Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

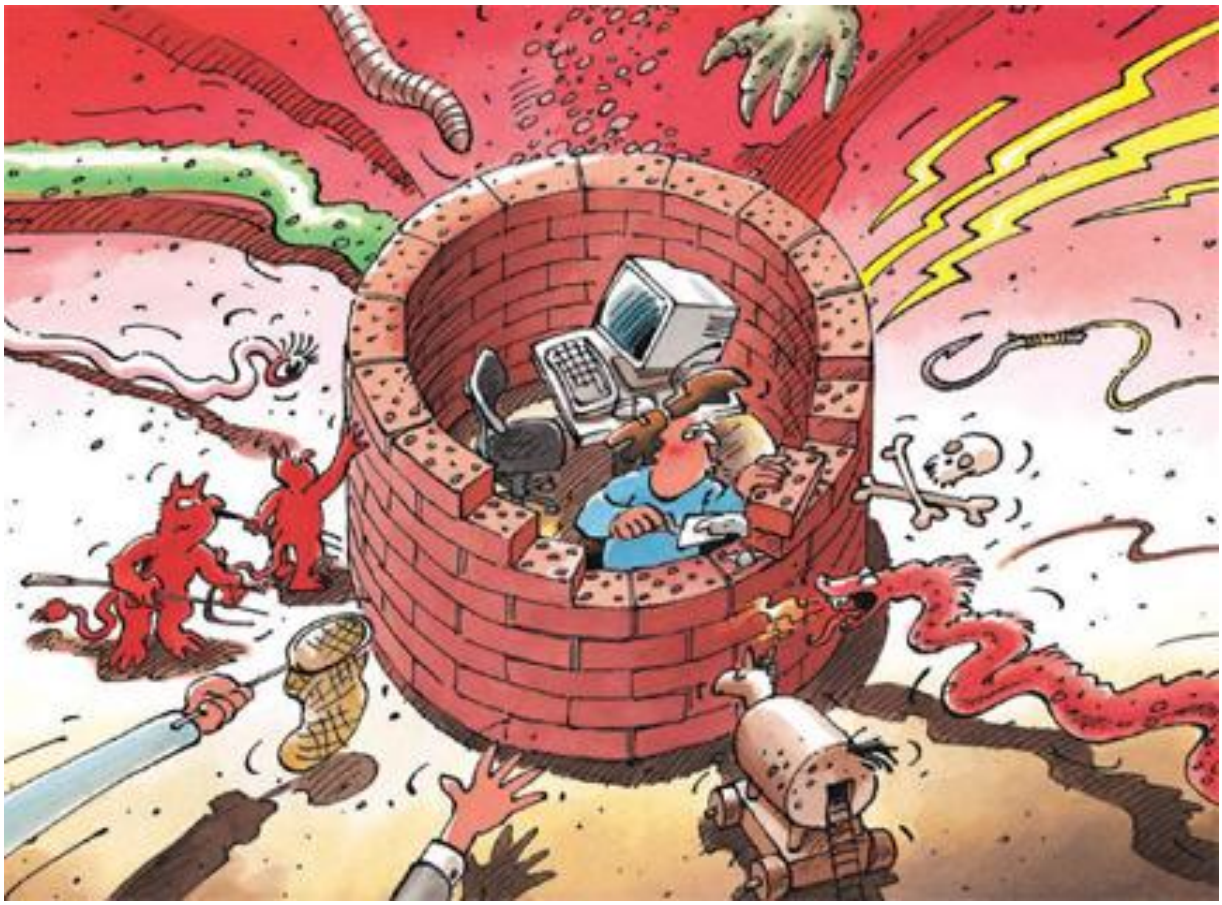
Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

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

Sicurezza dell'informazione

La situazione in Svizzera e a livello internazionale

Rapporto semestrale 2013/II (luglio – dicembre)



Indice

1 Cardini dell'edizione 2013/II

- **Ulteriori rivelazioni sulla NSA e il GCHQ**
  Anche nel secondo semestre del 2013 la pubblicazione delle diverse attività della National Security Agency statunitense (NSA) e del General Communication Headquarter britannico (GCHQ) sulla base dei documenti di Edward Snowden ha costituito un vasto tema. Nel corso del secondo semestre si è consolidata l'immagine di un rilevamento generalizzato e integrale dei dati da parte di questi due servizi segreti. Le conoscenze acquisite mettono in luce i problemi che comporta un'istituzione transnazionale come Internet al quale ogni individuo e ogni Stato può partecipare, procedendo come preferisce e come le leggi nazionali lo consentono, senza dovere preoccuparsi delle ripercussioni globali.

  ► Situazione attuale a livello internazionale: capitolo 4.1
  ► Tendenze / Prospettive: capitolo 5.1

- **Bitcoin: successo e prezzo del successo**
  Bitcoin è una moneta elettronica decentralizzata, ciò che significa che il suo funzionamento non dipende da nessun emittente centrale. Questo aspetto la differenzia dalle divise tradizionali, ma anche da numerose altre monete elettroniche centralizzate. La popolarità crescente del Bitcoin solleva numerose problematiche, in particolare a livello di sicurezza, ma anche per quanto riguarda lo statuto legale e la regolamentazione di queste divise.

  ► Tendenze / Prospettive: capitolo 5.2

- **Ransomware in avanzata**
  In ambito di ransomware (in italiano software nocivo per estorsioni) sono diffusi i cavalli di Troia di bloccaggio che visualizzano sui computer infettati una comunicazione proveniente apparentemente da un'autorità di polizia. Molto più grave, è l'infezione con il software nocivo Cryptolocker, osservato per la prima volta in Svizzera nel novembre 2013. Nel caso di questo software nocivo tutti i dati che si trovano sul disco rigido e su altri supporti di dati collegati sono irrimediabilmente criptati e quindi inutilizzabili.

  ► Situazione attuale in Svizzera: capitolo 3.1

- **Vasti furti di dati**
  Sono stati nuovamente resi noti furti di dati riguardanti milioni di serie di dati. Nel caso di Adobe si tratta di 38 milioni di dati dei clienti, di password e di dati di carte di credito. La catena di empori Target è stata anch'essa colpita da un furto di dati. Le informazioni pubblicate fanno stato del furto di dettagli riguardanti 40 milioni di carte di credito e di debito, come pure di dati personali concernenti 70 milioni di clienti.

  ► Situazione attuale a livello internazionale: capitolo 4.3, capitolo 4.4

- **Sistemi industriali e domestici di controllo – Sempre più sistemi su Internet**
  Nel frattempo è divenuto relativamente semplice e buon mercato procurarsi sistemi con funzioni di interrogazione a distanza e di pilotaggio oppure di potenziare l'installazione esistente con un'interfaccia di comunicazione. A prescindere dalle funzioni e dalla convivialità di una soluzione di accesso remoto occorre prestare un'attenzione corrispondente alla protezione contro le manipolazioni non autorizzate. Al riguardo MELANI ha pubblicato nell'ottobre del 2013 un elenco di controllo per la protezione dei sistemi industriali di controllo.

  ► Situazione attuale a livello internazionale: capitolo 4.7

2 Introduzione

Il diciottesimo rapporto semestrale (luglio – dicembre 2013) della Centrale d’annuncio e d’analisi per la sicurezza dell’informazione (MELANI) espone le principali tendenze nel campo dei pericoli e dei rischi che accompagnano le tecnologie dell’informazione e della comunicazione (TIC). Presenta un compendio degli avvenimenti in Svizzera e all’estero, illustra i principali sviluppi in ambito di prevenzione ed espone in sintesi le principali attività degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (termini *in corsivo*) sono riunite in un **glossario** alla fine del presente rapporto **(capitolo 6)**. Le valutazioni di MELANI sono di volta in volta evidenziate in un riquadro.

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

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti della seconda metà del 2013. Il capitolo 3 tratta i temi nazionali e il capitolo 4 i temi internazionali.

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

Il **capitolo 5** contiene per la prima volta una scelta di interventi parlamentari con riferimento alle tematiche della sicurezza dell’informazione.

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Estorsione mediante Cryptolocker & Co

Il *ransomware*, il software nocivo a scopo di estorsione destinato a estorcere i proprietari dei computer infettati, esiste già da parecchio tempo. Sono molto diffusi i cavalli di Troia che visualizzano sui computer infettati una comunicazione proveniente apparentemente da un'autorità di polizia, come il Bundeskriminalamt germanico o il Dipartimento federale di giustizia e polizia (DFGP). La comunicazione in questione esige il pagamento di una multa adducendo il pretesto di avere rilevato file illegali sul computer infettato. In caso di mancato pagamento il computer viene, rispettivamente rimane bloccato. Rispetto agli altri ransomware questo genere di software nocivo è relativamente innocuo perché non procura danni veri e propri al computer e il bloccaggio può essere eliminato con mezzi relativamente semplici.

Nella maggior parte dei casi il parassita può essere eliminato analizzando il computer con un *CD Antivirus Live* corrispondente allo stato più recente. Una guida di allestimento e di utilizzazione di un CD AntiVirus Live è disponibile sul sito del Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI)[1].

È invece molto più grave l'infezione con il software nocivo Cryptolocker, osservato per la prima volta in Svizzera nel novembre 2013. Nel caso di questo software nocivo tutti i dati che si trovano sul disco rigido e su altri supporti di dati collegati sono irrimediabilmente criptati e quindi inutilizzabili. Si ritiene invero che la diffusione in Svizzera sia relativamente bassa. Ma le storie personali dietro a ogni singolo caso sono drammatiche: le persone private perdono il loro intero passato digitale. Nel caso delle PMI sono sovente colpiti importanti dati aziendali, circostanza che può giungere a minacciarne l'esistenza se non è stato effettuato un *backup* corrispondente o se il backup risulta difettoso.

Sembra che Cryptolocker si propaghi attraverso allegati infettati alle e-mail e siti Web appositamente predisposti, le cosiddette infezioni di siti Web o i *download drive-by*. In alcuni casi l'apparecchiatura interessata era già stata colpita da un altro malware che carica successivamente Cryptolocker. Esistono già imitatori che hanno sviluppato software nocivo analogo e lo mettono in circolazione.

Ad avvenuta infezione alla vittima viene inoltrata una comunicazione mediante la quale i criminali formulano una pretesa pecuniaria. In controparte la vittima dovrebbe ricevere la chiave per poter ripristinare i dati. Diversi prodotti antivirus possono invero individuare ed eliminare il software nocivo. Nella maggior parte dei casi tuttavia è troppo tardi perché i dati situati sul computer sono già stati criptati. Il vero problema non è pertanto l'eliminazione del software nocivo, bensì il ripristino dei dati originali. Nel caso dei ransomware attuali con cifratura dei dati integrata, la chiave è stata programmata in maniera fissa al loro interno e può quindi essere estratta in maniera corrispondentemente semplice dal codice sorgente. Ciò non è più possibile con Cryptolocker: per ogni vittima viene generata una chiave propria su un server di comando e controllo (command and control server).
Sembra pertanto che al momento non esista alcun metodo di decriptare i dati senza la chiave nota al solo truffatore. MELANI sconsiglia tuttavia di cedere alle pretese dei criminali e di

[1] Guida del Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) per l'allestimento di un CD Antivirus Live: http://www.cybercrime.admin.ch/content/kobik/de/home/dokumentation/informationen/2012-07-06.html

effettuare un pagamento. Non è infatti per niente garantito che i criminali inviino effettivamente alla vittima la chiave necessaria per decriptare i dati e non è escluso che gli estorsori sfruttino la disponibilità manifesta di pagamento della vittima per presentare altre pretese.

MELANI ha già adottato unitamente ai provider svizzeri di servizi Internet (ISP) misure per minimizzare le minacce provenienti da Cryptolocker.

Cryptolocker evidenzia chiaramente quanto sia importante eseguire backup regolari e garantirne la qualità.

Nel caso di Cryptolocker l'aggravante è costituita dal fatto che anche i dischi rigidi esterni collegati al computer sono colpiti dalla cifratura. Si è rivelato particolarmente tragico il caso dell'attacco di Cryptolocker durante una procedura di backup, nel senso che sono andati simultaneamente criptati e quindi resi inutilizzabili i dati originali e i dati di backup. Si raccomanda pertanto di utilizzare due dischi rigidi e di collegare i supporti di dati del backup soltanto durante il processo di backup.

Allo stato attuale i *dischi di rete* non sono colpiti dalla cifratura a condizione che non siano stati assegnati a una *lettera di disco*. Il software nocivo verrà sicuramente ulteriormente sviluppato, ragione per la quale è possibile che in futuro esso comprenda questa e altre funzioni.

3.2 I banner pubblicitari distribuiscono software nocivo

Gli *AdServer* servono a visualizzare pubblicità sui siti Web. La pubblicità può provenire da diversi servizi pubblicitari e reti pubblicitarie. AdServer noti e sovente utilizzati sono per esempio OpenX e il Revive Adserver basato su di esso. Gli AdServer costituiscono un bersaglio molto interessante per i criminali perché il codice nocivo può essere diffuso in maniera semplice sotto forma di pubblicità manipolata per il tramite di numerosi siti Web, in parte molto frequentati. Una tattica corrente consiste nel collocare *Iframes* in aggiunta ai banner pubblicitari. L'Iframe è un'istruzione *HTML* utilizzata per collegare contenuti estranei – ad esempio il rinvio a un sito contenente software nocivo.

Qui l'aggravante è costituita dal fatto che nel corso dell'ultimo semestre sono state individuate a più riprese lacune di sicurezza riguardanti OpenX. Questa circostanza, unita al fatto che numerosi amministratori non effettuano tempestivamente gli aggiornamenti, provoca un rischio notevole per la sicurezza:

In questo senso nel luglio del 2013 è stata individuata nell'OpenX degli AdServer una lacuna di sicurezza che consente agli aggressori di infiltrarvi qualsiasi *Scriptcode* o HTML (*Cross Site Scripting*). Nell'agosto del 2013 è stato reso noto che la versione libera di OpenX comportava da parecchio tempo una *backdoor*. Tutti gli utenti che avevano utilizzato questa versione hanno installato automaticamente anche questa backdoor che gli aggressori inseriscono per i loro scopi nel software e utilizzano anche attivamente. Nel mese di settembre è stata resa nota un'ulteriore lacuna in OpenX e in Revive, lacuna grazie alla quale gli utenti registrati possono eseguire qualsiasi codice *PHP* sul server. Nel mese di dicembre infine è stata resa nota una lacuna molto grave riguardante sia OpenX che Revive. Questa lacuna schiudeva la possibilità di accedere direttamente alla banca dati del server (*SQL Injection)* e di manipolare i dati dell'AdServer senza disporre di alcun dato di accesso.

In Svizzera sono stati colpiti da eventi diversi siti Web, in parte molto utilizzati. MELANI raccomanda generalmente di eseguire patch regolari del software esposto su Internet e di attenersi a un *Life Cycle Management*. Occorre inoltre verificare regolarmente i logfile e indagare le anomalie. Le misure di protezione dei *Content Management Systems*[2] possono essere applicate per analogia anche agli AdServer. Nel caso di OpenX e Revive è peraltro messo a disposizione un elenco di controllo[3] che indica i principali compiti da effettuare regolarmente.

