che in futuro anche «Dragonfly» preveda di portare a termine tali attacchi, in particolare se cambia la situazione politica. Gli attuali tentativi di spionaggio potrebbero anche servire, ad esempio, per farsi un quadro delle possibilità per poi essere pronti a qualsiasi eventualità politica. Gli attacchi del gruppo «Sandworm» - un altro soggetto con caratteristiche simili, che nel 2015/2016 aveva sabotato la rete elettrica ucraina - hanno dimostrato che servono lunghi mesi di preparativi per capire le configurazioni dei sistemi di controllo presi di mira e le combinazioni di comandi necessarie per mettere in atto il sabotaggio. Un problema è rappresentato dal fatto che anche i tentativi di disinfestazione possono provocare danni collaterali indesiderati in caso di cattiva esecuzione. I tentati attacchi osservati dimostrano l'importanza dell'impiego di un'ampia gamma di misure come descritto nel capitolo 4.2.

5.3.2 Attacco contro i sistemi di controllo di sicurezza

Nel dicembre 2017 diverse società di sicurezza hanno pubblicato articoli riguardanti un software maligno denominato «Triton/Trisis», che colpisce le soluzioni di sicurezza dei processi per impianti di controllo industriali. Questo software maligno, scoperto a metà novembre 2017 e attivo almeno dall'agosto 2017, attacca nello specifico singole configurazioni del sistema «Triconex» della società francese Schneider Electric. Si è parlato di almeno un obiettivo situato in Medio Oriente.

Finora gli attacchi riguardavano direttamente i comandi del processo principale. Le soluzioni di sicurezza dei processi sorvegliano e controllano invece la gestione di un impianto. Se ad esempio la pressione o la temperatura del processo da sorvegliare supera un valore critico che potrebbe danneggiare l'impianto, vengono attivate automaticamente le contromisure (come ad esempio l'arresto o l'impedimento di un'operazione). Se si riesce a manomettere un sistema di sicurezza di questo tipo in modo da impedire l'arresto automatico in caso di anomalia, si può danneggiare l'impianto o addirittura distruggerlo oppure ferire o uccidere persone. Talvolta sul sistema interviene un operatore per avviare manualmente queste misure.

Gli attacchi mirati ai sistemi industriali di controllo sono ancora rari. «Triton/Trisis» è solo il quinto software maligno noto, che aggredisce specificamente i controlli industriali. Il più famoso malware di questo tipo è «Stuxnet», scoperto nel 2010 per danneggiare o distruggere le centrifughe di impianti di arricchimento dell'uranio iraniani. Esempi più recenti sono gli attacchi

di dicembre 2015[46] e 2016[47] alla rete di alimentazione elettrica dell'Ucraina con rispettivamente il malware «Blackenergy» e «Industroyer/Crashoverride».

Conclusione

Questi attacchi sono stati finora utilizzati con molta circospezione, probabilmente perché un'operazione di questo tipo comporta sempre il rischio di un danno collaterale incontrollabile che può anche avere conseguenze incalcolabili per gli hacker. In questo caso l'esito è stato fatale per gli hacker. I loro tentativi di manomissione tramite il malware hanno provocato l'arresto di emergenza automatico del sistema attaccato e la ricerca di tale arresto ha portato alla scoperta del malware. Questo è il motivo per cui questi attacchi vengono sferrati in genere contro una specifica configurazione del sistema e pertanto sono costosi. Costi così elevati non sono assolutamente sostenibili per gli hacker che puntano a guadagnare denaro, ma generalmente possono essere sostenuti soltanto da uno Stato. Il sistema «Triconex» è molto utilizzato nell'industria, ma ogni implementazione è a sé stante e un vettore d'attacco non può essere trasferito su un altro sistema senza costi significativamente maggiori. Il fatto che gli hacker mirino alle soluzioni di sicurezza dei processi dimostra però la loro volontà di procurare il maggior danno fisico al sistema o al processo analogico comandato.

5.3.3 Attacco sperimentale di hacker a un aereo tramite il DHS

Il tema alla conferenza «CyberSat – Security in Aerospace» negli Stati Uniti erano gli attacchi informatici ai settori dei satelliti e dell'aviazione. Un rappresentante del ministero della difesa USA (DHS) ha reso noto alla CyberSat di novembre 2017 che in occasione di un esperimento eseguito nel settembre 2016 gli esperti di sicurezza del DHS sono riusciti a penetrare nel sistema computerizzato di un Boeing 757 nell'aeroporto di Atlantic City[48]. L'aereo era stato precedentemente acquistato dal DHS per scoprire eventuali vulnerabilità ai cyber-attacchi. Si tratta di un tipo di aereo utilizzato da molte linee aeree statunitensi. L'attacco è stato lanciato ai collegamenti radio dell'aereo e si è svolto da remoto senza l'aiuto di appoggi interni. La vulnerabilità sfruttata per portare a termine l'attacco è stata scoperta nel giro di due giorni dal DHS. Questo esperimento era stato effettuato in seguito a un caso verificatosi nell'aprile 2015[49], quando l'esperto di sicurezza informatica Chris Robert sostenne via Twitter, di aver scoperto falle nei sistemi di intrattenimento per passeggeri (IFE) dei modelli Boeing 757-200, Boeing 737-800, Boeing 737-900 e Airbus A-320 e di averle sfruttate per attaccare sistemi critici dell'elettronica di bordo. L'esperimento dimostra l'importanza di una netta separazione

---

46 Rapporto semestrale MELANI 2015-2, capitolo 5.3.1, https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-2.html (stato: 31.01.2018).

47 Rapporto semestrale MELANI 2016-2, capitolo 5.3.1, https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2016-2.html (stato: 31.01.2018).

48 https://www.bleepingcomputer.com/news/security/dhs-team-hacks-a-boeing-757/ (stato: 31.01.2018).

49 Rapporto semestrale MELANI 2015/1, capitolo 5.3.3, https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-1.html (stato: 31.01.2018).

fisica tra avionica (aviazione ed elettronica) e i sistemi di informazione e comunicazione raggiungibili dall'esterno, in modo che non si possa creare né sfruttare alcun collegamento tra le due reti di comunicazione, nemmeno in caso di errori di configurazione.

Conclusione / raccomandazione

La crescente computerizzazione e interconnessione di qualsiasi oggetto d'uso quotidiano (Internet delle cose) offre un gran numero di nuove e interessanti funzioni e comodità, di cui fanno parte anche l'elettronica di intrattenimento e l'accesso a internet dal veivolo. Al tempo stesso, però, non si devono trascurare i rischi connessi. Le nuove opportunità celano sempre nuovi pericoli di cui è bene tenere conto già in fase di sviluppo (security by design).