3.3 Compromissione a ripetizione di siti Web

Le *pagine di phishing* costituiscono un problema persistente. Se in passato i truffatori creavano espressamente domini per collocarvi le pagine di phishing, oggi si preferisce analizzare i siti Web dal profilo della presenza di vulnerabilità e, nell'affermativa, collocarvi una pagina di phishing (nella maggior parte dei casi in un sottorepertorio). Come descritto nell'ultimo Rapporto semestrale MELANI 2013/1[4] la ricerca di siti Web che presentano *vulnerabilità* è poco dispendiosa perché numerosi gestori di siti Web non aggiornano regolarmente il loro *software di applicazione* – ad esempio i Content Management Systems.

Uno degli obiettivi di MELANI è di eliminare al più presto possibile dalla rete le pagine di phishing. A tale scopo, nel caso che venga resa nota una pagina di phishing, MELANI si rivolge al servizio di contatto del provider (*Servizio Abusi*), invitandolo a eliminare dalla rete la pagina corrispondente. Al riguardo si è affermato a livello internazionale l'esercizio da parte di ogni webhoster di un servizio abusi che riceve le comunicazioni relative alla pagine fraudolente.

I processi e i tempi di reazione entro i quali sono eliminate la pagine fraudolente non sono tuttavia disciplinati in maniera uniforme e variano fortemente. Se alcuni provider eliminano immediatamente e autonomamente le pagine in questione dalla rete, altri provider informano invece anzitutto i titolari dei siti Web intimando loro di adottare le misure necessarie. È soltanto in caso di mancata reazione entro un termine stabilito dal provider che quest'ultimo interviene personalmente.

Anche la disponibilità dei servizi abusi è estremamente diversa. Se alcuni webhoster offrono un servizio non stop, altri webhoster operano soltanto durante le ore di ufficio. Ciò comporta in particolare ritardi se il webhoster si situa in un altro fuso orario e se l'evento phishing si verifica durante il fine settimana o nei giorni festivi.

Non esistono tuttavia soltanto differenze in fatto di velocità e disponibilità. Anche il trattamento degli eventi è effettuato secondo approcci diversi. La semplice cancellazione della pagina di phishing non basta se per collocarla è stata ad esempio sfruttata una vulnerabilità di un CSM. Occorre inoltre rendere attento il titolare del sito Web alla necessità di aggiornare le applicazioni utilizzate. Il mancato aggiornamento ha per conseguenza che i medesimi siti Web forniscano un'impressione negativa per il fatto del ripetuto collocamento di pagine di phishing e di malware. È quanto risulta da un caso che si è verificato in Svizzera nel secondo semestre del 2013: nel periodo compreso tra ottobre e dicembre 2013 il medesimo sito Web

---

2 Liste di controllo e guide MELANI: Misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti (CMS): http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=de (stato: 20 febbraio 2014).

3 https://checkpanel.com/checklist-templates/openx-maintenance (stato: 20 febbraio 2014).
https://checkpanel.com/checklist-templates/revive-maintenance (stato: 20 febbraio 2014).

4 Rapporto semestrale MELANI 2013/1, capitolo 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

svizzero è stato utilizzato abusivamente tre volte consecutive per collocarvi pagine di phishing ai danni di diversi fornitori di servizi finanziarie e di ditte di carte di credito.

Il provider di hosting non ha alcun obbligo di istituire un servizio abusi. Se però non è gestita sufficientemente una rete finisce rapidamente in una *blacklist*. È ciò che viene praticato in maniera corrispondente specialmente in ambito di spam. Se lo spammer si trova su una rete può capitare rapidamente – senza azione corrispondente da parte del provider – che il settore di rete *(IP Range)* finisca in un filtro spam e che tutti i clienti non possano più inviare e-mail. Nel caso delle pagine di phishing questo principio non è applicato in maniera conseguente, circostanza che offre ai singoli provider un margine di manovra nel trattamento delle pagine di phishing.

3.4 Professionalizzazione della truffa dell'anticipo

Oltre ai dati delle carte di credito si derubano sempre più anche i dati di accesso alla posta elettronica. Ma a quale scopo questi dati di accesso alla posta elettronica sono poi effettivamente utilizzati? Dai nostri precedenti rapporti semestrali è nota la variante della truffa all'anticipo mediante e-mail che pretendono che il loro mittente è trattenuto all'estero e si trova in difficoltà[5]. Dato che il conto di posta elettronica si trova nelle mani del truffatore, questi può fare credere alla vittima che la comunicazione proviene effettivamente da una persona che gli è nota. La vittima è allora indotta a versare un importo.

Un'ulteriore variante, osservata reiteratamente, consiste nella perlustrazione delle e-mail alla ricerca di comunicazioni con un istituto finanziario. Il truffatore tenta successivamente di riprendere questa comunicazione con gli impiegati della banca e di convincerli a effettuare un pagamento. Questa variante viene soprattutto osservata all'estero, ma esistono anche singoli casi in Svizzera.

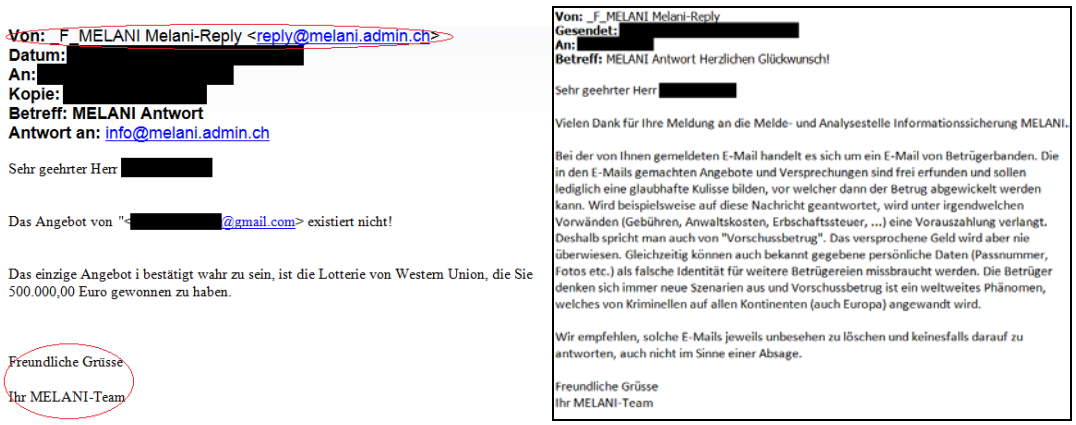
A fine 2013 MELANI ha osservato una variante molto più perfida. Tutto è iniziato con una semplice e-mail di truffa all'anticipo. Una siffatta e-mail prospetta alla vittima ingenti guadagni o ingenti somme provenienti da un'eredità. Se la vittima ha abboccato una prima volta si succedono poi richieste di presunti e indispensabili anticipi, come le imposte sugli utili, sulle successioni e sulle transazioni. La vittima non vede tuttavia l'ombra del denaro promesso.

Nel caso descritto qui sopra la vittima fece prova di scetticismo e decise di chiedere alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) se l'e-mail era autentica e se doveva accettare l'offerta. Come sempre in simili casi MELANI diede la risposta standard di stare alla larga da siffatte e-mail, di distruggerle e di non contattare affatto i truffatori. Per questo motivo è apparsa ancor più sorprendente la reazione della vittima che richiese nuovamente per scritto a MELANI se riteneva effettivamente che l'affare fosse pulito e se le imposte richieste dovessero essere pagate in anticipo.

MELANI, irritata, si mise telefonicamente in contatto con la persona che aveva effettuato la comunicazione per chiarire che questa e-mail era una e-mail di truffa e che non doveva essere eseguito in nessun caso un versamento. Nel corso della telefonata emerse chiaramente che i truffatori avevano manipolato la e-mail di MELANI, modificandola in maniera tale da indurre la vittima a effettuare il versamento. I truffatori avevano quindi accesso al conto di posta elettronica della vittima per effettuare le manipolazioni corrispondenti.

---

[5] Rapporto semestrale MELANI 2012/1, capitolo 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 20 febbraio 2014).



Von: _F_MELANI Melani-Reply <reply@melani.admin.ch>
Datum: [redacted]
An: [redacted]
Kopie: [redacted]
Betreff: MELANI Antwort
Antwort an: info@melani.admin.ch

Sehr geehrter Herr [redacted]

Das Angebot von "<[redacted]@gmail.com> existiert nicht!

Das einzige Angebot i bestätigt wahr zu sein, ist die Lotterie von Western Union, die Sie 500.000,00 Euro gewonnen zu haben.

Freundliche Grüsse

Ihr MELANI-Team

Von: _F_MELANI Melani-Reply
Gesendet: [redacted]
An: [redacted]
Betreff: MELANI Antwort Herzlichen Glückwunsch!

Sehr geehrter Herr [redacted]

Vielen Dank für Ihre Meldung an die Melde- und Analysestelle Informationssicherung MELANI.

Bei der von Ihnen gemeldeten E-Mail handelt es sich um ein E-Mail von Betrügerbanden. Die in den E-Mails gemachten Angebote und Versprechungen sind frei erfunden und sollen lediglich eine glaubhafte Kulisse bilden, vor welcher dann der Betrug abgewickelt werden kann. Wird beispielsweise auf diese Nachricht geantwortet, wird unter irgendwelchen Vorwänden (Gebühren, Anwaltskosten, Erbschaftssteuer, ...) eine Vorauszahlung verlangt. Deshalb spricht man auch von "Vorschussbetrug". Das versprochene Geld wird aber nie überwiesen. Gleichzeitig können auch bekannt gegebene persönliche Daten (Passnummer, Fotos etc.) als falsche Identität für weitere Betrügereien missbraucht werden. Die Betrüger denken sich immer neue Szenarien aus und Vorschussbetrug ist ein weltweites Phänomen, welches von Kriminellen auf allen Kontinenten (auch Europa) angewandt wird.

Wir empfehlen, solche E-Mails jeweils unbesehen zu löschen und keinesfalls darauf zu antworten, auch nicht im Sinne einer Absage.

Freundliche Grüsse
Ihr MELANI-Team

Figura 1: Sinistra: e-mail falsificata dei truffatori; destra: e-mail originale di MELANI

3.5 Estratti conto bancari a un falso indirizzo

In seguito a un errore di programmazione l'invio di fine anno della Banca Coop ha comportato in parte distribuzioni errate: alcuni estratti conto sono stati inviati a destinatari sbagliati. Nel frattempo la Banca Coop ha accertato la causa e individuato la ragione della distribuzione errata, che va posta in relazione con l'introduzione di un nuovo compendio puntuale del programma Supercard al quale partecipa la banca. I destinatari della documentazione inviata per errore sono stati invitati a restituirla alla banca. Dal canto suo la Banca Coop ha promesso di adottare tutte le misure necessarie per evitare simili errori in futuro.

A Basilea Città, la sede principale della banca, il Ministero pubblico ha reso noto di avere avviato un'inchiesta di polizia per sospetto di violazione per negligenza del segreto bancario.

Questo caso non è unico. A febbraio 2014 venne reso pubblico il caso del revisore PricewaterhouseCoopers (PWC) che, in modo simile, aveva sbagliato a inviare dei certificati di salario ai propri impiegati.[6] In ambito di TIC esiste una chiara tendenza a integrare programmi sempre più complessi con un numero sempre maggiore di funzioni. Il fatto che all'aumento del numero di righe di programma corrisponda anche un incremento del rischio di errori va da sé. Un problema particolare è costituito dalle applicazioni che possono essere modificate o aggiornate soltanto in fase d'esercizio. Sebbene vengano effettuati numerosi esperimenti preliminari su sistemi di collaudo, non è possibile testare tutte le interdipendenze che esistono a iosa in questi programmi.

3.6 Furto di dati dal sistema di informazione Schengen: colpita anche la Svizzera

Nel corso del mese di dicembre diversi media svizzeri hanno riportato un'informazione facente stato di un furto di dati ai danni della banca dati SIS (sistema d'informazione Schengen). Il SIS è un sistema di informazione al cui interno possono essere segnalati gli oggetti rubati e le persone ricercate dalla polizia ai fini di estradizione, che sono colpite da un divieto di entrata o che sono considerate scomparse. Le autorità di polizia e doganali dei Paesi membri dello spazio Schengen hanno accesso a questa banca dati.

[6] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/PWCMitarbeiter-erhalten-Lohnausweise-der-Kollegen/story/26934239 (stato: 20 febbraio 2014).

L'accesso non autorizzato ha avuto luogo attraverso una lacuna di sicurezza della società che gestiva la banca dati per conto della polizia danese nel 2012. Per il fatto della natura transnazionale del SIS la lacuna concerne potenzialmente e automaticamente i dati raccolti in tutti i Paesi aventi accesso al sistema. La Svizzera è pertanto stata informata della lacuna nel mese di maggio del 2013. Sul totale di 1.2 milioni di dati derubati, 26'478 sono stati immessi dalle autorità svizzere. Il repertorio derubato contiene dati personali e dati codificati che si riferiscono segnatamente al motivo del loro inserimento nella banca dati. Questi ultimi dati non sono direttamente interpretabili e in linea di principio non è pertanto possibile abbinare degli atti a persone che figurano nell'elenco. La lacuna riguarda unicamente il sistema SIS 1, poi sostituito nel maggio del 2013 dal sistema SIS 2.

I dettagli dell'attacco (metodo utilizzato, lacuna) e le motivazioni degli autori sono ancora poco chiari e non saranno probabilmente resi pubblici prima della fine delle investigazioni effettuate in Danimarca. Le autorità danesi hanno nondimeno precisato di aver posto rimedio alla lacuna utilizzata. Diversi elementi sono stati peraltro rivelati dalle autorità germaniche nel quadro della risposta alle domande di un deputato. Le autorità germaniche avanzano l'ipotesi di un attacco poco mirato che non era diretto specificamente contro il SIS, ma aveva sfruttato una lacuna su un server contenente anche altri dati. Due hacker, un danese e uno svedese, sarebbero implicati nell'attacco.

Questo evento evidenzia una problematica essenziale in ambito di specificazione e di implementazione di sistemi di scambio internazionale di dati delicati e sensibili. A livello politico simili sistemi sono sovente anzitutto specificati con riferimento ai dati che devono essere scambiati. Le esigenze tecniche di implementazione sono trattate soltanto a livello subordinato oppure lasciate alla decisione dei singoli Stati membri. Ciò va di pari passo con il rischio che in caso di attuazione subottimale in uno Stato membro anche i dati degli altri Paesi sarebbero compromessi. In futuro pertanto anche nel caso di altri progetti di scambio di informazioni si dovrà insistere affinché sia disponibile non soltanto una definizione dei dati da scambiare, ma sia anche stato chiaramente predefinito uno standard minimo valido per tutti in ambito di tutela, di elaborazione e di trasmissione tecnica.

3.7 NZZ irraggiungibile – problemi tecnici

Il 19 agosto 2013 il sito Web della NZZ non ha potuto essere raggiunto da alcuni visitatori. Dietro questo evento si è inizialmente presunto un attacco. Secondo Swisscom all'origine di questa avaria c'è un errore nel rinnovamento del nome a dominio tra il servizio di rete Networksolutions e Swisscom.

A quel momento il dominio ip-plus.net di Swisscom era registrato presso la ditta Networksolutions. Il 19 agosto 2013 alle 12:40 la ditta Networksolutions ha troncato i *domini*, ragione per la quale la risoluzione di ip-plus.net non ha più potuto essere effettuata, con la conseguenza che questo dominio non ha più funzionato. Dato che sotto di esso operavano anche i *servizi DNS* di imprese terze, come ad esempio la NZZ, anche questi siti si sono inevitabilmente arrestati e non sono più stati raggiungibili. Fin dalle 15:25 Swisscom aveva potuto risolvere il problema e anche la divisione IT della NZZ aveva immediatamente cancellato tutti i server interesati dalle registrazioni DNS, sostituendoli con server funzionanti. Dato che le risoluzioni mancate rimangono memorizzate nel Name Server e nella *Internet Explorer Cache* durante 24 ore, ci sono volute quasi 24 ore finché tutti i servizi hanno nuovamente funzionato

perfettamente[7]. In seguito a questo evento, Swisscom ha introdotto immediatamente delle misure per evitare il ripetersi di un caso simile.