Lista di controllo delle misure di protezione dei sistemi industriali di controllo:

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, drive-by)

5.4.1 DDoS

Nel periodo in rassegna gli attacchi DDoS sono stati strumenti spesso utilizzati per diversi tipi di attacchi. Il danno causato da un attacco informatico dipende in gran parte dalla necessità di mantenere un servizio online ad ogni costo. Gli autori degli attacchi conoscono bene questa realtà e prendono di mira più sistematicamente determinati settori di attività, in particolare quelli per cui la presenza online è necessaria dal punto di vista economico. Questo è il motivo per cui nel periodo in rassegna diversi attacchi hanno colpito l'industria dei giochi e delle lotterie. Un attacco che ha particolarmente richiamato l'attenzione è stato quello sferrato alla lotteria nazionale del Regno Unito. Il 30 settembre è stato impossibile giocare online o su un dispositivo mobile per 90 minuti. Il momento dell'attacco è stato abilmente scelto, poiché la perturbazione è iniziata la domenica sera, momento d'intensa attività che precede l'estrazione. La motivazione dell'attacco è sconosciuta e, in particolare, non è stata resa pubblica alcuna richiesta di riscatto.

A seguito della pubblicità eccessiva delle criptovalute, anche le diverse piattaforme che propongono di acquistarle e cambiarle sono diventate bersagli di attacchi DDoS. Un esempio in tal senso ci è stato fornito dall'attacco che ha interessato Electroneum, una criptovaluta sviluppata per dispositivi mobili. L'incidente ha costretto l'azienda a ritardare il lancio della sua applicazione mobile.

Se, da un lato, gli autori degli attacchi DDoS sono costantemente alla ricerca di nuovi bersagli, dall'altro aggiungono nuove armi al loro arsenale. Il 2016 ha visto l'avvento di MIRAI che ha

colpito su larga scala gli oggetti connessi, non adeguatamente protetti[50] e nel 2017 è stato sviluppato un metodo chiamato *Pulse Wave*, descritto da Imperva Incapsula[51]. Contrariamente agli attacchi convenzionali, in cui la potenza aumenta progressivamente prima di raggiungere il picco, un attacco di tipo *Pulse Wave* è costituito da onde successive, ciascuna delle quali raggiunge immediatamente la massima intensità fino a 350 Gbps. A volte queste onde si susseguono per parecchi giorni. Il successo di questo tipo di attacco beneficia in parte delle peculiarità dei metodi di difesa DDoS ibrida che non fanno intervenire una soluzione basata sul cloud finché l'attacco raggiunge un determinato livello e non può più essere assorbito a livello applicativo. Gli attacchi di tipo *Pulse Wave* sono particolarmente dannosi, poiché il livello massimo di traffico viene raggiunto immediatamente. Imperva Incapsula ipotizza che in futuro questo tipo di attacchi sarà utilizzato sistematicamente.

5.4.2 Ransomware: Bad Rabbit

Alla fine di ottobre un nuovo ransomware, chiamato Bad Rabbitt, ha risvegliato le apprensioni precedentemente generate da WannaCry e NotPetya. Propagatosi mediante falsi aggiornamenti di Adobe Flash, avrebbe utilizzato l'exploit EternalRomance per infiltrarsi, come Mimikatz, nei sistemi delle aziende colpite al fine di ottenerne i dati d'accesso. Secondo il Gruppo IB il codice nocivo è una versione modificata di NotPetya[52], ma è dotato di un algoritmo di cifratura diverso. La maggior parte delle vittime di Bad Rabbit si trovano in Russia, ma alcuni casi sono stati rilevati in Ucraina, Germania e Turchia.

5.4.3 Criptovalute

L'anno scorso non solo il pubblico e i media si sono molto interessati alle criptovalute, ma anche i criminali informatici hanno mostrato un vivo interesse in merito e hanno cercato dei mezzi per approfittare dell'impennata dei prezzi. Alcuni attacchi hanno colpito anche le piattaforme. In questo modo, con l'ausilio di metodi spesso sofisticati i criminali possono rubare somme di denaro molto cospicue in una sola volta. La piattaforma di cloud mining NiceHash, ad esempio, nel mese di dicembre del 2017 ha subito un furto di oltre 70 milioni di dollari e nel mese di gennaio del 2018 è stato rubato il controvalore di oltre mezzo miliardi di dollari in NEM nella piattaforma di trading Coincheck. Sebbene i dettagli precisi di questi eventi non siano completamente chiari, essi dimostrano i rischi associati alla centralizzazione di un numero elevato di valute sulle stesse piattaforme. Tuttavia, esse non sono le uniche ad essere colpite e attacchi specifici sono sferrati anche ai singoli possessori di valute virtuali. Il New York Times[53] ha riportato la notizia di una modalità operativa particolarmente nociva che ha colpito diversi investitori in valute virtuali negli Stati Uniti. In questo caso, gli autori dell'attacco sono riusciti ad ottenere i numeri di telefono di determinati soggetti che potenzialmente disponevano di grandi quantità di valute virtuali. A tal fine, gli autori dell'attacco hanno contattato gli operatori di telefonia mobile delle loro vittime e, utilizzando tecniche di social engineering, li hanno convinti a riattribuire il numero di cellulare di cui avevano preso il controllo, dopo di che è stato

---

50 Si veda il rapporto semestrale 2016/2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (stato: 31.01.2018).

51 https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html (stato: 31.01.2018).

52 https://www.group-ib.com/blog/badrabbit (stato: 31.01.2018).

53 https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html (stato: 31.01.2018).

facile per loro accedere agli account collegati a tale numero inizializzando di nuovo la password mediante il numero di cellulare. Un altro metodo per approfittare della manna delle valute virtuali consiste nel richiedere le risorse degli utenti di Internet per comprometterne la valuta. Rientrano in questa categoria gli script che sono tornati in auge nel 2017, inseriti su siti Internet, che compromettono le valute virtuali direttamente attraverso il browser. Questa tendenza è descritta in un paragrafo nel capitolo 6.2 del presente rapporto.

5.5 Vulnerabilità

Molte gravi vulnerabilità hanno fatto scalpore nel periodo in esame. L'apice è stato raggiunto con la pubblicazione della falla «Spectre/Meltdown» in processori di diversi produttori. Questo tipo di falle, che non si possono rattoppare con un semplice aggiornamento, costringe i responsabili della sicurezza a definire nuove strategie per ridurre al minimo le conseguenze. La vulnerabilità «Spectre/Meltdown» verrà trattata in dettaglio nel prossimo rapporto semestrale.

5.5.1 Falla nello standard di cifratura WPA2 finora considerato sicuro

Nell'ottobre 2017 due ricercatori dell'Università di Leuven hanno reso pubblica una falla nello standard di cifratura WPA2. Questa falla denominata «KRACK», acronimo di «Key Reinstallation AttaCK», consente non solo l'accesso a dati cifrati, ma anche la creazione di connessioni tra due dispositivi, ad esempio tra un browser e un server. A prima vista la situazione sembra davvero molto critica. Tuttavia, per poter sfruttare questa vulnerabilità devono avverarsi alcune premesse particolari. In particolare l'hacker deve trovarsi nelle immediate vicinanze del dispositivo WLAN e poter ricevere i segnali radio. Quindi, questa falla non può essere sfruttata da Internet. Inoltre non è possibile accedere alla password WLAN o al router, ad esempio per violare direttamente il dispositivo in un momento successivo. Vengono crackate esclusivamente singole connessioni esistenti.

Questa falla non si basa su un errore di programmazione, ma su un errore di design dello stesso standard WPA2.

Valutazione

I servizi Internet sensibili in termini di sicurezza, come ad esempio il banking online, vengono già crittati nel browser, che segnala tale stato nella riga degli indirizzi con https://. La crittazione di queste connessioni non viene messa a rischio da questa falla. Colpita è la crittazione a livello superiore di connessione Wi-Fi.

Si raccomanda in ogni caso di installare al più presto gli aggiornamenti forniti dalle aziende per questa falla.

5.5.2 ROBOT – il ritorno di una falla ovvero

Il cosiddetto «attacco Bleichenbacher» è tornato al centro dell'attenzione e questo «ritorno» sorprende visto che sono già passati 20 anni da quando è stato scoperto. Da un controllo sistematico è risultato che 27 dei 100 domini più popolari sono ancora vulnerabili a questo tipo di attacco, tra cui spiccano anche Facebook e Paypal. La falla si chiama «The Return of

Bleichenbacher's Oracle Threat» (Il ritorno del caso Bleichenbachers Oracle) o in breve ROBOT.

Il crittografo svizzero Daniel Bleichenbacher aveva scoperto nel 1998 che i messaggi di errore di un server SSL rivelavano informazioni sui dati da decrittare. Tramite richieste accuratamente selezionate e ripetute si può riuscire a decrittare per fasi successive un messaggio. L'attuale standard TLS 1.2 utilizza ancora la versione PKCS #1 v1.5 RSA contenente l'errore. Affinché gli attacchi vadano comunque a vuoto, un server con un blocco di dati non correttamente formattato deve restituire, al posto dei dati criptati, dati casuali e quindi proseguire l'handshake. Per impedire possibili attacchi di timing, i dati casuali restituiti devono essere generati ancor prima della decrittazione. L'intera procedura è estremamente complessa. e quindi non sorprende che alcuni server non dispongano di un'implementazione corretta.[54]

Per riconoscere un server vulnerabile, gli attuali attacchi ROBOT sfruttano, oltre ai suddetti messaggi d'errore, anche altri tipi di messaggi come ad esempio sospensioni del collegamento TCP, Timeouts o errori di protocollo.

In totale i prodotti colpiti sono quelli di produttori diversi. Particolarmente problematici sono i dispositivi che hanno già raggiunto l'End Of Life Cycle e che di conseguenza non dispongono di nuovi aggiornamenti.

5.5.3 Vulnerabilità nel chip di sicurezza di Infineon

Nell'ottobre 2017 i ricercatori hanno scoperto una falla nella generazione della chiave RSA nei chip di sicurezza di Infineon, che permette di estrapolare la chiava privata partendo dalla chiave pubblica. La vulnerabilità sfruttata dall'attacco chiamato ROCA si annida in una libreria crittografica del chip, che viene utilizzata per generare numeri primi RSA ormai evidentemente diventati troppo deboli. Una chiave pubblica RSA è costituita da due valori numerici. Uno di questi è il prodotto di due grandi numeri primi generati casualmente e chi conosce entrambi i numeri primi può calcolare la chiave privata. Il costo per il calcolo è però notevole e ridimensiona la minaccia di questa falla, perché una chiave a 2048 bit richiederebbe 141 anni CPU. Ciononostante è possibile sfruttare questa falla con una sufficiente potenza di calcolo. I chip di Infineon interessati sono implementati in diversi prodotti, ad esempio smartcard, dispositivi mobili e notebook. Anche l'Estonia, un precursore della digitalizzazione nella vita quotidiana, o per meglio dire le carte d'identità elettroniche (eID) estoni sono state violate. Ciò ha indotto il governo a ritirare e bloccare definitivamente dai suoi sistemi tutti i 760.000 certificati colpiti.

5.5.4 Vulnerabile ancor prima del rilascio del sistema operativo.

Come ogni sistema operativo, anche MacOS è sistematicamente affetto da falle. Quando queste falle vengono divulgate da terze parti, per le aziende interessate si tratta sempre di un brutto momento. Nel presente caso il momento non avrebbe potuto essere peggiore: poco prima della pubblicazione del sistema operativo «MacOS 10.13 High Sierra» alla fine di settembre 2017 il ricercatore di sicurezza ed ex-collaboratore della NSA Patrick Wardle ha pubblicato una falla Zero-Day che è presente anche in versioni più vecchie del sistema. Questa

[54] https://www.golem.de/news/robot-angriff-19-jahre-alter-angriff-auf-tls-funktioniert-immer-noch-1712-131607-2.html (stato: 31.01.2018).

falla permette di leggere tutte le password memorizzate sul computer, nel cosiddetto Accesso Portachiavi, che contiene vari tipi di dati sensibili, come numeri di carte di credito, password di account e-mail e webshop. Disponendo del corrispondente malware, che si installa sul computer tramite un allegato e-mail o anche inserito in un'app legittima, si può sfruttare la vulnerabilità e accedere ai dati sensibili. L'errore era già stato segnalato ad Apple all'inizio di settembre 2017, che però non era ormai più in grado di fornire l'aggiornamento e High Sierra venne distribuito con la falla.[55]

Ai primi di settembre 2017 Wardle aveva già pubblicato dettagli su un ulteriore metodo che permettevano di aggirare una funzione di sicurezza di «High Sierra» senza grandi costi. La funzione interessata, «Secure Kernel Extension Loading», impedisce di caricare estensioni di kernel di terzi sviluppatori senza il consenso dell'utente.

5.6 Misure preventive

5.6.1 Un malware per training dà filo da torcere ai produttori di antivirus

Per tre anni i ricercatori di sicurezza della software house giapponese Trendmicro[56] sono ripetutamente incappati nello stesso malware, che attacca persone in posizioni influenti del settore dell'energia e dei trasporti in Corea del Sud. Gli attacchi sono stati raggruppati sotto lo pseudonimo «OnionDog». Anche altre aziende hanno incontrato questo malware, lo hanno analizzato e hanno pubblicato rapporti[57]. A un'attenta analisi si è però scoperto che «OnionDog» fa parte di un più ampio progetto di esercitazione in grande stile.

I dispositivi infettati comunicavano con un Command and Control System, ma non ne ricevevano mai i comandi. Il sistema registrava solamente l'infezione. Dagli indirizzi sottostanti si è potuto risalire al National Cyber Security Center (NCSC) sudcoreano, scoprendo così che il malware faceva parte dell'esercitazione «Ulchi Freedom Guard» organizzata dalla Corea del Sud e dagli Stati Uniti.