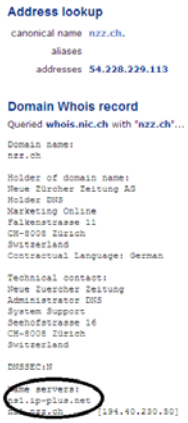


Figura 2: Registrazione Whois della NZZ con il server DNS di ip-plus.net

Con l'ausilio del Domain Name Systems (DNS) è possibile utilizzare Internet e i suoi servizi in maniera conviviale perché al posto degli indirizzi IP si possono utilizzare gli indirizzi Web (URL). Senza server DNS Internet rimane funzionante ma al posto degli URL occorre immettere i numeri IP. Al livello massimo della gerarchia dei numeri IP si situano i Root-Server, che come istanza superiore hanno la competenza sulle informazioni relative ai domini (p.es. .com, .net, .ch). Le istanze inferiori (Second Level Domains) sono esercitate da numerosi grandi e piccoli fornitori di servizi Internet. Un'avaria o una manipolazione può avere di volta in volta ampie ripercussioni, in particolare quando – come nella fattispecie – si tratta di un importante server DNS di una grande impresa.

3.8 La Svizzera vince la prima Cyber Security Alpen Cup

Per prevenire il problema della mancanza di specialisti di Cyber Security nel Paese e agevolare nel contempo la ricerca di talenti all'economia, l'associazione Cyber Security Austria (CSA) ha dato il via nel 2012 al Cyber Security Challenge. Nel quadro di questa competizione indetta in cooperazione con il Kuratorium Sicheres Österreich (KSÖ) e con l'Abwehramt centinaia di scolari si sono battuti per la vittoria nell'ambito di una procedura di selezione su Internet.

Nel 2013 l'associazione Swiss Cyber Storm ha ripreso questa idea con il patrocinio della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) della Confederazione e dell'associazione Verein Swiss Police ICT[8]. Sotto la direzione di Cyber Security Austria si è poi decisa l'esecuzione di una competizione transnazionale, come pure l'estensione della partecipazione a scolari e studenti. Era così nata la Security Alpen Cup.

Dal 5 al 7 novembre 2013 si è svolta a Linz la prima Cyber Security Alpen Cup. Dopo una prima giornata consacrata ad attività di costituzione dei team e al tempo di fare conoscenza, il secondo giorno si è svolta la competizione vera e propria. Entrambi i team provenienti dall'Austria e dalla Svizzera hanno tentato per oltre undici ore di decifrare codici, individuare lacune di sicurezza e trovare possibilità di accesso a telefoni mobili e tablet. Non si trattava soltanto di attacchi ma anche di misure per impedire l'accesso alle persone non autorizzate.

[7] http://www.nzz.ch/aktuell/digital/nzz-dns-1.18135806 (stato: 20 febbraio 2014).

[8] Rapporto semestrale MELANI 2013/1, capitolo 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

Il team Svizzera è risultato alla fine vincitore di questa competizione e ha ricevuto la coppa nel corso di una cerimonia di premiazione che si è svolta all'Heeresgeschichtliches Museum di Vienna, alla presenza di numerosi ospiti provenienti da ambienti della politica, dell'esercito e dell'economia.

Il concetto di una competizione in ambito di Cyber Security come piattaforma di ricerca di talenti e di promovimento delle nuove leve, così come la riuscita della sua attuazione nel quadro della prima Security Alpen Cup, non sono rimasti inosservati: l'anno prossimo anche la Germania parteciperà alla competizione. L'eliminatoria svizzera per la partecipazione alla competizione si svolgerà nuovamente nel quadro della Conferenza IT Security Swiss Cyber Storm, la cui quinta edizione avrà luogo il 22 ottobre 2014 al KKL di Lucerna. Gli scolari e gli studenti interessati possono già effettuare la loro preregistrazione su www.verbotengut.ch.

3.9 Malware anche sui sistemi Linux

Il software nocivo non colpisce soltanto i sistemi Windows (Microsoft) e OSX (Apple), ma anche Unix / Linux. Nel corso del secondo semestre del 2013 è stata annunciata a MELANI la compromissione in Svizzera di numerosi sistemi Unix / Linux, infettati da un ingegnoso *Rootkit* denominato Ebury. In questo contesto i criminali sono riusciti, in maniera tuttora sconosciuta, a procurarsi l'accesso al sistema delle vittime e a installarvi il *rootkit* Ebury. Al riguardo il *Daemon SSH* solitamente installato sul sistema della vittima è modificato in maniera tale che ad avvenuta infezione i dati di accesso di tutti gli utenti che effettuano il login via SSH sul sistema infettato sono trasmessi ai criminali. Il *rootkit* Ebury deruba inoltre le chiavi private SSH che si trovano sul sistema. Grazie ai dati di acceso derubati gli aggressori possono accedere in ogni momento al sistema infettato e utilizzarlo per scopi illegali, come ad esempio l'*hosting* di *server C&C* oppure l'invio di e-mail di *spam*.

Dato che nel caso di Ebury si tratta di un software nocivo con funzionalità rootkit esso è difficilmente individuabile sui sistemi infettati. Inoltre Ebury utilizza un protocollo basato su DNS come canale di comunicazione tra il sistema che ha infettato e i criminali. In molti casi ciò rende difficile individuare l'infezione.

Ulteriori informazioni su Ebury e sulle modalità di individuazione di questo software nocivo sono disponibili sul sito Web del CERT-Bund germanico[9].

L'Open Source viene sovente postulato come possibile alternativa all'utilizzo di cosiddette soluzioni di software proprietario. La logica secondo la quale *Open Source* è tracciabile e quindi più sicuro è troppo semplicistica. Le soluzioni Open Source consentono invero di sondare il codice di programma al ricerca di errori. Se però nessun errore dovesse essere rintracciato e non dovesse quindi essere eliminato dalla Community anche le soluzioni Open Source rimarrebbero un vettore di attacco. Per non dipendere dagli interessi della Community Open Source si dovrebbe prospettare in ambito di uso professionale di soluzioni Open Source che un team interno esamini il software utilizzato dal profilo delle priorità aziendali. Questa considerazione va integrata in maniera corrispondente nella ponderazione economica dell'uso dell'Open Source o di *sistemi proprietari*.

[9] https://www.cert-bund.de/ebury-faq (stato: 20 febbraio 2014).

3.10 Attacchi di amplificazione NTP – L'infrastruttura svizzera già oggetto di uso abusivo

Anche nel corso degli ultimi mesi i cosiddetti attacchi di *Distributed Denial Of Service* (DDoS) hanno costituito un metodo frequentemente utilizzato dai cibercriminali per limitare o addirittura interrompere la raggiungibilità di determinati servizi o siti Web. Al riguardo si possono distinguere diversi generi di attacchi: dopo un forte incremento degli attacchi di amplificazione DNS[10] nel corso dell'ultimo semestre, ciò che potenzia gli attacchi di un fattore compreso tra 20 e 50 (cfr. in merito il Rapporto semestrale MELANI 2013/1[11]), si è assistito nel secondo semestre del 2013, in vista di attacchi DDoS, ad abusi del medesimo genere del *protocollo NTP* destinato alla sincronizzazione degli orologi. In questo contesto gli aggressori richiedono dati ai server NTP utilizzando indirizzi di mittente falsificati. Le risposte, che superano di un multiplo le richieste, pervengono poi agli indirizzi presunti dei mittenti, ossia all'obiettivo effettivo dell'attacco. Dato che le risposte costituiscono dati legittimi provenienti da server affidabili è particolarmente difficile bloccare questo genere di attacchi. Gli attacchi NTP sono ancora più efficaci degli attacchi di amplificazione DNS e possono provocare un'amplificazione di fattore 500[12]. MELANI ha già rivolto la propria attenzione a diversi server NTP in Svizzera, utilizzati in maniera abusiva per sferrare attacchi.

Gli attacchi NTP si basano sullo sfruttamento del comando «monlist» – una caratteristica attivata in standard nelle apparecchiature idonee all'NTP più vecchie[13]. Questo comando fornisce un elenco dei 600 *indirizzi IP* che si sono collegati per ultimo al server NTP. In caso di falsificazione dell'indirizzo originario si invia pertanto l'intero elenco alla vittima.

Per impedire che un'apparecchiatura NTP venga utilizzata abusivamente per simili attacchi la funzione «monlist» può essere disattivata oppure aggiornata alla versione più recente di NTP che la disattiva in standard.

In considerazione dell'incremento di attacchi DDoS si consiglia a ogni impresa la cui attività aziendale dipende dalla raggiungibilità del suo sito Web e/o della connettività Internet di accertare i rischi di simili attacchi e di pianificare misure di difesa. Oltre a misure tecniche di individuazione e di difesa ciò comprende tipicamente anche una valutazione delle capacità del provider e dei suoi obblighi contrattuali in caso di evento.

---

[10] Nel caso di un attacco di amplificazione DNS vengono inviate richieste DND falsificate ad un server aperto DNS su Internet. Dato che gli indirizzi IP sorgente sono falsificati le risposte sono inviate all'indirizzo IP della vittima e non a quello del mittente effettivo del pacchetto di dati.

[11] Rapporto semestrale MELANI 2013/1, capitolo 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

[12] http://www.zdnet.de/88184056/rekord-ddos-angriff-europa-erreicht-400-gbits/?ModPagespeed=noscript (stato: 20 febbraio 2014).

[13] https://www.us-cert.gov/ncas/alerts/TA14-013A (stato: 20 febbraio 2014).

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Ulteriori rivelazioni sulla NSA e il GCHQ

Anche nel secondo semestre del 2013 la pubblicazione da parte di diversi giornalisti delle attività della National Security Agency statunitense (NSA), del General Communication Headquarter britannico (GCHQ) e di altri servizi segreti stranieri sulla base dei documenti di Edward Snowden ha costituito un vasto tema. Sempre nel corso del secondo semestre si è consolidata – dopo le prime rivelazioni su Prism, XKeyscore e Tempora, già tematizzate da MELANI nel suo ultimo Rapporto semestrale[14] – l'immagine di un rilevamento generalizzato e integrale dei dati da parte di questi servizi segreti statunitensi e britannici. In questo senso ad esempio si è venuti a sapere che la NSA, in maniera analoga all'operazione britannica Tempora, gestisce un programma denominato Upstream[15] per accedere ai dati sulle fibre ottiche. Questa collaborazione con le imprese statunitensi di telecomunicazione dovrebbe essere costata alla NSA circa 278 milioni di dollari nel 2013.[16] Si è altresì venuti a conoscenza di un progetto comune della NSA e del GCHQ, noto con il nome di codice Muscular, che persegue l'obiettivo di procurarsi l'accesso ai centri di calcolo di Google e di Yahoo[17]. Il documento pubblicato stima in 181 milioni le serie di dati carpite sull'arco di 30 giorni. Un'ulteriore idea sulle dimensioni è fornita da una presentazione del 2012, dalla quale risulta che a livello mondiale la NSA avrebbe infettato con malware 50'000 computer per accedere a dati sensibili[18]. Un documento pubblicato nel gennaio del 2014 fa stato di 100'00 computer hackerati dalla NSA[19].

I dibattiti non sono stati alimentati soltanto dalle dimensioni ma a che dagli obiettivi perseguiti dalla NSA. In questo senso l'obiettivo primario dell'intercettazione andrebbe tuttora intravvisto nella difesa contro il terrorismo. Il fatto che nelle diverse azioni di intercettazione siano stati presi di mira capi di Governo e diplomatici ha comunque reso rapidamente evidente la presenza di una componente politica. In America latina ha suscitato indignazione l'intercettazione della presidentessa brasiliana Rousseff, dell'attuale presidente messicano Peña Nieto e del precedente presidente messicano Felipe Calderón[20]. A livello internazionale la presunta intercettazione al vertice G8/G20 di Toronto[21] è stata tema di discussioni, mentre in

---

14 Rapporto semestrale MELANI 2013/1, capitolo 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

15 http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (stato: 20 febbraio 2014).

16 http://www.heise.de/newsticker/meldung/Ueberwachungsaffaere-NSA-zahlt-Hunderte-Millionen-Dollar-an-Provider-1945984.html (stato: 20 febbraio 2014).

17 http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (stato: 20 febbraio 2014).

18 http://www.spiegel.de/netzwelt/netzpolitik/nsa-soll-50-000-netzwerke-weltweit-infiltriert-haben-a-935335.html (stato: 20 febbraio 2014).

19 http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0 (stato: 20 febbraio 2014).

20 http://www.bbc.co.uk/news/world-latin-america-23938909 (stato: 20 febbraio 2014).

21 http://www.spiegel.de/netzwelt/netzpolitik/kanada-erlaubte-nsa-spionage-bei-g-8-gipfel-a-936255.html (stato: 20 febbraio 2014).

Europa ha soprattutto fatto titolo l'intercettazione del telefono mobile della cancelliera federale germanica Angela Merkel[22].

È parimenti divenuta di dominio pubblico l'Operation Socialist[23]. Essa consisteva in un attacco alla filiale Bics di Belgacom (una joint-venture di Belgacom con Swisscom e la sudafricana MTM). I grandi clienti di questa impresa di telecomunicazione sono tra l'atro la Commissione dell'UE, il Consiglio degli Stati membri e il Parlamento europeo.

Operation Socialist / Attacco alla Bics

Nel contesto delle rivelazioni sulla NSA Belgacom aveva ordinato un'inchiesta interna e constatato un attacco, inizialmente attribuito alla NSA. A seguito di una seconda rivelazione i sospetti si sono portati sul GCHQ, nel senso che i britannici avrebbero utilizzato tecnologie sviluppate dalla NSA. Nel caso dell'«Operation Socialist» si sarebbe trattato di «meglio spiare Belgacom» e di una «migliore comprensione dell'infrastruttura». Secondo la presentazione sono stati infettati a tale scopo i computer dei collaboratori di Belgacom e si è successivamente tentato di accedere ai server centrali di *roaming* a partire da questi computer.

Questo caso concerne anche direttamente e indirettamente la Svizzera perché Swisscom partecipa nella misura del 24 per cento alla Bics. Swisscom a sua volta appartiene nella misura del 51 per cento allo Stato svizzero e quindi ai contribuenti svizzeri.

Standard di cifratura corrotto?

Dal profilo della sicurezza dell'informazione uno dei quesiti più importanti è in quale misura i programmi di cifratura e gli standard di cifratura siano attualmente ancora affidabili. In questo ambito ha fatto soprattutto titolo lo standard Dual_EC_DRBG, un generatore di numeri aleatori sviluppato dalla NSA, ma che non fornisce i numeri in maniera così aleatoria come dovrebbe realmente: nel dicembre del 2013 è stato reso noto che la NSA avrebbe presumibilmente versato 10 milioni di dollari alla ditta RSA-Security affinché questa impresa di sicurezza implementasse in standard questo generatore discutibile di numeri aleatori nel software BSAFE diffuso a livello mondiale[24]. RSA ha smentito questi rapporti, mentre la NSA non ha reagito a questa pubblicazione.