---

55 http://www.zdnet.de/88313439/macos-high-sierra-sicherheitsforscher-macht-zero-day-luecke-oeffentlich/?inf_by=5a91d408671db898358b4e40 (stato: 31.01.2018).

56 https://blog.trendmicro.com/trendlabs-security-intelligence/oniondog-not-targeted-attack-cyber-drill/ (stato: 31.01.2018).

57 http://zhuiri.360.cn/upload/APT-C-03-en.pdf (stato: 31.01.2018).

Raccomandazione

Ben vengano le esercitazioni in ambiente reale, ma il malware non dovrebbe valicare lo scenario dell'esercitazione. Malintenzionati potrebbero infatti acquisire nuove conoscenze e sfruttarle per futuri attacchi e nel caso peggiore si potrebbe abbassare la guardia verso attacchi di questo tipo, perché il malware sarebbe già noto dalle esercitazioni passate e verrebbe classificato come innocuo. Un altro aspetto è quello delle conclusioni affrettate in merito all'attribuzione. Le oltre 200 versioni scoperte in questo caso hanno suscitato un acceso dibattito riguardo all'origine e all'intenzione dei pirati informatici. Le attribuzioni delle colpe possono però condurre rapidamente a un'escalation indesiderata. Se il malware viene impiegato in un'esercitazione, si deve assicurare che non debordi dalla piattaforma di esercitazione o che perlomeno non funzioni al di fuori di essa.

Uno dei pilastri della sicurezza in Internet è una buona e periodica sensibilizzazione dei collaboratori, che si può ottenere anche con esercitazioni. Per garantirne il corretto svolgimento, prima dell'attuazione di un test di questo tipo è buona prassi informare perlomeno tutti i soggetti interessati dell'infrastruttura: si tratta in particolare dell'ufficio di registrazione del Top Level Domain (SWITCH per i domini .ch), registrar e hosting provider nonché eventualmente il gestore e-mail (esterno). Infine è opportuno anche un annuncio a MELANI, affinché si possa rispondere ad eventuali messaggi nell'ottica degli organizzatori della campagna Awareness e MELANI non adotti misure contro il sito web.

Formulario d'annuncio MELANI

https://www.melani.admin.ch/melani/it/home/meldeformular/formular.html

5.6.2 Cambio di registrazione di domini APT

Il gruppo «Fancy Bear» (noto anche come «APT28», «Sofacy» o «Strontium») sfrutta nomi di dominio simili a nomi di aziende o prodotti famosi per far apparire affidabili link o mittenti. Gli hacker prediligevano denominazioni che al pubblico ricordavano i prodotti Microsoft, come livemicrosoft[.]net o rsshotmail[.]com, a causa della loro ampia diffusione.

Microsoft non è riuscita a portare in tribunale i veri responsabili della campagna, ma gli avvocati del gigante del software hanno comunque convinto il giudice che, in base alle leggi sulla proprietà intellettuale, i domini dovevano essere riassegnati a Microsoft[58]. Con il cambio di registrazione le vittime non finivano più sui server controllati dagli hacker, ma su quelli controllati da Microsoft. In tal modo è stato possibile identificare le vittime e informarle affinché potessero ripulire i loro dispositivi.

58 http://www.zdnet.com/article/us-election-hack-microsoft-wins-latest-round-in-court-against-fancy-bear-phishers/ (stato: 31.01.2018).

5.6.3 Rescam-Bot – intelligenza artificiale contro le truffe

Da anni circolano truffe in cui si raccontano storie strappalacrime allo scopo di estorcere denaro alle potenziali vittime.[59] Le truffe più famose sono quelle dei principi nigeriani che promettono di ottenere l'eredità del monarca anticipando un'imposta.

L'organizzazione non-profit neozelandese Netsafe[60] stima che il danno generato da questo tipo di truffe ammonti a 12 miliardi di dollari ogni anno. Ben sapendo che è impossibile fermare l'invio di questi tentativi di truffa, Netsafe ha scelto un approccio risolutivo diverso, cercando di tenere occupati il più a lungo possibile i truffatori utilizzando chatbot[61] dotati di intelligenza artificiale. Un e-mail truffaldine possono essere inoltrate al bot all'indirizzo e-mail, che ne analizza il contenuto, generando risposte sensate e coinvolgendo gli hacker in lunghe discussioni. In questo modo, tenendo impegnato a lungo il truffatore, il chatbot gli impedisce di perpetrare altri attacchi reali. Sull'account Twitter[62] di rescam sono disponibili alcuni esempi classici di queste comunicazioni. Il dialogo che scaturisce talvolta può anche far sorridere e dimostra l'inettitudine dei truffatori quando restano imbrigliati nelle maglie delle loro stesse reti.

6 Tendenze e prospettive

6.1 Neutralità della rete

La neutralità della rete definisce il principio secondo cui tutti i dati devono essere trattati allo stesso modo durante il trasporto in Internet, indipendentemente da mittente, ricevente e destinatario, servizio, applicazione, dispositivo o contenuto. Il suo compito è quindi quello di proteggere da interventi discriminatori nel traffico dei dati. Le condotte al centro delle discussioni nell'ambito della neutralità della rete sono segnatamente il blocco, la prioritizzazione e il rallentamento di servizi nonché la differenziazione di prodotti nell'accesso a Internet. Pertanto la neutralità della rete deve garantire, ad esempio, che gli operatori di telefonia mobile non blocchino i servizi VoIP, i fornitori di accessi non privilegino la loro offerta di pacchetti IP-TV a discapito di servizi di streaming, i protocolli peer-to-peer e le trasmissioni video non vengano rallentati e i servizi di messaggistica e streaming vengano trattati allo stesso modo nell'ambito del conteggio del volume di dati consumati.

Negli Stati Uniti l'autorità di vigilanza sulle telecomunicazioni (Federal Communications Commission FCC) ha emanato il 14 dicembre 2017 un regolamento[63] con cui revoca le disposizioni rilasciate nel 2015 dalla FCC[64] sulla neutralità della rete. In concreto gli operatori Internet sono stati riclassificati a livello giuridico e non sono più servizi di telecomunicazione ed «erogatori di servizi di base» (Common Carriers), ma tornano ad essere soltanto servizi di

---

59 https://www.skppsc.ch/de/faq/was-versteht-man-unter-vorschussbetrug/#was-versteht-man-unter-vorschussbetrug (stato: 31.01.2018).

60 https://www.netsafe.org.nz/ (stato: 31.01.2018).

61 https://www.rescam.org/ (stato: 31.01.2018).

62 https://twitter.com/rescambot/ (stato: 31.01.2018).

63 Restoring Internet Freedom Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf (stato: 31.01.2018).

64 Open Internet Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf (stato: 31.01.2018).

informazione e come tali non sottostanno più alla regolamentazione e alla sorveglianza della FCC che finora vigilava sulla neutralità della rete.