I limiti della cifratura – Bullrun e Edgehill

Dai dati pubblicati emerge quanto sistematicamente entrambi i servizi segreti GCHQ e NSA abbiano abbordato la tematica della decodificazione[25] [26]. Nel corso degli ultimi anni entrambi i servizi segreti hanno apparentemente accumulato una massa di misure e di tecniche per forzare o eludere le cifrature. Ne costituisce un aspetto l'indebolimento del generatore di numeri aleatori menzionato qui sopra. Grazie a siffatti generatori manipolati la cifratura sembra invero forte, ma può essere forzata con un dispendio calcolatorio relativamente esiguo. Anche il «procacciamento» di chiavi costituisce una possibilità di decodificare i dati criptati in tempo reale o anche a posteriori.

---

22 http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html (stato: 20 febbraio 2014).

23 http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html (stato: 20 febbraio 2014).

24 http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 (stato: 20 febbraio 2014).

25 http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (stato: 20 febbraio 2014).

26 https://www.schneier.com/blog/archives/2013/10/defending_again_1.html (stato: 20 febbraio 2014).

Nel dicembre del 2013 è stato infine reso noto pubblicamente che la NSA può forzare in maniera semplice lo *stream* Cipher A5/1, quello maggiormente utilizzato a livello mondiale, che garantisce la cifratura tra telefono mobile e antenna[27]. È così possibile decodificare le chiamate e i messaggi di testo.

Altrimenti rimane ancora la possibilità di introdursi nei sistemi e carpire i dati prima ancora della loro cifratura. A livello di NSA è competente in merito la cosiddetta divisione «Tailored Access Operation» (TAO)[28].

Qui di seguito ulteriori tematiche incentrate sul contesto dell'affaire Snowden:

Royal Concierge

Il settimanale tedesco Spiegel ha pubblicato nel novembre del 2013 un articolo sul programma di sorveglianza Royal Concierge, gestito dal GCHQ britannico. Esso può sorvegliare a livello mondiale le prenotazioni presso almeno 350 alberghi di lusso e quindi constatarvi il soggiorno di diplomatici o di alti funzionari[29].

TOR – non direttamente forzabile

Sempre secondo una presentazione pubblica di Snowden anche il *servizio di anonimizzazione* TOR ha suscitato l'attenzione della NSA. La NSA non ha potuto invero forzare direttamente la rete TOR per smascherarne i singoli utenti. Sembra tuttavia possibile attaccare singoli utenti di TOR sfruttando le vulnerabilità dei browser Firefox. Come rilevato dalla presentazione[30] ciò sarebbe nondimeno possibile soltanto nel caso di una piccola parte degli utenti di TOR.

Follow the Money - SWIFT

In Svizzera ha soprattutto provocato scalpore l'annuncio che il fornitore di servizi finanziari SWIFT sarebbe stato spiato dalla NSA. Uno dei tre centri di calcolo di SWIFT si trova nella località turgoviese di Diessenhofen. Qui vengono elaborate quotidianamente fino a 15 milioni di transazioni finanziarie. Nel contesto di questa pubblicazione si è altresì preteso che presso la NSA esisteva una divisione denominata «Follow the Money», competente per lo spionaggio di dati finanziari. SWIFT ha dichiarato che non esistono motivi per supporre che si sia mai tentata una penetrazione non autorizzata nel sistema[31].

La «Signals Intelligence Strategy (SIGINT)» della NSA del febbraio del 2012, pubblicata sul New York Times nel novembre del 2013, puntualizza molto chiaramente la strategia della NSA: «Ensure Signals Intelligence provides THE decisive edge in advancing the full spectrum of U.S. national security interests». In order to fulfil this vision, it is ready to: «Defeat ad-

[27] http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html (stato: 20 febbraio 2014).

[28] http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html (stato: 20 febbraio 2014).

[29] http://www.spiegel.de/netzwelt/netzpolitik/royal-concierge-britischer-geheimdienst-ueberwacht-diplomatenhotels-a-933997.html (stato: 20 febbraio 2014).

[30] http://www.zdnet.de/88171545/nsa-arbeitet-sich-an-anonymisierungsdienst-tor-ab/?ModPagespeed=noscript (stato: 20 febbraio 2014).

[31] http://www.nzz.ch/aktuell/schweiz/swift-bestreitet-nsa-spionage-1.18151215 (stato: 20 febbraio 2014).

versary cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere»[32].

I dati devono pertanto poter essere ottenuti dalla NSA in qualsiasi momento, in qualsiasi luogo e da qualsiasi persona. Le pubblicazioni e i dati ormai resi pubblici confermano che le dichiarazioni in merito a questa strategia non sono soltanto una mera dichiarazione di intenti, ma che la NSA e suoi partner attuano anche effettivamente questa strategia. Le ripercussioni che queste rivelazioni avranno sull'evoluzione di Internet sono al momento ancora difficilmente prevedibili.[33] Nel frattempo si sono già elevate voci che predicono la fine dell'Internet attuale. In futuro gli utenti commerciali ma anche privati di Internet dovranno maggiormente dibattere su questo tema tenendo conto delle conseguenze causate dalla pubblicazione dei documenti da parte di Snowden e dei conseguenti potenziali rischi.

4.2 APT - rinnovo dei metodi

«NetTraveler» è una *APT* (acronimo di «advanced persistent threat») illustrata da Kaspersky nel giugno del 2013. Ne erano bersagli società attive nell'industria, la produzione di energia, le telecomunicazioni e le nuove tecnologie o ancore enti governativi. Nel settembre del medesimo 2013 Kaspersky ha fornito alcuni elementi che testimoniano del rinnovo di questa APT, che integra ormai nuovi vettori di attacco. Se in passato NetTraveler ha già fatto ampio uso di *spear phishing* per diffondere codice nocivo, l'utilizzazione di un metodo di tipo *watering hole* costituisce un'osservazione inedita[34]. Un'ulteriore novità rivelata dai ricercatori di FireEye è lo sfruttamento di una lacuna di sicurezza del software Java.

L'operazione «Molerats» è stata rivelata dalla società FireEye nell'ottobre del 2012. Essa era diretta contro bersagli governativi in Israele, ma anche in Palestina, e sarebbe stata condotta a partire dal Medio Oriente. Questo gruppo sembrava allora privilegiare XtremeRAT, un malware diffuso e sovente associato ad aggressori provenienti da queste regioni. Talune nuove rivelazioni effettuate da FireEye nell'agosto del 2013 attestano ormai che questo gruppo utilizza Poison Ivy nell'ambito di attacchi diretti contro gli USA e il Medio Oriente. Poison Ivy è un altro malware sovente associato ad autori cinesi. La sua utilizzazione da parte di aggressori originari di una diversa zona geografica è un'informazione inedita.

Questi due esempi testimoniano della grande capacità di adattamento e dell'opportunismo di cui possono fare prova i gruppi che sferrano attacchi di tipo APT. I metodi e gli strumenti utilizzati da questi gruppi non sono fissi e possono evolvere ed essere ridefiniti in funzione delle circostanze o del bersaglio. Questa capacità di rinnovamento va integrata ad ogni analisi.

Ciò comporta segnatamente implicazioni in ambito di attribuzione di un attacco. Occorre prendere in considerazione tutto un complesso di elementi per arrischiare l'espressione di un simile giudizio. Un approccio troppo meccanico che si basasse unicamente sul modus operandi e sugli strumenti utilizzati si rivela in genere rischioso. Di conseguenza ai fini dell'attribuzione occorre anche fondarsi su informazioni non tecniche e vanno sempre presi in considerazione i veri intenti, il motivo, la vittima e le ripercussioni.

---

[32] http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?pagewanted=all (stato: 20 febbraio 2014).

[33] Si veda il capitolo 5.1 del presente rapporto.

[34] Rapporto semestrale MELANI 2013/1, capitolo 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

4.3 Derubati milioni di dati di clienti Adobe

Uno dei maggiori furti di password è stato reso noto all'inizio del mese di ottobre. Ne sé stata vittima la ditta Adobe. Se inizialmente fu questione di 2.9 milioni di dati di utente, di password e di dati di carte di credito, dopo poche settimane Adobe ne corresse il numero in 38 milioni[35]. Un file con una capienza di 3.8 GB apparso ulteriormente avrebbe addirittura contenuto 150 milioni di dati di utente e di password *con crittografia hash*. Questa circostanza non è però stata confermata ufficialmente da Adobe. Secondo Adobe sono stati derubati dati di carte di credito e password criptati. Per decodificare i dati è necessaria una chiave di sicurezza (*3DES*) che gli aggressori non sono apparentemente riusciti a derubare. Senza decodificazione sono tuttavia leggibili i suggerimenti password, tramite i quali si può in parte desumere la password. In questo senso ad esempio il suggerimento «1-6» consente di desumere la combinazione di numeri «123456». Dato che è sempre stata utilizzata la medesima chiave 3DES, tutte le password identiche avevano la medesima apparenza anche dopo la cifratura, di modo che è stato possibile riunire le password identiche. Queste indicazioni sono bastate per allestire e pubblicare un elenco delle 100 password maggiormente utilizzate[36]. Ciò che ha sorpreso è che numerosi utenti hanno scelto password molto semplici. Questa circostanza può da un canto essere riconducibile a una mancanza di sensibilità mentre d'altro canto è possibile che i clienti considerino «senza valore» determinati account e password, perché intendono utilizzare il conto soltanto per un acquisto oppure perché ritengono che il conto non contenga dati degni di protezione.

Adobe ha resettato tutte le password dopo che è stato reso noto l'attacco. I 38 milioni di utenti direttamente colpiti secondo Adobe sono stati informati via e-mail e obbligati a immettere una nuova password.

Sembra che oltre ai dati di utente agli aggressori sia anche stato possibile procurarsi i *Sourcecodes* dei prodotti Adobe ColdFusion, Acrobat e Photoshop. L'attacco sarebbe stato effettuato nel mese di agosto del 2013.

A prescindere da tutti gli inconvenienti che un simile evento comporta per un'impresa, la comunicazione con la clientela costituisce un importante elemento per contenere il danno nella misura del possibile. Adobe ha resettato tutte le password, informato i clienti via e-mail dell'attacco e li ha invitati a scegliere una nuova password.

Ma proprio queste e-mail devono essere inviate in maniera molto meditata perché da un canto esse sono predestinate a fungere da modello per ulteriori attacchi (di phishing). D'altro canto la sensibilità degli utenti di Internet è nel frattempo divenuta talmente elevata da considerare rapidamente fraudolente siffatte e-mail. In questo senso MELANI ha ricevuto numerose comunicazioni da cittadini scettici sull'effettiva provenienza da Adobe di queste e-mail di informazione di Adobe. Una comunicazione troppo spensierata con la clientela può anche influenzare negativamente il comportamento dei clienti in fatto di e-mail fraudolente[37].

Un problema che non va sottovalutato in simili casi è che gli utenti non utilizzano una password per un solo servizio, ma per più servizi. In caso di furto della password unitamente al relativo indirizzo e-mail si schiudono possibilità di accedere ad altre prestazioni di servizi Internet.

[35] http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ (stato: 20 febbraio 2014).

[36] http://stricture-group.com/files/adobe-top100.txt (stato: 20 febbraio 2014).

[37] Rapporto semestrale MELANI 2012/1, capitolo 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 20 febbraio 2014).

4.4 Attacchi ai punti di vendita degli empori Target

Nel corso del mese di dicembre diversi articoli confermati da un comunicato stampa della catena di empori Target hanno reso pubblico un attacco di grandi dimensioni ai danni di questa impresa. Le informazioni pubblicate fanno stato del furto dei dettagli concernenti 40 milioni di carte di credito e dei dati personali riguardanti 70 milioni di clienti.

L'attacco è stato perpetrato durante il periodo commercialmente molto attivo che precede le feste di fine anno, tra il 27 novembre e il 15 dicembre. Target ha inizialmente comunicato in maniera molto lapidaria in merito all'incidente ed è soltanto poco alla volta – a ridosso delle ricerche e delle rivelazioni pubblicate da diverse fonti – che è stato possibile ricostruire in parte le circostanze dell'attacco e i metodi utilizzati. All'atto della redazione del presente rapporto alcuni aspetti ne rimangono tuttora incerti.

Le prime analisi, confermate da Target, precisano che l'intrusione è avvenuta tramite un malware che ha infettato i terminali dei *punti di vendita*[38]. I sospetti si portano invero sul malware BlackPOS o una delle sue varianti, che sarebbe presumibilmente stato implementato da bande criminali dell'Europa dell'Est. Il malware in questione riesce a copiare i dati contenuti nella striscia magnetica della carta negli istanti che seguono la sua utilizzazione sul terminale di pagamento, quando essi sono disponibili in chiaro nella memoria ad accesso casuale (*RAM*). Questo metodo, conosciuto con il nome di ram scraping era già stato oggetto di messe in guardia, segnatamente di comunicati di VISA nel corso dell'estate.[39] Le questioni centrali dell'estrapolazione dei dati e della compromissione iniziale («entry point») hanno ricevuto una risposta soltanto dopo parecchie settimane e in seguito a diverse rivelazioni e prese di posizione. La ditta Target ha inizialmente imputato l'intrusione a un furto di dati di accesso alla rete presso uno dei suoi fornitori. Nel quadro delle rivelazioni successive è stato designato un fornitore in particolare, ossia un'impresa che gestisce il sistema di riscaldamento e di aria condizionata. I dati di accesso sarebbero stati ottenuti in seguito all'invio di e-mail contenenti un malware specializzato nel furto delle password. Le autorizzazioni di cui disponeva questo fornitore avrebbero successivamente consentito ai criminali di accedere al sistema di pagamento per installarvi il malware di intercettazione dei dati.

Questo caso è stato seguito nel mese di gennaio dalla rivelazione di un attacco similare alla catena di empori Neiman Marcus. Anche in questo ultimo caso i dati della striscia magnetica delle carte di credito utilizzate sono stati carpiti immediatamente dopo la loro utilizzazione. In entrambi i casi sembra che si ricorra a metodi prossimi, senza che si possa attualmente affermare che ne siano responsabili i medesimi criminali. Diverse fonti infine fanno stato del fatto che numerosi altri commerci ne sono stati colpiti, senza che essi siano tuttora stati identificati.

La pirateria ai danni di Target, ma anche in altri casi similari, sottolinea i rischi provenienti dall'utilizzazione di carte di credito che funzionano con una semplice striscia magnetica. Questo sistema ancora fortemente diffuso negli USA, beneficia di un livello di sicurezza nettamente inferiore a quello dei sistemi che funzionano con *chip* e *PIN*. I dati della carta di credito possono infatti essere facilmente intercettati. Nella maggior parte dei casi i dati così intercettati sono rivenduti su siti e forum specializzati, nell'intento finale della fabbricazione di carte di carte di credito falsificate.

[38] Le vulnerabilità a livello di POS sono già state tematizzate nel Rapporto semestrale MELANI 2012/2. Rapporto semestrale MELANI 2012/2, capitolo 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (stato: 20 febbraio 2014).

[39] http://usa.visa.com/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf (stato: 20 febbraio 2014).

Un'ulteriore problematica sollevata da questo incidente è quella dei prestatori di servizi che intervengono sulla rete dell'impresa e dispongono di ampi diritti. Come è stato dimostrato nella fattispecie questi ultimi costituiscono altrettanti punti potenziali di entrata per un attacco.