Diversi Stati federali e anche il parlamento hanno intrapreso dei tentativi di procedere contro la decisione della FCC. Nell'UE la centralità della rete è stata disciplinata nel 2015 in un regolamento che sancisce le «norme comuni per garantire un trattamento equo e non discriminatorio del traffico nella fornitura di servizi di accesso a Internet».[65] Tuttavia sono state anche definite numerose eccezioni. «Servizi specializzati» come la telemedicina, ad esempio, per la quale è necessario un livello qualitativo specifico, vengono trattati in modo privilegiato, ma questo solo se il servizio specializzato non può essere utilizzato per l'accesso generale a Internet. Inoltre sono ammesse misure di gestione del traffico in cui si distinguono categorie di traffico oggettivamente diverse. Tuttavia, ogni differenziazione di questo tipo è consentita solo sulla base di requisiti oggettivamente diversi riguardanti la qualità tecnica dei servizi (ad esempio per quanto riguarda rallentamenti, variazioni del ritardo, perdita pacchetti e larghezza di banda), ma non sulla base di considerazioni di tipo commerciale. Inoltre è consentita l'esclusione di volumi di dati utilizzati per servizi selezionati da un conteggio su volumi di trasferimento mensili limitati o modalità di conteggio diverse (cosiddetto zero-rating). Agli Stati membri è concesso emettere regole più restrittive sulla neutralità della rete.

In Svizzera la neutralità della rete non è regolamentata per legge. Nel quadro dell'attuale revisione parziale della legge sulle telecomunicazioni (LTC)[66], l'Ufficio federale delle comunicazioni (UFCOM) ha fatto stilare nel 2014 un rapporto sulla neutralità della rete[67] per analizzare il fabbisogno di regolamentazione. Il disegno di legge è però limitato agli obblighi generali di comunicazione di limitazioni. In Svizzera continuerà quindi presumibilmente a mancare una neutralità della rete regolamentata per legge nel prossimo futuro, anche se vari esponenti hanno già annunciato di volerla inserire nel dibattito parlamentare in occasione della revisione della LTC.

Resta da vedere se gli operatori Internet si asterranno dal violare la neutralità della rete in base alle normative sulla trasparenza e al conseguente rischio di esposizione a critiche pubbliche. Probabilmente questa problematica in Svizzera non avrà gli stessi effetti che negli altri paesi grazie al buono standard di realizzazione dell'infrastruttura di rete e della modulazione dell'offerta degli operatori.

Negli Stati Uniti come pure nell'UE esiste un obbligo sostanziale di comunicazione trasparente di misure limitative. Spetta quindi alla società civile tenere monitorati gli sviluppi nell'ambito della neutralità della rete e intervenire all'occorrenza.

---

65 REGOLAMENTO (UE) 2015/2120, http://eur-lex.europa.eu/eli/reg/2015/2120/oj (stato: 31.01.2018).

66 Panoramica sul sito web dell'UFCOM: https://www.bakom.admin.ch/bakom/it/pagina-iniziale/l-ufcom/organizzazione/basi-legali/leggi-federali/modifica-della-ltc-2017.html; messaggio concernente la revisione della LTC: https://www.admin.ch/opc/de/federal-gazette/2017/6559.pdf; disegno di legge: https://www.admin.ch/opc/de/federal-gazette/2017/6705.pdf (stato: 31.01.2018).

67 https://www.bakom.admin.ch/bakom/it/pagina-iniziale/digitale-e-internet/internet/neutralita-della-rete.html (stato: 31.01.2018).

6.2 Parassiti informatici: quando il malware usurpa la vostra CPU

Il successo delle criptovalute offre opportunità molto allettanti ai criminali informatici. Il capitolo 5.4.3 del presente rapporto descrive, ad esempio, casi di furti di Bitcoin su larga scala. Tuttavia, i criminali hanno attaccato il mercato delle criptovalute anche in un altro modo, aggirando un processo specifico per questo tipo di valuta: il cosiddetto processo di *mining*, con il quale le transazioni in una criptovaluta vengono convalidate dai membri della rete e vengono create nuove unità monetarie. Questo processo richiede la risoluzione di complessi calcoli matematici che necessitano di notevoli capacità computazionali e viene compensato con una determinata somma di valuta «estratta», proporzionale al lavoro di calcolo svolto. Alla fine il *mining* contribuisce a creare valuta.

Poiché questo processo produce valuta, alcuni attori da qualche tempo hanno già cercato di aggirarlo (questo tipo di casi è già stato menzionato nel nostro rapporto semestrale 2013/2[68]). Nel frattempo si sono moltiplicati gli attacchi volti a sfruttare la potenza di calcolo dei computer a scopo di *mining*. Nel 2017 si sono verificati numerosi casi, al punto che alcuni si sono chiesti se ormai non si trattasse del modello di guadagno più proficuo per i criminali informatici. Inoltre, in alcuni codici malevoli si è optato per far eseguire del *mining,* sebbene fossero disponibili altre metodi di compromissione altrettanto redditizi, come la crittografia dei dati. Si pensi, ad esempio, a Wannamine, un malware sofisticato che si propaga mediante l'exploit EternalBlue, che è già stato utilizzato dal ransomware WannaCry e NotPetya. Tuttavia, contrariamente a questi ultimi, i criminali informatici hanno scelto di parametrizzare il loro strumento, poiché una volta installato, esso genera valuta virtuale anziché crittografare i dati dell'utente.

L'installazione di un software nocivo non è l'unica opzione possibile per utilizzare un computer all'insaputa del suo possessore per generare criptovaluta. Infatti, alcuni siti contengono degli script mirati a generarla mediante i browser. Se alcuni siti richiedono l'autorizzazione dell'utente che, acconsentendo, mette consapevolmente a disposizione il proprio computer per contribuire al finanziamento di un sito Internet, altri siti non si preoccupano di prendere questa precauzione. Infine, in parecchi casi i siti sono stati compromessi per introdurvi tali script a vantaggio dei criminali informatici.

Se il fatto di sfruttare le risorse di un computer può sembrare più innocuo di altri tipi di attacchi, ad esempio di un ransomware che cripta i dati, non si deve sottovalutare il danno potenziale di tali attacchi. Innanzitutto, il prezzo da pagare per il *mining* inaspettato è quello dell'elettricità consumata dalle risorse depredate. Inoltre, se le risorse informatiche che devono essere a disposizione dei processi vengono depredate da un software malevolo, non si possono escludere problemi di stabilità o di avaria, ancor più preoccupanti se interessano sistemi critici. Anche l'eliminazione del software malevolo può causare interruzioni di servizio.