4.5 Seconda scheda SIM e sue ripercussioni

Gli attacchi agli smartphone per accedere ai sistemi di e-banking protetti con *mTAN* sono già stati tematizzati nell'ultimo Rapporto semestrale[40]. Il fatto che siano anche possibili attacchi che sfruttano vulnerabilità organizzative piuttosto che vulnerabilità tecniche è stato dimostrato a fine ottobre 2013. All'epoca circolavano primi rapporti secondo i quali in Germania i truffatori erano riusciti a compromettere mediante una seconda *scheda SIM* (Subscriber Identity Module) applicazioni di e-banking protette con mTAN. A tale scopo i truffatori si sarebbero fatti inviare a un indirizzo qualsiasi una seconda scheda SIM grazie alla quale avrebbero letto il mTAN in arrivo.

La scheda SIM protegge l'autorizzazione dell'utente. La persona in possesso di questa scheda può in linea di massima connettersi alla rete di telefonia mobile in nome dell'utente. A seconda della politica del gestore della rete di telefonia mobile è possibile l'esercizio parallelo di più schede SIM. Se l'offerente di telefonia mobile accetta una sola scheda, le carte di disturbano a vicenda.

A prescindere da queste limitazioni tecniche sussiste nondimeno la questione organizzativa delle misure di sicurezza che il gestore della rete di telefonia mobile applica al momento della consegna della scheda SIM. Dato che per mezzo del telefono mobile si disbrigano con sempre maggior frequenza prestazioni di servizi critiche, anche la sicurezza dei telefoni mobili e quindi pure dei gestori di reti di telefonia mobile occupa maggiormente la ribalta.

4.6 Hackeraggio dell'algoritmo DES e ripercussioni sulle schede SIM

Lo specialista tedesco di crittografia Karsten Nohl ha pubblicato nel luglio del 2013 i primi risultati delle sue ricerche nel campo della sicurezza delle schede SIM. Secondo tali risultati parecchi milioni di schede SIM nel mondo intero sarebbero insufficientemente protette ed esposte a compromissione. Ciò consentirebbe ad esempio una violazione dell'identità dell'utente, intercettazioni o anche manipolazioni di pagamenti disbrigati per il tramite del telefono mobile[41].

Le reti degli offerenti di telefonia mobile comunicano regolarmente con le schede SIM, senza che l'utente se ne accorga. A tale scopo viene utilizzata una tecnologia che consente di accedere a distanza ai dati di una scheda SIM (tecnologia «*Over-the-air*»). In questo modo vengono ad esempio installati gli aggiornamenti e scambiate diverse informazioni. La sicurezza della comunicazione tra la scheda SIM e il gestore della rete è protetta mediante cifratura. Karsten Nohl pone appunto in forse questa cifratura. Concretamente si tratta del «Data Encryption Standard» (DES), sviluppato fin dagli anni Settanta, ma ancora utilizzato in talune applicazioni. L'algoritmo DES è da tempo considerato poco sicuro, in particolare a causa del-

[40] Rapporto semestrale MELANI 2013/1, capitolo 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

[41] https://srlabs.de/rooting-sim-cards/ (stato: 20 febbraio 2014).
http://www.heise.de/security/artikel/DES-Hack-exponiert-Millionen-SIM-Karten-1920898.html (stato: 20 febbraio 2014).

la lunghezza insufficiente della chiave a 56 bit utilizzata. Secondo Nohl è possibile scoprire la chiave crittografica di determinate schede SIM con cifratura DES.

Dopo che è venuto in possesso di questa chiave lo hacker ha la possibilità di lanciare diversi attacchi contro la scheda SIM e il suo titolare. Ricorrendo a questa lacuna di sicurezza Nohl ha hackerato con successo un quarto delle schede SIM testate. Si ritiene che nel mondo intero circa 500 milioni di schede SIM siano esposte a questo rischio. Le schede SIM più recenti – che utilizzano il successore di DES – non sono più attaccabili in questo modo.

La lacuna di sicurezza oggetto di pubblicazione comporta un grave potenziale di danno per gli utenti di schede SIM protette dal metodo DES. Per quanto riguarda il mercato svizzero non esiste alcun pericolo. Secondo le informazioni che MELANI ha ricevuto dalle imprese svizzere di telecomunicazione lo standard DES non viene più utilizzato in Svizzera.

4.7 Sistemi industriali e domestici di controllo

Impianti industriali in rete e installazioni domestiche telecomandate

MELANI ha già rammentato a più riprese i rischi dell'accresciuta messa in rete di apparecchiature di comando di processi fisici nel settore industrie e anche privato[42]. Grazie all'evoluzione tecnica si aggiungono sempre nuove possibilità di accedere a distanza ai sistemi, di fare ricerche sui dati e infine di pilotare le apparecchiature situate dietro di essi. Nel frattempo è divenuto semplice e relativamente buon mercato procurarsi sistemi con funzioni di interrogazione e pilotaggio a distanza oppure di equipaggiare successivamente un impianto esistente con un'interfaccia di comunicazione. Ciò corrisponde sovente ai desideri dei clienti: sulla via della propria casa di vacanze è pratico e comodo poter accendere con un tablet e uno smartphone al riscaldamento o allo scaldacqua oppure verificare se il fornello è spento. Questo vale anche per i custodi di immobili che grazie all'accesso a distanza ai sistemi possono sorvegliare e pilotare la domotica. Anche i proprietari di piccoli impianti idroelettrici o di altri impianti che non sono occupati non stop apprezzano di potere verificare il loro funzionamento ed effettuare determinate parametrazioni dal divano di casa.

Ogni sistema che consente un *accesso a distanza* legittimo può in linea di massima essere oggetto di un accesso non autorizzato, sia direttamente che mediante infiltrazione attraverso un'apparecchiatura autorizzata all'accesso, perché vale come sempre il principio «Tutto ciò che è raggiungibile attraverso la rete è hackerabile»[43]. La messa in rete di sistemi industriali di controllo e il pilotaggio TIC della domotica suscita viepiù l'interesse degli esperti di sicurezza. In questo senso nel corso degli ultimi anni sono state individuate diverse lacune di sicurezza in simili prodotti o al livello della loro implementazione[44].

I diversi sistemi comandabili a distanza svolgono diversi compiti e le eventuali manipolazioni hanno conseguenze diverse per gli interessati: se si spegne uno scaldacqua gli abitanti di un immobile non possono più fare la doccia; l'accensione dell'impianto di illuminazione di uno stadio costa in termini di energia elettrica e di denaro; se viene fermata un catena di produzione industriale si blocca magari tutto l'esercizio, ciò che può avere vaste conseguenze per l'impresa e i suoi lavoratori.

---

[42] Ad esempio: Rapporto semestrale MELANI 2013/1, capitolo 4.5: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

[43] «If you can ping it, you own it!» Kyle Wilhoit, The SCADA That Didn't Cry Wolf, 2013

[44] http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities (stato: 20 febbraio 2014).

Ci si può infine immaginare un scenario nel quale numerose apparecchiature di consumo sono accese e spente in maniera coordinata, con la conseguenza di pregiudicare la stabilità della rete elettrica. Oltre che alle funzioni e alla convivialità di una soluzione di accesso a distanza occorre pertanto anche porre attenzione alla sua protezione da manipolazioni non autorizzate.

Le TIC dovrebbero invero supportare anzitutto processi aziendali. Ma il loro uso comporta sempre ripercussioni fisiche e procedurali che vanno prese in considerazione.

MELANI ha pubblicato nell'ottobre del 2013 un elenco di controllo per la protezione dei sistemi industriali di controllo[45].

«Good Practices» dell'OSCE per diminuire i rischi informatici nel settore dell'energia

L'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) ha pubblicato una guida destinata agli Stati e alle imprese energetiche private, relativa alle modalità di protezione delle loro infrastrutture da possibili attacchi di terrorismo informatico[46]. Sebbene il titolo del documento suggerisca un ambito relativamente ristretto, la guida introduce alla tematica a partire da una vasta prospettiva e raccomanda misure generali che possono essere applicate indifferentemente ad altri settori industriali e comportano un effetto di prevenzione e di incremento della resilienza non soltanto nei confronti degli attacchi terroristici. L'OSCE si adopera a favore di un promovimento della consapevolezza (Awareness Rising) attraverso corsi di formazione, a favore di un'accresciuta cooperazione di tutti i partecipanti e di uno scambio di informazioni. Queste misure sono diffuse da più parti e vengono ora suggerite per il settore energetico non nucleare. L'energia nucleare è unicamente stata esclusa per non provocare un conflitto di competenze con i regolatori corrispondenti – le raccomandazioni dell'OSCE sono nondimeno di rilievo anche per gli esercenti di centrali nucleari.

È nella responsabilità comune di tutti i partecipanti garantire la sicurezza di approvvigionamento in un'Europa dove l'approvvigionamento è tuttora fortemente frammentato e sempre più in rete. Molti altri settori dipendono dall'approvvigionamento energetico, in particolare dall'elettricità. Ciò fa apparire l'approvvigionamento energetico particolarmente critico. A questa circostanza si aggiunge lo sviluppo di reti elettriche intelligenti, che accrescono ulteriormente i rischi; oltre a fornire nuove comode possibilità agli approvvigionatori i servizi supplementari di misura e di regolazione pilotati dalle TIC offrono anche nuove superfici di attacco ad attori malevoli, che per questo tramite possono intervenire nell'approvvigionamento energetico. In ambito di approvvigionamento energetico occorre pertanto prendere debitamente in considerazione la sicurezza delle componenti «intelligenti».

4.8 Il conflitto in Siria – Guerra dell'informazione 2.0

La Syrian Electronic Army (SEA) è un gruppo di hacker che sostengono il regime vicino al presidente siriano Bashar al-Asad. I rapporti tra la SEA e i dirigenti siriani non sono tuttavia chiari. Secondo alcune dichiarazioni della SEA essi non fanno parte del Governo, né ne sono sostenuti. La SEA si compone piuttosto di hacker patrioti che combattono contro le relazioni sulla guerra civile siriana che ritengono false.

[45] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=de (stato: 20 febbraio 2014).

[46] «Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace», http://www.osce.org/atu/103500 (stato: 20 febbraio 2014).

Nel corso dell'ultimo semestre la SEA ha soprattutto attaccato siti Web di informazione (New York Times, BBC News, Al-Jazeera e altri) e ha potuto tra l'altro compromettere i conti Twitter di agenzia di stampa come Reuters e Associated Press (AP) nell'intento di diffondere la propria propaganda o notizie volutamente false[47].

Già oltre duemila anni fa il poeta greco Eschilo annotava: «La prima vittima della guerra è la verità». Con l'avvento di Internet e in particolare dei media sociali la condotta informatica della guerra si è «democratizzata». Non è più necessario obbligatoriamente l'intervento dello Stato per fare circolare nel mondo informazioni (false o corrette) – bastano soltanto un collegamento Internet e una storia da poter diffondere in maniera virale.

I conti dei media sociali e gli altri canali di informazione che autenticano l'accesso e la successiva diffusione dell'informazione con i soli nomi di utente e password possono essere infiltrati in maniera relativamente semplice con metodi come lo *Spear-Phishing*. I principali canali e piattaforme di informazione devono pertanto essere protetti nella misura del possibile con un'*autentificazione a due fattori*.

Oltre alle misure tecniche occorrerebbe inoltre riflettere e definire preliminarmente come e attraverso quali canali una notizia falsa può essere smentita in maniera possibilmente efficace, rispettivamente rettificare, per poter in tal modo impedire una maggiore confusione e altre ripercussioni.

4.9 Quando i DDoS distraggono da altri attacchi

Una tendenza apparsa nel corso dell'ultimo anno è quella di *attacchi* di distributed denial of service (*DDoS*) di intensità relativamente debole, utilizzati come tentativi di diversione in vista di altri attacchi. Questo fenomeno è stato riportato da diversi esperti e articoli di stampa e si basa in particolare su casi relativi a banche statunitensi. Mentre i responsabili della sicurezza erano occupati un attacco DDoS al sito Web dell'impresa o al suo portale di e-banking, un altro attacco più serio era in atto simultaneamente. Di fatto gli attacchi erano diretti contro il sistema di giro della banca e non i conti di persone particolari. L'analisi dell'evento è resa difficile dalla grande quantità di dati di log.

Sebbene debba essere trattato come tale, un attacco DDoS dovrebbe anche incitare a elevare il livello di attenzione a fronte della potenzialità di altri attacchi. Ciò è vero in particolare se l'attacco è di intensità relativamente debole.

4.10 Hacker e contrabbandieri sotto il medesimo tetto

Tra il 2011 e il 2013 sono scomparsi diversi container marittimi dal porto di Anversa. Dalle inchieste delle autorità di perseguimento penale risulta che i container legali sono stati utilizzato abusivamente da criminali per contrabbandare droghe. A tale scopo essi si sono introdotti nei sistemi TIC dell'impresa di container per rintracciare le ubicazioni dei container interessati e derubarli prima che i proprietari legittimi potessero ritirarli.

La penetrazione originaria nei sistemi di informazione è stato operata mediante semplici e-mail di «*Social Engineering*» che inducevano gli impiegati della ditta ad aprire gli attachment

[47] Cfr. in merito il capitolo 4.4 dell'ultimo Rapporto semestrale MELANI 1/ 2013: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

e quindi all'installazione di programmi di spionaggio. Dopo la scoperta di questi eventi le misure di sicurezza (TIC) dell'impresa di container sono state rafforzate. Gli autori si sono successivamente procurati l'accesso fisico agli uffici installandovi hardware manipolato per poter continuare ad accedere alle informazioni necessarie – tra l'altro i codici di sicurezza che consentono ai conducenti di accedere all'area e di ritirare determinati container.

Numerosi settori sono ormai impensabili senza un'infrastruttura informatica che supporti la pianificazione e l'esecuzione delle attività aziendali. In particolare non è più possibile portare a termine compiti logistici esigenti senza sistemi informatici. Inoltre molte imprese del settore della logistica auspicano di poter appurare in ogni momento l'ubicazione attuale delle forniture e dei mezzi di trasporto. Queste informazioni che rendono possibile uno sfruttamento delle risorse e una fornitura di prestazioni più efficienti, offrono simultaneamente possibilità di azion criminali mirate. Occorre altresì considerare che le manipolazioni di queste informazioni possono pregiudicare l'andamento regolare delle attività. I sistemi TIC costituiscono anzitutto un ulteriore mezzo di sostegno di determinati iter aziendali. A livello di direzione è in questo senso determinante la comprensione delle ripercussioni fisiche e procedurali

Come su ogni mercato anche sul mercato clandestino si delinea un'accresciuta specializzazione e professionalizzazione. Questa tendenza si osserva da alcuni anni. Nel caso degli hacker non si tratta più di giovani curiosi che desiderano testare i limiti del possibile, ma sempre più di tecnici sperimentati che offrono le loro capacità in un intento di profitto. Anche nella fattispecie gli hacker sono stati presumibilmente reclutati via Internet dai contrabbandieri. Non esiste alcuna prestazione di servizi che non possa essere acquistata sul mercato clandestino.

4.11 Il Parlamento dell'UE adotta pene più severe nei confronti dei cibercriminali

In futuro i cibercriminali saranno esposti a pene più severe nell'Unione europea. Adottando lo scorso 12 agosto 2013 la direttiva 2013/40/UE EU, il Parlamento europeo ha deciso l'introduzione di pene più severe in caso di attacchi contro i sistemi di informazione. L'obiettivo è tra l'altro un'armonizzazione delle leggi e delle pene negli Stati membri perché gli attacchi sono frequentemente transfrontalieri e perché questi atti sono puniti in maniera diversa negli Stati dell'UE. L'uniformazione del quadro penale istituisce la base indispensabile alla cooperazione in ambito di perseguimento penale.

La direttiva prevede pene detentive di almeno due anni. In questo senso ad esempio la creazione di *reti bot* è punita con almeno tre anni di carcere. I criminali responsabili di attacchi a infrastrutture critiche come centrali elettriche, sistemi di trasporto o reti governative sono passibili di almeno cinque anni di carcere. Lo stesso dicasi se l'attacco non è perpetrato da una sola persona ma da un'associazione criminale o se vengono provocati gravi danni.

La direttiva istituisce inoltre compiti per le autorità di polizia e giudiziarie. In questo senso gli Stati membri dell'UE devono scambiarsi informazioni sugli attacchi informatici per garantire l'esercizio delle reti. Per migliorare lo scambio di informazioni sugli attacchi informatici i servizi competenti devono reagire entro otto ore alle richieste urgenti.

Questo nuovo corso persegue anzitutto l'obiettivo di un'armonizzazione conforme in fatto di approccio delle basi di diritto penale in ambito di criminalità informatica negli Stati dell'UE. Dalla prassi è emerso che il perseguimento penale in caso di criminalità informatica transfrontaliera si scontra con barriere formali riconducibili ai diversi approcci della procedura penale. L'attuazione in futuro della nuove comminatorie di pena dipenderà per l'essenziale

dalle modalità di recepimento di questo quadro comune nella procedura penale degli Stati membri.

5 Tendenze / Prospettive

5.1 Internet al bivio o business as usual?

Con il proseguimento della pubblicazione dei documenti relativi alla prassi della NSA e di altri servizi segreti nel corso degli ultimi mesi si sono anche elevate voci per esprimersi sul futuro di Internet come tale. Come ci si aspettava le diverse valutazioni vanno in tutte le direzioni: in questo senso ad esempio l'esperto Bruce Schneier rammarica in un suo articolo il tradimento fondamentale di Internet e dei valori di base che rappresenta.[48] Schneier sottolinea anche il paradosso che proprio le azioni degli USA – l'anima del mondo libero – confortano le intenzioni di quegli Stati totalitari che propugnano da sempre una nazionalizzazione di Internet. Il timore di una «balcanizzazione crescente di Internet» ha indotto ad esempio Vinton Cerf, il vicepresidente di Google, a evocare fin da ora il declino di Internet come lo conosciamo.[49] Per le imprese non sarà più economicamente interessante partecipare a Internet se si considerano il sempre maggiore isolamento nazionale e l'eterogeneizzazione che va di pari passo con tale isolamento. Voci critiche provengono anche dalle cerchie di chi sostiene che Internet è l'invenzione per eccellenza della democrazia di base, apportatrice di libertà. Ora essi considerano Internet come una perfetta piattaforma di sorveglianza e si rimproverano la loro propria ingenuità per non avervi mai intravisto qualcosa di diverso.

Simultaneamente Internet sembra tuttora estremamente vivo e, almeno a breve termine, nulla dovrebbe cambiare a questa situazione. Le attività di singoli servizi segreti divenute note in seguito ai documenti di Snowden spingono perlomeno alla conclusione che la fiducia in Internet è andata proprio definitivamente persa a diversi livelli.

Ne emergono anche i problemi eclatanti che comporta una simile istituzione transnazionale e alla quale ogni individuo e ogni Stato può partecipare e operare come preferisce e come lo consentono le leggi nazionali, senza dover prendere in considerazione le ripercussioni globali. È contrario al principio della buona fede e a tutta una serie di altre normative nazionali il fatto che gli standard globali di sicurezza a livello tecnico possano essere modificati a propria discrezione da un solo Paese o che le proprie imprese di quel Paese siano costrette da misure coercitive segrete a fornire informazioni in grande stile per accedere ai dati in maniera possibilmente semplice e capillare. Ciò consente ai funzionari dello Stato di raggiungere i loro obiettivi in maniera un po' più semplice e comoda. Apparentemente ci si scorda che nel procacciamento di informazioni e di dati personali da parte dello Stato l'avidità unita alla pigrizia costituisce pur sempre un approccio ai limiti da un punto di vista liberale e democratico.

Nel caso soprattutto delle imprese del settore IT ciò significa che esse operano invero in un contesto globale, ma che sono in definitiva esposte a normative nazionali diverse e non sempre corrispondenti. Ciò non riguarda soltanto le grandi imprese che operano nel settore

[48] http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying (stato: 20 febbraio 2014).

[49] http://www.tagesanzeiger.ch/digital/internet/GoogleVize-warnt-vor-Untergang-des-Internets/story/12499111 (stato: 20 febbraio 2014).

IT. Una delle tematiche principali deve pertanto consistere nell'abbordare per l'appunto questa assenza di consenso nei confronti dei principi fondamentali nei rapporti con Internet e con gli attori partecipanti.

A questi quesiti è anche abbinato il ripristino della fiducia proprio in seno alla comunità IT. In altri termini la fiducia e gli scambi internazionali tra quegli organi di sicurezza IT anzitutto orientati a proteggere le reti, i prodotti e le applicazioni. In questo contesto costituisce ad esempio una complicazione il fatto che negli Stati Uniti l'organismo preposto agli standard di sicurezza, il «Directorate for Information Assurance», sia sottoposto al capo del NSA, che a mente del suo elenco degli oneri non dovrebbe certo interessarsi esclusivamente di prodotti IT sicuri e di standard robusti. Anche il fatto che i CERTs responsabili per lo scambia internazionale d'informazioni per la protezione delle reti dipendano da unità di Signal Intelligence offensive, conforta solo parzialmente i CERTs degli altri stati sulle intenzioni di questo partner. Tuttavia è proprio questa Community tecnica e il suo sistema transnazionale di scambio di informazioni – sistema che deve assumere una parte notevole dei compiti – che deve riordinare Internet, rispettivamente la sicurezza delle sue componenti, in maniera tale da evitare ulteriori isolamenti e da ripristinare la fiducia di base nei confronti di Internet.

È eccessivo decretare la morte Internet nel suo quasi venticinquesimo anno di esistenza. Tuttavia il ripristino della fiducia di base in Internet e della fiducia reciproca degli attori rilevanti in ambito di sicurezza IT non è affatto un compito banale. Non comporta neppure risposte semplici la soluzione del quesito fondamentale di come si possa eludere il fatto che l'applicazione della legislazione nazionale in un sistema transnazionale provochi de facto sempre una ripercussione extraterritoriale dell'applicazione del diritto. Questo dibattito dovrà soprattutto essere esteso a tutti i livelli, dall'ottica di politica di sicurezza fino agli organismi Multi-Stake-Holder che si occupano di standard e di condizioni e in seno ai quali prende posto come principale interessato anche l'economia.

Sono in ogni caso opportuni un inventario e un ritorno all'idea di base che ha rappresentato Internet: anzitutto un sistema decentralizzato e altamente resistente di trasmissione di informazioni. La sicurezza e la confidenzialità di queste informazioni si situavano, si situano e si situeranno anche in futuro nella responsabilità di coloro che collocano queste informazioni e dati su Internet.

5.2 Bitcoin - il successo e il prezzo del successo

Funzionamento

Bitcoin è una moneta elettronica decentralizzata, ciò che significa che il suo funzionamento non dipende da nessun emittente centrale. Questo aspetto la differenzia dalle divise tradizionali, ma anche da numerose altre monete elettroniche.

Nel Bitcoin coabitano due diversi tipi di attori principali. Gli utenti sono rappresentati dal loro portamonete, che consiste in un paio di chiavi crittografiche pubblica/privata. Si può considerare per analogia la chiave pubblica come il numero di conto verso il quale è possibile trasferire denaro. La chiave privata consente di firmare una transazione, ovvero di effettuare un pagamento.

Affinché il pagamento sia effettivo occorre ancora validarlo. È nel quadro di questo processo che interviene la rete dei «miner», che sono i secondi maggiori attori del sistema. Da un punto di vista concreto questi ultimi partecipano alla costituzione di «block chain», il cuore del funzionamento del Bitcoin. Si tratta di una sorta di libro contabile che raggruppa tutte le transazioni, consultabile da parte di tutti gli utenti. Questo processo di validazione, denominato «mining» è volto a confermare le transazioni in attesa includendole in un «block». La valida-

zione di un «block» necessita la soluzione da parte di un «miner» di una prova di lavoro (proof of work). Questa fase richiede una forte potenza di calcolo ed è rimunerata in Bitcoin, circostanza che determina un aumento della massa monetaria in circolazione. L'integrità della «block chain» è centrale dato che per autorizzare una nuova transazione deve essere possibile farle corrispondere un'entrata anteriore registrata dal mandante. In assenza di una simile traccia il suo utilizzatore potrebbe infatti firmare una transazione totalmente irrealistica.

Esistono tre modi principali di procurarsi Bitcoin: partecipando al «mining», facendo remunerare una prestazione in Bitcoin oppure acquistando Bitcoin su una piattaforma di scambio che consente di scambiarli e con divise «classiche». I Bitcoin possono essere successivamente utilizzati nei commerci che utilizzano questo modo di pagamento. Il carattere anonimo delle transazioni che utilizzano Bitcoin è sovente evocato e merita di essere precisato. L'utente è infatti teoricamente anonimo perché è unicamente identificato dalla detenzione di una *chiave crittografica*. Diversamente da quanto esiste nel sistema bancario classico, le transazioni sono invece pubbliche.

Sfide in ambito di sicurezza

La popolarità crescente del Bitcoin solleva numerose problematiche, in particolare a livello di sicurezza, ma anche per quanto riguarda lo statuto legale e la regolamentazione di queste divise.

Diversi avvenimenti recenti dimostrano chiaramente che i Bitcoin e i loro utenti sono divenuti dei bersagli interessanti per i criminali e che variano i metodi utilizzati finora per acquistare fraudolentemente i Bitcoin. Diversi attacchi e incidenti in ambito di sicurezza sono stati rilevati nel corso degli ultimi mesi, con livelli di complessità e bersagli variabili.

La chiave privata e per il suo tramite il proprietario del portamonete sono generalmente il bersaglio più attraente per gli aggressori. Infatti la confidenzialità del portamonete poggia esclusivamente su questa chiave e la sicurezza della sua conservazione è centrale. Numerosi utenti sono già stati oggetto di attacchi diretti contro questo elemento. I servizi Web propongono inoltre di conservare la chiave privata dei lori clienti. In considerazione della centralizzazione dei portamonete e delle somme importanti che essi possono rappresentare, questi siti sono divenuto bersaglio prioritario di attacchi. Uno di questi servizi, input.io, è ad esempio stato vittima nel mese di luglio del 2013 di un furto di Bitcoin per un valore di 1.2 milioni di dollari.

Le piattaforme di scambio costituiscono un altro bersaglio potenziale. In dicembre il mercato di cambio Bitcoin Svizzera ha ammesso di essere stato vittima di un attacco. L'attacco in questione è stato coronato dal successo nonostante un modus operandi estremamente poco perfezionato e principalmente inspirato al «*social engineering*». Nella fattispecie i pirati si sono indirizzati al fornitore del conto e-mail della piattaforma, facendosi passare per Bitcoin Svizzera. Essi hanno successivamente richiesto il cambiamento delle password del conto di Bitcoin Svizzera, richiesta alla quale il fornitore ha dato seguito. Il responsabile di Bitcoin Svizzera ha da allora cambio fornitore, ma non ha precisato se i pirati hanno utilizzato gli identificanti per commettere attività delittuose. Sono stati parimenti osservati attacchi di altro genere diretti anch'essi contro borse di scambio. Una tendenza marcata è segnatamente quella di attacchi DDoS. In alcuni casi gli aggressori hanno richiesto il pagamento di un riscatto contro la cessazione dell'attacco, questo è un secondo modus operandi conosciuto. Ulteriori attacchi di questo genere sembrano avere perseguito altri obiettivi. Sono ad esempio state segnalate alcune manovre volte a destabilizzare il mercato, spingendo il corso del Bitcoin al ribasso per poterlo acquistare successivamente a un miglior prezzo. La volatilità del corso del Bitcoin e le possibilità di manovre speculative inerenti sono qui al centro delle preoccupazioni.

Un ultimo angolo di attacco consiste nel prendere di mira i guadagni generati dall'attività di «mining». All'inizio del 2014 è stato rintracciato su diversi siti del gruppo Yahoo un malware trasmesso mediante le pubblicità (ads). Quest'ultimo presenta la particolarità di sfruttare la potenza di calcolo dei computer che ne sono vittima per fare loro effettuare un lavoro di «mining» all'insaputa del loro proprietario e quindi di generare Bitcoin.

A prescindere da questi attacchi Bitcoin è stato regolarmente evocato a motivo della sua utilizzazione nel quadro di transazioni illegali. Bitcoin è segnatamente ampiamente utilizzato per effettuare transazioni su piattaforme che offrono prodotti illegali, come Silk Road, una piattaforma di e-commerce, utilizzata per attività illegali (mercato nero).

Queste diverse sfide in ambito di sicurezza sottolineano ancora una volta il grande opportunismo dimostrato dai criminali che operano su Internet. Al successo di un servizio oppure, come nella fattispecie, di una modalità di pagamento corrispondono in genere molto rapidamente attacchi su misura. A livello di utente occorre essere coscienti di questo rischio, del valore dei Bitcoin e quindi della necessità di proteggerlo. Ciò avviene anzitutto attraverso una conservazione sicura. A questo livello si raccomanda di conservare la chiave crittografica privata su un supporto elettronico, senza collegamento a Internet o su carta (Paper Wallet). La sicurezza generale dell'apparecchiatura e segnatamente la sua protezione contro le infezioni rimane di importanza centrale.

L'organizzazione e la regolamentazione di uso dei Bitcoin costruiscono aspetti che dovrebbero ancora conoscere importanti sviluppi. La popolarità di questa moneta e le preoccupazioni quanto alle possibilità di abuso o ancora la sua estrema volatilità incitano attualmente gli Stati a interessarvisi e più precisamente a prospettarne delle regolamentazioni. In questo senso la Germania ha accordato uno statuto ufficiale di «moneta privata» al Bitcoin. In Svizzera i due ultimi mesi dell'anno hanno visto tre parlamentari interessarsi al Bitcoin e più precisamente ai suoi rischi e alle possibilità di offrirgli uno statuto legale.

5.3 Il ruolo dell'informatica nei conflitti

La componente informatica svolge nel frattempo un ruolo in numerosi conflitti, come lo mostra ad esempio la Syrian Electronic Army nel conflitto in Siria [50]. In questo contesto si osservano soprattutto propaganda e disinformazione, ma anche attacchi diretti contro le infrastrutture. Se ne citano volentieri come esempio gli attacchi DDoS ai danni dell'Estonia, gli attacchi DDoS contro banche statunitensi, come pure gli attacchi in Corea del Sud e in Corea del Nord. Ogniqualvolta si utilizzano i termini di guerra informatica o di terrore informatico, circostanza che sembra inopportuna in considerazione dei danni effettivamente arrecati. In caso di attacco terroristico o di guerra si pensa inevitabilmente al panico, alla paura e a feriti o morti. Gli attacchi informatici hanno avuto finora effetti ben diversi: segnatamente crash di sistemi, inconvenienti e perdite di denaro.