Data l'evoluzione di questo tipo di attacchi, attualmente essi sembrano offrire un rapporto costi-benefici molto interessante. Per i criminali informatici, questi metodi devono essere applicati su larga scala per risultare economicamente vantaggiosi, in quanto le capacità di calcolo di un

[68] Si veda il rapporto semestrale 2013/2 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2013-2.html (stato: 31.01.2018).

numero ridotto di computer non sono sufficienti. Per contro, offrono il vantaggio di produrre redditi regolari. Non è necessario che la vittima scelga di pagare dopo che sono stati crittografati i suoi dati o che avvii una sessione di e-banking che si cercherà di aggirare: un computer infetto inizierà automaticamente a generare denaro. Alla fine si tratta del passaggio più diretto dalla compromissione di un computer alla generazione di reddito. Inoltre, questo tipo di raggiro offre il vantaggio di essere difficilmente individuabile. Lo scopo è, pertanto, disporre di un grande numero di computer ciascuno dei quali, discretamente, con regolarità e un'interruzione minima, apporti una piccola somma di denaro. La preoccupazione maggiore potrebbe essere la seguente: cosa accadrà a questi computer compromessi il giorno in cui l'andamento del mercato renderà questa attività meno attrattiva sotto il profilo finanziario? Sussiste il rischio che essi vengano utilizzati con modalità operative probabilmente più distruttive. Sarebbe pertanto ingenuo considerare il *mining* abusivo, a seguito dell'installazione di un software malevolo, come una semplice intrusione innocua.

6.3 Outsourcing? Ma sicuro!

In un mondo globalizzato e specializzato praticamente nessuna azienda può più permettersi di gestire internamente tutta la propria attività. Per essere competitivi è necessario che i processi siano impostati con la massima efficienza possibile e che i costi restino contenuti. L'esternalizzazione di determinati servizi (outsourcing) può contribuire all'ottimizzazione, ma è importante che il criterio decisivo nella scelta del partner esterno sia la sicurezza. Gli offerenti più convenienti non devono essere necessariamente quelli più sicuri, perché se è vero che si può esternalizzare un servizio, non è così per la responsabilità e il rischio. Nell'esternalizzazione di servizi, ogni azienda deve sempre tenere presente i dati che intende affidare all'esterno e le possibili conseguenze per l'azienda qualora venissero manomessi. I dati, la cui perdita rappresenterebbe una minaccia esistenziale per l'azienda, non devono finire in mani estranee.

E questo il primo ministro svedese Stefan Löfven lo ha capito sulla propria pelle. Nel luglio 2017 ha dovuto ammettere davanti alla stampa la possibilità di un accesso non autorizzato ai dati dell'esercito svedese, dell'autorità di rilascio dei permessi di guida e addirittura del programma di protezione dei testimoni. L'autorità che gestisce i dati aveva esternalizzato la gestione informatica al gruppo IBM, che a sua volta aveva ingaggiato dei subappaltatori nella Repubblica ceca e in Romania. Sebbene tutti i file fossero archiviati in Svezia, i tecnici dei due subappaltatori vi potevano accedere senza verifiche di sicurezza. L'autorità ha sottolineato che nulla lascia sospettare un abuso dei dati.

Raccomandazione

Per proteggersi da queste sorprese indesiderate, durante la fase preliminare dei progetti di questo tipo vanno definiti precisi requisiti, sviluppando un concetto di sicurezza IT per i reparti esternalizzati. A tal fine va chiarito esattamente quali rischi comporta l'esternalizzazione dei dati e quali misure devono essere adottate per ridurre al minimo tali rischi. È importante gestire un risk management onesto, senza sottovalutare i rischi e senza farsi accecare dal risparmio di costi.

Le misure adottabili possono essere, ad esempio, una definizione chiara dei diritti di accesso, il coinvolgimento esclusivo di persone autorizzate sia nel processo di installazione che in quello di manutenzione e la crittazione dei dati durante il trasporto e l'archiviazione. Oltre a un salvataggio regolare dei dati, tra i requisiti figurano anche controlli fisici sicuri degli accessi. Le aziende non devono semplicemente affidarsi alle promesse dei fornitori di servizi, ma devono pretenderne l'attuazione (ad esempio sotto forma di certificati di sicurezza) verificandoli periodicamente. Vanno definite anche le misure per il caso in cui si verifichi un imprevisto nonostante tutti i provvedimenti adottati.

Conclusione

La complessità della gestione dei rischi è destinata ad aumentare nei prossimi anni proprio nell'ambito dei servizi esternalizzati. Eclatanti in tal senso sono le falle hardware «Spectre» e «Meltdown» salite alla ribalta delle cronache a cavallo tra i due millenni. Anche l'hardware può contenere vulnerabilità e nessun elemento di un sistema informatico può essere considerato sicuro al 100%. Una politica di sicurezza deve comprendere pertanto diverse attività (organizzative e tecniche), per contenere al massimo il rischio in presenza di vulnerabilità in una componente. Le due falle citate hanno colpito in particolare gli ambienti virtuali e quindi i servizi esternalizzati. Le imprese che elaborano i dati in centri di calcolo di terzi devono pertanto assicurarsi che i loro gestori abbiano adottato tutte le misure necessarie per ridurre al minimo i rischi insiti nelle varie falle. Per casi come questi si possono stabilire per contratto le garanzie sulle misure adottate.

7 Politica, ricerca, policy

7.1 Svizzera: interventi parlamentari

Affare	Numero	Titolo	Depositato da	Data di deposito	Consiglio	Uffucui	Stato e link
Ip	17.4285	Definire ruoli chiari per gli attori della cyberdifesa e della cybersicurezza in Svizzera	Fathi Derder	15.12.2017	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174285
Ip	17.4100	Digitalizzazione della politica estera e di sicurezza. Quali sono i rischi e le opportunità per la Svizzera?	Damian Müller	13.12.201	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174100
Ip	17.4004	Urge una visione d'insieme. Forse anche un coordinamento?	Sylvia Flückiger-Bäni	30.11.201	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174004