Ricorso ad attacchi informatici, in particolare sotto la soglia di conflitto

La storia insegna che si ricorre agli attacchi informatici quando devono essere eseguite operazioni mirate che si situano al di sotto della soglia di conflitto e che, se sono eseguite in maniera convenzionale, possono provocare gravi discordie tra gli Stati. Ne è un esempio tipico il ricorso al software nocivo Stuxnet che perseguiva l'obiettivo di perturbare le centrifughe degli

[50] Presente Rapporto semestrale MELANI 2013/2, capitolo 4.8, nonché Rapporto semestrale MELANI 2013/1, capitolo 4.4: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (stato: 20 febbraio 2014).

impianti iraniani di arricchimento dell'uranio. Un simile attacco condotto con mezzi convenzionali avrebbe presumibilmente provocato un serio conflitto nella regione.

Numerosi attori e motivazioni

La molteplicità degli attori e delle motivazioni rende ancor più difficile una valutazione. Un attacco DDoS a una banca può avere un retroscena criminale (estorsione) oppure un retroscena ideologico, come ad esempio i diversi attacchi di Anonymous ai danni delle banche nel corso degli ultimi anni. Ma è anche ipotizzabile un retroscena statale quando si tenta ad esempio di indebolire l'intero sistema finanziario attraverso un attacco.

Rispondere alla domanda dell'attribuzione sarà ancora più difficile in futuro, perché l'enorme potenziale di persone con capacità informatiche – provenienti tra l'altro anche da cerchie criminali – viene individuato da diversi Stati e sfruttato per i loro obiettivi. In questo senso è possibile assegnare ed eseguire azioni senza che lo Stato debba esporsi alla minaccia di un'attribuzione

Attacchi futuri

Il pericolo di attacchi informatici con un grave potenziale di danno è quindi ridotto? Esiste ovviamente la possibilità che vengano attaccati sistemi particolarmente critici, il cui crash avrebbe conseguenze notevoli. Siffatti attacchi esigono tuttavia almeno conoscenze tecniche e insider approfondite, come pure un grande dispendio. Nel caso dei sistemi critici è poi particolarmente elevata l'attenzione accordata alla sicurezza. Non sono perciò esclusivamente i rischi di attacchi informatici che dovrebbero incitare a una riflessione, ma sopratutto il fatto che i sistemi divengono sempre più complicati e vengono viepiù messi in rete. Da ciò discende che i collegamenti e le dipendenze non sono più distinguibili in modo semplice. Un problema o una perturbazione può quindi provocare ripercussioni imprevedibili. Non è nemmeno necessario che si tratti di un attacco – anche le avarie possono provocare ripercussioni di maggiore portata e il debugging dei sistemi complessi esige sovente un certo tempo.

5.4 Individuazione dei virus nel 21° secolo – Cosa farà seguito ai programmi antivirus basati sulla firma?

Il primo *virus* è stato osservato fin del 1971. Si trattava di Creeper, che si era propagato all'intermo della Advanced Research Projects Agency Network, *ARPANET*, il predecessore dell'attuale Internet. Sebbene all'epoca non venisse ancora utilizzato il concetto di «virus» è possibile designare «The Reaper» come primo antivirus della storia. Nel frattempo esistono oltre venti soluzioni commerciali antivirus e si è sviluppata una notevole industria antivirus. Ma dove si situa al momento questa industria e quali possibilità di difesa offrono i prodotti antivirus attuali?

Il rapporto di test pubblicato nel 2012 da «AV-Comparatives.org» rivela che la percentuale di software nocivo bloccato con successo, rispettivamente delle pagine Web nocive bloccate, è sorprendentemente elevata. Il tasso di individuazione raggiunge in questo caso oltre il 90%:

Whole Product Dynamic "Real-World" Protection Test – (March-June) 2012 www.av-comparatives.org

Summary Results (March-June)

Test period: March – June 2012 (2159 Test cases)

	Blocked	User dependent	Compromised	PROTECTION RATE [Blocked % + (User dependent %)/2][4]	Cluster[5]
BitDefender	2150	-	9	99,6%	1
G DATA	2147	1	11	99,5%	1
Kaspersky	2146	2	11	99,4%	1
Qihoo	2143	6	10	99,4%	1
BullGuard	2131	21	7	99,2%	1
F-Secure	2135	10	14	99,1%	1
Avast	2110	28	21	98,4%	2
ESET	2117	1	41	98,1%	2
AVIRA	2107	13	39	97,9%	2
Sophos	2112	-	47	97,8%	2
Trend Micro	2108	-	51	97,6%	2
AVG	2103	6	50	97,5%	2
GFI	2102	-	57	97,4%	2
Panda	2097	-	62	97,1%	2
eScan	2094	-	65	97,0%	2
PC Tools	2024	126	9	96,7%	2
Tencent	2052	32	75	95,8%	3
Fortinet	2046	-	113	94,8%	3
McAfee	2041	6	112	94,7%	3
AhnLab	1999	-	160	92,6%	4
Webroot	1963	1	195	90,9%	4

Figura 3: Rapporto di test dell'«AV-Comparatives.org»

Da una valutazione in base a questa statistica sembra che i programmi antivirus individuino ed eliminino la maggior parte dei virus. Le condizioni del test erano però state specialmente stabilite. Premesso che si doveva simulare un contesto reale si era partiti dall'ipotesi che il 40 – 50 % degli indirizzi Web integrati nell'analisi conducesse direttamente a un software nocivo, mentre il rimanente 50 – 60 % portasse a un cosiddetto *Exploit Pack*. Diversamente dal software nocivo che perviene direttamente al computer, gli Exploit Pack possono essere verificati e individuati relativamente bene dai prodotti antivirus. L'elevato tasso di successo si spiega con queste ragioni.

Un test analogo con condizioni statistiche condotto dal CRDF Threat Center[51], un'agenzia pubblicitaria francese senza scopo commerciale, e nel cui contesto il codice nocivo è stato analizzato esclusivamente in funzione della sua firma digitale, mostra invece un'immagine differente. Esistono effettivamente programmi antivirus che hanno riconosciuto come nocivo oltre il 70% del codice analizzato. Altri prodotti invece hanno individuato il software nocivo nel solo 1 – 3 % dei casi. Secondo questo studio il tasso medio di individuazione è del 33 %.

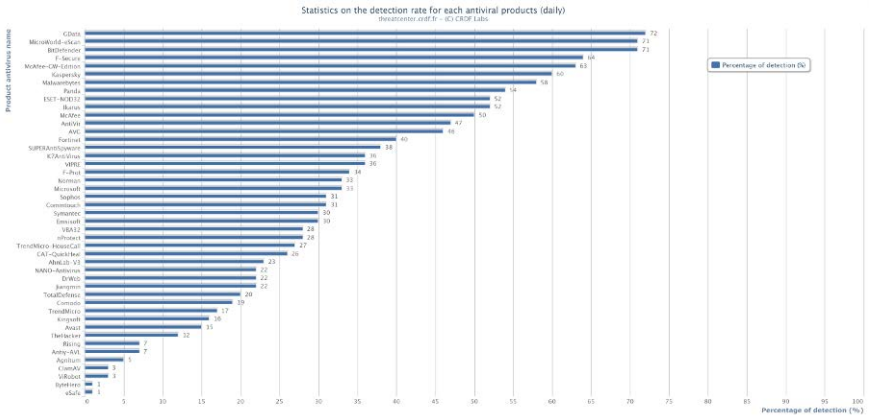


Figura 4: Rapporto di test del «CRDF Threat Center

[51] https://threatcenter.crdf.fr/?Stats (stato: 20 febbraio 2014).

Quale è la realtà nel mondo criminale e in particolare nel settore della criminalità economica?

Per evitare di essere scoperti dai programmi antivirus i criminal spacchettano sovente il malware più volte al giorno. Nel contesto di questa operazione il codice che vi è celato rimane identico, ma viene combinato in maniera tale da presentarsi come nuovo verso l'esterno per non essere individuato dai software antivirus. I criminali utilizzano al riguardo speciali piattaforme che verificano quanti e quali programmi antivirus sono in grado di individuare il software nocivo nel suo nuovo imballaggio. Diversamente dalle offerte presentate dai fornitori di servizi di sicurezza[52], nel caso delle piattaforme utilizzate dai criminali si accerta meticolosamente che nessuna informazione relativa a questi nuovi virus pervenga ai produttori di antivirus.

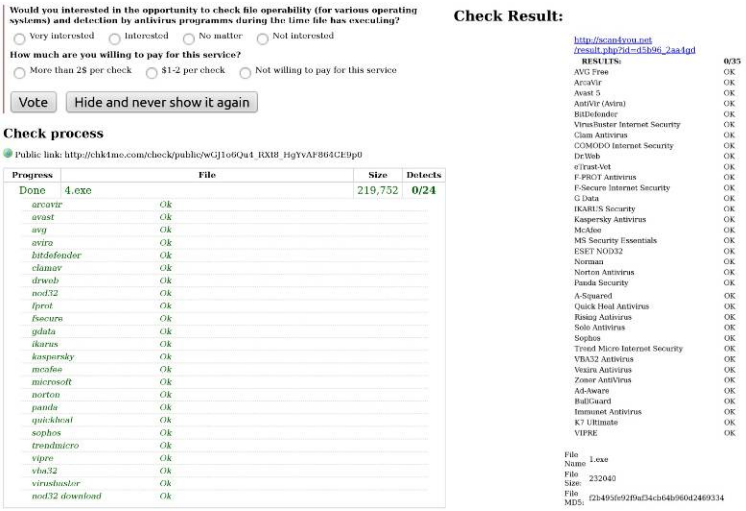


Figura 5: Esempio di un tool di controllo antivirus dei criminali. Se accanto al prodotto antivirus figura un «ok» ciò significa che il codice nocivo non è stato individuato come virus. Se invece un prodotto antivirus ha riconosciuto il codice come nocivo il criminale impacchetterebbe nuovamente il software nocivo.

Nel caso di così tante varianti di virus e di imballaggi di programmi è sempre più difficile per i produttori di antivirus identificare il software con il solo ausilio della sua firma. Anche se le condizioni minime necessarie alla sicurezza di base (sistema aggiornato, *firewall* e software AV) rimangono valide, queste misure non sono più in grado di garantire una protezione al 100 %.

Efficienza solo nel caso di software nocivo molto diffuso

L'efficienza dei prodotti antivirus si limita in particolare ai software nocivi usuali molto diffusi. Nel caso degli attacchi mirati , che riguardano soltanto una parte minima dei clienti, l'individuazione diviene tuttavia problematica e praticamente impossibile. Mikko Hypponen, capo ricercatore presso F-Secure afferma in merito a Duqu, Flame, Gauss e Co.: «All of us had missed detecting this malware for two years, or more. That's a failure for our company, and for the antivirus industry in general»[53].

Anche se in genere gli attacchi mirati non sono diretti contro utenti usuali, nel caso di Stuxnet si è osservato che nell'ambito di simili azioni vengono infettate anche apparecchiature che non hanno niente a che fare con l'obiettivo vero e proprio, rispettivamente con la vittima potenziale. Nell'ambito della criminalità economica esiste pure la tendenza a effettuare attacchi

52 Ad esempio Virustotal: http://www.virustotal.com (stato: 20 febbraio 2014).

53 http://www.f-secure.com/weblog/archives/00002376.html (stato: 20 febbraio 2014).

di miniore entità sfruttando lacune di sicurezza sconosciute e con software nocivo appositamente impacchettato per un determinato scopo per rimanere sotto il radar dei prodotti antivirus.

Si richiedono nuove misure

Ci si deve pertanto chiedere quali ulteriori misure siano necessarie per accrescere il grado di sicurezza affinché possano essere individuati anche attacchi più piccoli e mirati. Numerose ditte, soprattutto di grandi dimensioni, ricorrono già oggi ai più diversi sistemi supplementari per individuare e bloccare anomalie e traffico Internet sospetto. Al riguardo sono richiesti sistemi intelligenti di individuazione che analizzano il traffico sulle reti aziendali e riconoscono le deviazioni rispetto alla «media». Ai firewall e ai software antivirus si accompagnano sistemi di individuazione di attacchi (*Intrusion Detection System*, IDS), liste bianche e *liste nere* per filtrare il traffico di rete, la sorveglianza (monitoring) della rete o addirittura la sorveglianza dei comportamenti di singoli computer.

Un ulteriore aspetto è costituito dalla tracciabilità. Nell'ipotesi che una volta o l'altra un software nocivo (mirato) si dovesse introdurre nella rete aziendale è molto importante poter ricostruire attraverso quale percorso esso sia penetrato nella rete aziendale e quali altri computer e server siano coinvolti. È l'unica opportunità di eliminare completamente il software nocivo dalla rete. Come dimostrato da attacchi precedenti tra la penetrazione del software nocivo nella rete e il momento della sua scoperta possono passare alcuni mesi o addirittura anni[54]. Va pure aperta una discussione sulla durata di conservazione dei *dati di log*.

Un'ulteriore conoscenza acquisita nel corso degli anni è che le sole misure tecniche non bastano. In definitiva è sempre il collaboratore che dispone della possibilità più efficiente di individuare un attacco e di reagirvi correttamente. Al riguardo una formazione e sensibilizzazione regolare dei collaboratori è di importanza determinante. È altresì importante la creazione di un servizio al quale i collaboratori possano comunicare gli eventi sospetti e dove possano anche essere presi sul serio.

Necessità di intervento nel caso delle piccole imprese

È soprattutto nel caso delle piccole imprese che esiste una necessità di intervento a livello di misure supplementari di difesa contro gli attacchi informatici. Queste misure sono sovente insufficienti contro siffatti attacchi mirati. Si tratta sovente di imprese di nicchia che hanno investito un capitale notevole nei settori ricerca e sviluppo e che possono quindi divenire il bersaglio di possibili attività mirate di spionaggio. Sono soprattutto queste imprese che dovrebbero introdurre sistemi di sicurezza che non poggino esclusivamente sul software antivirus. Ci si scorda forse che i costi di implementazione di misure di sicurezza vanno raffrontati al rischio di ingenti perdite in caso di attacco riuscito.

Difficoltà di attuazione in ambito privato

Le misure descritte qui sopra non possono essere riportate sulle persone private. In un simile caso soluzioni ampliate e adeguate di sicurezza sono troppo dispendiose. Mancano inoltre il tempo e/o il know-how tecnico. Come deve dunque comportarsi l'utente normale di un computer e quali misure può adottare?

[54] Verizon: Data Breach Investigations Report 2012, figura 40, disponibile su: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf (stato: 20 febbraio 2014).

In futuro l'utente privato dovrà esigere dal proprio provider un collegamento Internet «pulito», anche se ciò dovesse comportare dei costi. Al riguardo il provider potrebbe eseguire a livello centrale per tutti i clienti le misure di cui qui sopra e offrire loro in tal modo una protezione supplementare. Attualmente il cliente non esige affatto l'aspetto sicurezza e, inversamente i provider non fanno pubblicità per il criterio sicurezza. A prescindere dal costo il criterio principale nella scelta di un collegamento Internet è in genere la sola velocità. Ciò (dovrà) cambiare in futuro.

5.5 Attacchi ai router domestici

I *router domestici* comportano tuttora configurazioni insicure o lacune di sicurezza. Mentre gli apparecchi più moderni possono essere aggiornati automaticamente dei provider, ciò non ne è sempre il caso degli apparecchi più vecchi.