Ip	17.3905	Legge sui cyber-rischi	Sibel Arslan	29.09.2017	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173905
Po	17.3875	Rafforzare la ricerca scientifica in seno all'esercito e intensificare le collaborazioni con gli istituti di ricerca	Fathi Derder	29.09.2017	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173875
Mo	17.3849	Esercito svizzero. Come garantire la nostra sovranità e la nostra indipendenza quando il digitale spinge verso l'interdipendenza?	Claude Béglé	28.09.2017	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173849
Ip	17.3731	Cybersicurezza per tutti invece che cyberguerra solo per il DDPS	Edith Graf-Litscher	27.09.2017	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173731
Ip	17.4296	Imposizione equa dei colossi del web. Introdurre un'imposta compensativa sulle cifre d'affari conseguite online	Balthasar Glättli	15.12.2017	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174296
Ip	17.4090	Misure contro tendenze discriminatorie	Nadine Masshardt	13.12.2017	CN	DFI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174090
Ip	17.3864	Offerte illegali su Internet. Ridurre i danni e i rischi	Raphaël Comte	28.09.2017	CS	DFGP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173864
Ip	17.4314	Che ruolo ha giocato la Posta nell'entrata di Amazon sul mercato svizzero?	Regula Rytz	15.12.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174314
Po	17.4249	Trasformare le regioni di montagna in un polo per i dati e la digitalizzazione	Martin Candinas	15.12.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174249
Po	17.4041	Meno incidenti stradali grazie all'assistente di guida? Più dati sui sistemi di guida assistita e il loro impatto sulla sicurezza	Jürg Grossen / Grünliberale Fraktion	07.12.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174041
Dom	17.5619	I social media devono essere assoggettati alla Legge sulla radiotelevisione?	Edith Graf-Litscher	06.12.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175619
Dom	17.5614	Basta una base giuridica per contrastare la diffusione di fake news tramite i social media?	Edith Graf-Litscher	06.12.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175614
Dom	17.5592	Cyber defence. Competenze per la comunicazione strategica e la conduzione di operazioni di informazione	Priska Seiler Graf	05.12.2017	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175592
Ip	17.3896	Come creare una piattaforma digitale multimodale di trasporti pubblici?	Claude Béglé	29.09.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173896
Ip	17.3870	Potenziamento della rete mobile	Susanne Leutenegger Oberholzer	29.09.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173870

Mo	17.3847	Internet delle cose. Creare le condizioni quadro per un ecosistema nazionale e internazionale	Claude Béglé	28.09.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173847
Ip	17.3733	Droni civili. Possiamo ignorare i pericoli?	Manuel Tornare	27.09.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173733
Ip	17.3734	Permettere i discorsi d'odio sulle reti sociali?	Manuel Tornare	27.09.2017	CN	DFGP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173734
Ip	17.3723	Rete mobile Swisscom. Come interpretare le cifre e la cartografia relative al tasso di copertura nazionale?	Jacques Nicolet	25.09.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173723
Dom	17.5397	Assicurare il vantaggio della piazza Svizzera con una potente rete mobile 5G	Karl Vogler	13.09.2017	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175397
Po	17.4017	Sfruttare le opportunità offerte dalla tecnologia civica	Damian Müller	04.12.2017	CS	CaF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174017
Po	17.4295	Standard di sicurezza per i dispositivi connessi a Internet, che costituiscono una delle maggiori minacce per la cyber-sicurezza	Balthasar Glättli	15.12.2017	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174295
Po	17.4273	Regtech. Favorirne la diffusione presso gli attori economici e le autorità pubbliche	Claude Béglé	15.12.2017	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174273
Ip	17.4062	Ottimizzare il servizio di convalida validatore.ch	Marcel Dobler	12.12.2017	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174062
Ip	17.3854	Una seconda occasione per l'imposta digitale	Géraldine Savary	28.09.2017	CS	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173854
Ip	17.3717	Conseguenze e sfide della trasformazione digitale per l'Ufficio federale della cultura	Kathy Riklin	25.09.2017	CN	DFI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173717
Dom	17.5415	Criptovalute. Produzione, utilizzo, controllo statale, potenziale di danno	Maximilian Reimann	18.09.2017	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175415

7.2 L'appello della «Global Commission on the Stability of Cyberspace» per la protezione della parte pubblica di internet

La «Global Commission on the Stability of Cyberspace (GCSC)» è stata fondata nel febbraio 2017 alla conferenza sulla sicurezza di Monaco e riunisce rappresentanti di spicco del governo, di imprese e di associazioni tecniche e civili provenienti da differenti regioni geografiche. La sua missione è il promuovimento della pace, della sicurezza e della stabilità in ambito internazionale, proponendo norme e iniziative per un comportamento responsabile degli attori statali e non nello spazio cyber.

In novembre 2017 i rapresentanti della GCSC hanno dato vita a una «Call to Protect the Public Core of the Internet», in cui tutti i partecipanti vengono esortati a osservare la norma seguente, che dovrebbe assicurare la disponibilità e l'integrità fondamentali di internet:

> Non-Interference with the public core
>
> Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

Secondo la commissione le parti del «nucleo pubblico» di internet comprendono tra l'altro l'Internet Routing, il Domain Name System, certificati e confidenzialità e la comunicazione tramite cavo.

> Conclusione
>
> Le società moderne dipendono sempre maggiormente da tecnologie di comunicazione collegate a internet e diventano a vista d'occhio più condizionate dalla stabilità e previdibilità di quest'ultime. Per quanto rigurada lo spazio cyber globalmente interconnesso, le misure che concernono il "nucleo pubblico" di internet possono causare ripercussioni su scala mondiale e conseguenze involontarie come danni collaterali, che sono molto difficili da prevedere. È perciò nell'interesse di tutti quelli che hanno a cuore il bene comune, evitare tutte le attività che possano mettere in pericolo il funzionamento generale di internet e contemporaneamente collaborare all'impedimento o all'attenuazione delle suddette attività.

8 Prodotti MELANI pubblicati

8.1 Blog GovCERT.ch

8.1.1 The Retefe Saga

03.08.2017 – Sorprendentemente, l'attenzione dei media al momento è focalizzata su OSX/Dok, un malware che attacca il sistema operativo macOS. Nelle ultime settimane diversi fornitori di antivirus e ricercatori in materia di sicurezza informatica hanno pubblicato dei post nei loro blog su questa minaccia e hanno riportato le loro analisi e scoperte in merito. Mentre alcune di queste scoperte erano molto interessanti, altre sono risultate fuorvianti o semplicemente errate.

➔ https://www.govcert.admin.ch/blog/33/the-retefe-saga

8.1.2 Leaked Accounts

29.08.2017 – MELANI/GovCERT è stata informata in merito ad account potenzialmente trafugati che potrebbero essere utilizzati per fini illeciti. MELANI/GovCERT fornisce uno strumento per verificare se il vostro account potrebbe essere stato trafugato, disponibile sul sito: https://checktool.ch

➔ https://www.govcert.admin.ch/blog/34/leaked-accounts

8.2 Newsletter di MELANI

8.2.1 E-Banking: i criminali prendono di mira le lettere d'attivazione

17.08.2017 – Alla fine del 2016 MELANI ha segnalato, tramite un bollettino d'informazione, l'aumento di criminali che prendono di mira i metodi d'autenticazione per accedere all'e-banking tramite dispositivi mobili. Ora i truffatori fanno un passo avanti e tentano di persuadere le vittime ad inviare loro una copia della lettera, ricevuta dalla banca, che contiene i dati d'attivazione per l'autenticazione a due fattori dell'e-banking.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html

8.2.2 21'000 dati d'accesso di servizi online rubati

29.08.2017 - La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha ricevuto circa 21'000 dati d'accesso, costituiti da login e password, che sono stati violati e che attualmente potrebbero venir utilizzati a fini illegittimi.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/passwoerter-von-21000-e-mail-konten-im-umlauf.html

8.2.3 In aumento i trojan di crittografia e le e-mail fasulle a nome delle autorità

02.11.2017 - Il 25° rapporto semestrale della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), pubblicato il 2 novembre 2017, è dedicato agli incidenti informatici più eclatanti avvenuti in Svizzera e all'estero nel primo semestre del 2017. Il rapporto si concentra sui trojan di crittografia WannaCry e NotPetya, che nella primavera del 2017 sono saliti alla ribalta delle cronache mondiali.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/rapporto-semestrale-1-2017.html

8.2.4 70'000 dati d'accesso di servizi online rubati

05.12.2017 - La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha di nuovo ricevuto una lista con dati d'accesso, costituiti da login e password, che sono stati violati e che attualmente potrebbero venir utilizzati a fini illegittimi. Questa volta i dati d'accesso rubato sono 70'000.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/passwoerter-von-70000-e-mail-konten-im-umlauf.html

8.3 Liste di controllo e guide

Nel secondo semestre MELANI non ha pubblicato né nuove liste di controllo né nuove guide.

9 Glossario

Termine	Descrizione
Advanced Persistent Threats (APT)	Questa minaccia provoca un danno ingente, che si ripercuote sulla singola organizzazione o su un Paese. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di notevoli risorse.
App	Il concetto di app (dall'abbreviazione inglese di Application) designa in generale ogni forma di programmi di applicazione. Nell'uso linguistico si fa nel frattempo perlopiù riferimento alle applicazioni per i moderni smartphone e tablet computer.
Attacchi Supply Chain	Attacco con cui si cerca di infettare l'obiettivo vero infettando un'azienda nella catena di fornitura.
Attacchi Watering Hole	Infezione mirata per mezzo di software maligno tramite siti che di preferenza vengono visitati solamente da un gruppo specifico di utenti.
Attacco DDoS	Attacco di Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Autentificazione a due fattori	A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. password, PIN ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.)
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezione di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.
Backup	Backup (in italiano: salvaguardia dei dati) designa la copia di dati nell'intento di poterli ricopiare in caso di perdita.
Bitcoin	Sistema di pagamento decentrato che può essere utilizzato in tutto il mondo e nome di un'unità di moneta digitale.

Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
Browser	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e Safari.
Browser / Navigatore	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e Safari.
Brute Force	Metodo di risoluzione di problemi nei settori dell'informatica, della crittologia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili.
Certificato	Un certificato digitale è per così dire l'equivalente di un documento d'identità nel cyberspazio e serve per assegnare una determinata chiave pubblica a una persona o un'organizzazione. Questa assegnazione viene certificata dall'ente certificante che appone la propria firma digitale.
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
Crittazione RSA	Acronimo della crittazione Rivest-Shamir-Adleman. Procedura di crittazione con chiavi pubbliche introdotta nel 1978. RSA è una procedura asimmetrica.
Defacement	Deturpamento di pagine web.
Domain Name System	Domain Name System. Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
Ethernet	Ethernet è una tecnologia utilizzata per le reti di dati collegate via cavo.
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.

Funzione hash	Una funzione hash è una rappresentazione che mappa una grande quantità di dati (la chiave) in una quantità target più piccola (i valori hash).
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 delle cose	L'espressione «Internet delle cose» indica che nel mondo digitale il computer è integrato in misura crescente da «oggetti intelligenti», ossia dall'applicazione dell'intelligenza digitale agli oggetti reali.
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. Né 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.
Macro-malware	Malware installato tramite macro. Una macro è costituita da una sequenza di istruzioni che possono essere eseguite con un semplice richiamo.
Malware	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, nonché le Logic Bombs.
Managed Service Provider (MSP)	Fornitore di servizi nell'ambito della tecnologia dell'informazione che si assume la responsabilità di predisporre un insieme definito di servizi per i suoi clienti e li amministra.

mobileTAN	mobileTAN (mTAN, Mobile Transaction Number) è la procedura che include il canale di trasmissione SMS. Dopo l'invio di un ordine di bonifico compilato, il cliente dell'online banking riceve dalla banca per SMS, sul proprio cellulare, un TAN unico da utilizzare esclusivamente per la transazione in questione.
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato.
Plug-Ins	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.
Port	Una porta è la parte di un indirizzo che assegna segmenti di dati a un protocollo di rete. Questo concetto è utilizzato ad esempio in TCP, UDP e SCTP per indirizzare i protocolli ai livelli superiori del modello OSI.
Protocollo SMB	Server Message Block (SMB): protocollo per la condivisione in rete di file, stampanti e server in reti di computer.
Proxy	Interfaccia di comunicazione in una rete che funge da intermediario che riceve le richieste da un lato per poi effettuare il collegamento dall'altro lato con il proprio indirizzo.
RAM	Random access memory: memoria di dati utilizzata soprattutto nei computer come memoria di lavoro, in prevalenza sotto forma di moduli di memoria.
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.

Remote Administration Tool	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
RootKit	Un insieme di programmi e di tecniche che consentono di accedere inosservatamente a un elaboratore e di assumerne il controllo.
Router	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Salt	In crittografia, salt definisce una successione casuale di caratteri che vengono aggiunti a un testo in chiaro prima dell'utilizzo come dato di una funzione hash per aumentare l'entropia del dato.
Script PowerShell	PowerShell è un framework multipiattaforma di Microsoft che consente di automatizzare, configurare e gestire sistemi ed è composto da un interprete a riga di comando (shell) e da un linguaggio di scripting.
Servizi di e-currency	Valore monetario sotto forma di credito nei confronti dell'ente emittente, salvato su un supporto dati e rilasciato dietro riscossione di una somma di denaro, il cui valore non è inferiore al valore monetario emesso e che viene accettato come mezzo di pagamento da aziende diverse dall'ente emittente.
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.
Smartphone	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
SMS	Short Message Service Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
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.
Spearphishing mail	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L'aggressore tenta di introdurre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
SS7	Il Signaling System #7 (SS7) è un insieme di protocolli e procedure di segnalazione usati per le reti di telecomunicazione. SS7 è utilizzato nella rete telefonica pubblica in correlazione con l'ISDN, la rete fissa e la rete mobile, e all'incirca dal 2000 impiegato in misura crescente anche nelle reti VoIP.
SSH	Secure Shell Protocollo che grazie alla cifratura dei dati consente tra l'altro l'accesso sicuro (Login) a un sistema di computer accessibile per il tramite di una rete pubblica (ad es. Internet).
Take down	Take down (rimozione) è un'espressione utilizzata quando un provider ritira un sito dalla rete a causa della presenza di contenuti fraudolenti.
Troll	Troll nel gergo della rete è una persona la cui comunicazione in Internet è limitata a contributi che mirano alla provocare emotivamente altri partecipanti alla discussione.
USB	Universal Serial Bus, Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo).
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.

Zero-Day	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
ZIP-Datei	Zip è un algoritmo e un formato di file per la compressione dei file, destinato a ridurre lo spazio di memorizzazione dei file per l'archiviazione e la trasmissione.