Configurazione per difetto insicura (impostazioni standard o di fabbrica)

I servizi che possono essere utilizzati abusivamente sui router domestici per effettuare attacchi DDoS costituiscono un problema che va attualmente preso molto sul serio. Al centro figurano *DNS* e *NTP*, entrambi basati su *UDP*. Se un simile servizio è configurato in maniera errata e accetta richieste dall'intero Internet, gli aggressori lo possono utilizzare per attacchi DDoS. In questo contesto si sfrutta sovente il fatto che una richiesta di dimensioni relativamente piccole può generare una grande risposta (amplificazione). Una parte di queste vecchie apparecchiature è stata fornita con una configurazione per difetto insicura e non può essere provvista mediante manutenzione a distanza di un *firmware* aggiornato e/o di una configurazione sicura. Numerosi utenti non sono affatto consapevoli della configurazione errata della loro apparecchiatura e dei pericoli che vi sono vincolati. Il potenziale di danno di queste apparecchiature è gigantesco. La rimozione di questa configurazione è dispendiosa in termini di denaro e di tempo. MELANI è in contatto con i grandi provider di telecomunicazione che devono eseguire l'aggiornamento delle apparecchiature vulnerabili.

Lacune di sicurezza anche sui router

Vengono reiteratamente rese note lacune di sicurezza delle versioni di firmware utilizzate nelle apparecchiature finali *ADSL*. Non esiste praticamente alcun produttore che non abbia dovuto colmare lacune di sicurezza. Nei mesi di giugno e di luglio del 2013 sono state rese note diverse gravi lacune di sicurezza nelle apparecchiature di Asus[55], come pure una lacuna del servizio *UPnP* delle apparecchiature di D-Link[56]. Nell'ottobre del 2013 è stata pubblicata una lacuna nel cui contesto la mera modifica dell'«*User Agents*» nel browser bastava per ottenere l'accesso al server Web nel caso di alcune apparecchiature Netgear[57]. Anche nel caso di altre apparecchiature di Netgear[58] e Draytek[59] esistono vulnerabilità che consentono agli aggressori di accedere al router e di eseguirvi codice nocivo. Lacune di questo genere sono state ad esempio sfruttate da vermi informatici, come Linux.Darlioz[60], oppure essere sfruttate dai criminali per deviare sessioni di online banking.

---

55 Bugtraq: http://seclists.org/bugtraq/2013/Jul/87 (stato: 20 febbraio 2014).

56 Heise: http://www.heise.de/security/meldung/D-Link-Router-mit-schwerwiegender-UPnP-Luecke-1914510.html (stato: 20 febbraio 2014).

57 Devttys0.com: http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/ (stato: 20 febbraio 2014).

58 The Shadow File: http://shadow-file.blogspot.ch/2013/10/complete-persistent-compromise-of.html (stato: 20 febbraio 2014).

59 CERT.org: http://www.kb.cert.org/vuls/id/101462 (stato: 20 febbraio 2014).

60 Symantec: http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices (stato: 20 febbraio 2014).

MELANI raccomanda di limitare in maniera possibilmente forte l'accesso all'interfaccia di manutenzione del router. Numerose apparecchiature supportano la restrizione a un solo *indirizzo IP* della rete interna. Se non si utilizzano le apparecchiature assistite dai provider, l'utente deve effettuare regolarmente e personalmente gli aggiornamenti. Vanno inoltre attivati soltanto i servizi effettivamente necessari. Green offre una guida dettagliata[61] per risolvere la problematica OpenResolver anche sulle apparecchiature domestiche.

5.6 Interventi parlamentari con riferimento alle tematiche della sicurezza dell'informazione

Scelta di interventi parlamentari del secondo semestre 2013 con riferimento alle tematiche della sicurezza dell'informazione.

Intervento	Numero	Titolo	Inoltrato da	Data di inoltro	Camera	Dipartimento	Stato della delibera & link
Interrogazione	13.5284	Contattare Edward Snowden per ottenere maggiori informazioni sulle attività di spionaggio degli Sati Uniti in Svizzera	Glättli Balthasar	09.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135284
Interrogazione	13.5283	Reazione insufficiente da parte del Consiglio federale nei confronti delle violazioni della sfera privata subite da persone e imprese svizzere	Glättli Balthasar	09.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135283
Interrogazione	13.5338	Generalizzazione del voto elettronico	Markwalder Christa	11.09.2013	CN	CaF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135338
Interrogazione	13.5334	Sfuocatura delle fotografie aeree delle zone sensibili nei documenti accessibili al pubblico	van Singer Christian	11.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135334
Interrogazione	13.5328	Voto elettronico	Sommaruga Carlo	11.09.2013	CN	CaF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135328
Interrogazione	13.5319	Quali misure possono essere adottate per impedire violazioni della protezione dei dati da parte della NSA	Schwaab Jean Christophe	11.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135319
Interpellanza	13.3677	Atti di spionaggio della NSA e di altri servizi informazioni anche in Svizzera?	Gruppo PS / Tschümperlin Andy	11.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133677
Interpellanza	13.3692	Mercato delle telecomunicazioni. Sono ancora attuali la legislazione e le misure di regolamentazione in vigore?	Hurter Thomas	12.09.2013	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133692
Interrogazione	13.5321	Anche la Svizzera è oggetto di spionaggio economico da parte della NSA?	Leutenegger Oberholzer Susanne / Gruppo PS	16.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135321
Postulato	13.3707	Strategia globale per il ciberspazio al passo con i tempi	Gruppo BD / Guhl Bernhard	17.09.2013	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133707
Interrogazione	13.5382	Controllo dell'esportazione di software di sorveglianza proveniente dalla Svizzera	Glättli Balthasar / Gruppo dei Verdi	18.09.2013	CN	DEFR	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135382
Interrogazione	13.5380	Insufficienza degli strumenti di lotta contro la cibercriminalità	Reinmann Maximilian	18.09.2013	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20135380
Postulato	13.3736	Strategia WiFi per la Svizzera	Buttet Yannick	18.09.2013	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133736
Interpellanza	13.3726	Usurpazione d'identità. Una lacuna penale da colmare?	Schwaab Jean Christophe	18.09.2013	CN	DFGP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133726
Interrogazione	13.1060	Abuso nel campo dei nomi di dominio	Fehr Jacqueline	18.09.2013	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20131060
IParl	13.445	Rendere punibile l'usurpazione d'identità nell'intenzione di nuocere per mezzo degli strumenti di comunicazione informatici	Golay Roger	18.09.2013	CN		http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20130445
Interpellanza	13.3773	Legge sulle telecomunicazioni al passo con i tempi. Una strategia globale per il ciberspazio	Wasserfallen Christian	24.09.2013	CN	DATEC	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133773
Mozione	13.3808	Non essere precipitosi nell'estensione del voto elettronico	Schwaab Jean Christophe	25.09.2013	CN	CaF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133808
Interpellanza	13.3799	Sicurezza TIC della Confederazione. Quale rapporto costi/benefici?	Cassis Ignazio	25.09.2013	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133799
Mozione	13.3812	Voto elettronico sicuro. Autorizzare unicamente i sistemi verificabili e muniti di un codice sorgente libero	Glättli Balthasar	26.09.2013	CN	CaF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133812
Mozione	13.3841	Commissione di esperti per il futuro del trattamento e della sicurezza dei dati	Rechsteiner Paul	26.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133841
Mozione	13.3930	Vietare l'esportazione di software di sorveglianza e spionaggio a Stati illegittimi	Glättli Balthasar	27.09.2013	CN	DEFR	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133930
Interpellanza	13.3927	Protezione dei bunker svizzeri per l'archiviazione dei dati	Reimann Lukas	27.09.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133927
Postulato	13.3989	Violazioni della personalità ricon-	Recordon Luc	27.09.2013	CS	DFGP	http://www.parlament.ch/d/suche/seiten/

[61] Green: http://www.green.ch/Portals/0/Support/pdf/Anleitung_OpenResolver_DE.pdf (stato: 20 febbraio 2014).

Intervento	Numero	Titolo	Inoltrato da	Data di inoltro	Camera	Dipartimento	Stato della delibera & link
		ducibili al progresso delle tecnologie dell'informazione e della comunicazione					geschaefte.aspx?gesch_id=20133989
Mozione	13.4009	Attuazione della Strategia nazionale per la protezione della Svizzera contro i cyberrischi	Commissione della politica di sicurezza del CN	05.11.2013	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134009
Interpellanza	13.4023	Piani informatici della Confederazione	Gruppo PPD/PDC - PEV	27.11.2013	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134023
Postulato	13.4069	Spionaggio da parte della NSA e di altri servizi informazioni esteri	Schwaab Jean Christophe	04.12.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134069
Interpellanza	13.4077	Spionaggio di dati e sicurezza su Internet	Gruppo UDC	05.12.2013	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134077
Mozione	13.4086	Programma nazionale di ricerca «Protezione idonea dei dati nella società dell'informazione»	Gruppo dei Verdi / Glättli Balthasar	05.12.2013	CN	DFGP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134086
Mozione	13.4091	Vietare l'utilizzo di installazioni a fini di spionaggio politico, militare o economico nei confronti della Svizzera o di Paesi stranieri	Gruppo dei Verdi / van Singer Christian	05.12.2013	CN	DFGP	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134091
Mozione	13.4165	Caso Snowden. Accordo «no-spy» con gli Stati Uniti	Allemann Evi	12.12.2013	CN	DDPS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134165
Postulato	13.4308	Migliorare la sicurezza e l'indipendenza del settore informatico svizzero	Graf-Litscher Edith	13.12.2013	CN	DFF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20134308

6 Glossario

3DES	Il Data Encryption Standard (DES) è un algoritmo simmetrico di codificazione molto diffuso.
AdServer	Gli AdServer sono utilizzati per distribuire e misurare il successo della pubblicità su Internet. Sia lo stesso server fisico, sia il software Ad che gira su di esso possono essere designati come AdServer.
ADSL	Asymmetric Digital Subscriber Line. Una tecnologia che consente di accedere ad alta velocità a Internet per il tramite di una linea telefonica.
Advanced Persistent Threat (APT)	Questa minaccia provoca un danno molto ingente, che si ripercuote sulla singola organizzazione o su un Paese. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di notevoli risorse.
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.
Applicazione	Un programma per computer che esegue un determinato compito. I programmi di elaborazione dei testi e i browser per Internet sono esempi di applicazioni.
ARPANET	Arpanet (Advanced Research Projects Agency Network) è stato in origine sviluppato a contare dal 1962 da un piccolo gruppo di ricercatori sotto la direzione del Massachusetts Institute of Technology e del Dipartimento della difesa degli Stati Uniti su mandato delle forze aeree US. È un precursore dell'attuale Internet.
Attacchi di Watering-Hole	Infezioni mirate con software nocivo per il tramite di siti Web che vengono visitati di preferenza da un gruppo specifico di utenti.
Attacco DDoS	Attacco Distributed-Denial-of-Service Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Attachments/ Allegato	Un attachment è un file inviato come allegato al testo di una e-mail.
Autentificazione a due fattori	A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. passwort, PIN

	ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.)
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezione di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.
Backup	Backup (in italiano: salvaguardia dei dati) designa la copia di dati nell'intento di poterli ricopiare in caso di perdita.
Black- / White-List	Black-List (lista nera): lista di istanze, come ad esempio pagine Web che devono essere pregiudicate nei confronti del pubblico. Tale pregiudizio può ad esempio essere espresso da un bloccaggio della corrispondente pagina Web. White-List (lista bianca): lista di istanze che secondo il parere del loro autore sono di per sé degne di fiducia.
Carta SIM	La carta SIM (in inglese: Subscriber Identity Module) è una carte chip inserita nel telefono mobile che serve all'identificazione dell'utente.
CD AntiVirus Live	CD di produttori di software antivirus che verifica la presenza di software nocivo sul computer ancor prima dell'avvio del sistema operativo.
Chiave crittografica	In ambito di crittografia si designa generalmente come chiave un'informazione che parametrizza un algoritmo crittografico.
Codice fonte	Il concetto di codice fonte, denominato anche codice sorgente (inglese: source code) designa in informatica la parte di un programma informatico scritto in linguaggio di programmazione che può essere letta dall'uomo.
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
Content Management Systemen (CMS)	Un «Content Management System» (acronimo CMS, in italiano «sistema di gestione dei contenuti») è un sistema che rende possibile e organizza la produzione e l'elaborazione comune di contenuti, consistenti in documenti di testo e multimediali, in genere destinati al World Wide Web. Un autore può servirsi di un simile sistema anche senza conoscenze di programmazione o di

	HTML. In questo caso il contenuto informativo da presentare è detto «content» (contenuto).
Cross Site Scripting	Il Cross-site scripting (XSS) è una vulnerabilità che affligge siti web dinamici che impiegano un insufficiente controllo dell'input nei form.
Daemon SSH	Protocollo di Secure Shell che grazie alla codificazione dei dati rende tra l'altro possibile l'annuncio sicuro (login) a un sistema di computer accessibile attraverso una rete (p.es. Internet). Un Daemon è un programma che gira in sottofondo.
Dischi di rete	Nella misura in cui viene allestito un collegamento permanente alla rete per accedere liberamente ai dati si crea un disco di rete che, come disco virtuale, visualizza in maniera consueta sul cliente le directory e i file di un server.
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).
Domini	Il nome di dominio (ad es. www.example.com) può essere risolto dal DNS (Domain Name System) in un indirizzo IP che può poi essere utilizzato per istituire collegamenti con questo computer.
Exploit Pack	Un Exploit Pack è un kit con il quale si può produrre in maniera semplice software nocivo che sfrutta le vulnerabilità.
File log	Un file log contiene il protocollo automatico di tutte o di determinate azioni dei processi su un sistema di computer.
Firmware	Dati di comando per il controllo di un apparecchio (ad es. scanner, carte grafiche ecc.), memorizzati in un chip. Questi dati possono di norma essere modificati per il tramite di Upgrades (aggiornamenti).
Funzione hash	Algoritmo che genera costantemente una serie di cifre a partire da qualsiasi testo. Le funzioni hash sono utilizzate in tre settori: - nella crittografia; - nei sistemi di banche dati. Essi le utilizzano per effettuare ricerche più efficienti nelle grandi raccolte di dati delle banche dati; - nelle somme di controllo. Un valore hash può essere attribuito a qualsiasi file. Un valore hash modificato fa presagire una manipolazione.

Hosting	L'hosting è l'archiviazione di progetti Internet che possono in genere anche essere richiamati dal pubblico via Internet.
HTML	HyperText Markup Language Le pagine Web sono elaborate in HTML. È così possibile definire le proprietà delle pagine Web (ad es. struttura della pagina, disposizione, link su altre pagine ecc.). Dato che HTML è basato sui caratteri ASCII, una pagina HTML può essere elaborata con un qualsiasi programma di elaborazione dei testi.
IFrame	Un IFrame (anche Inlineframe) è un elemento HTML che serve alla strutturazione delle pagine Web. Esso viene utilizzato per integrare contenuti Web esterni nella propria homepage.
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 Explorer Cache`	In ambito di TED la cache designa una memoria tampone rapida che consente l'accesso (rinnovato) a un media lento in secondo piano o è di ausilio per evitare nuovi calcoli dispendiosi.
IP-Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
Java	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Lettera del disco	I sistemi operativi Microsoft rappresentano con lettere maiuscole i dischi (o più esattamente le loro partizioni, che appaiono all'utente come veri e propri drive).
Life Cycle Management	Il ciclo di vita del prodotto è un concetto di economia aziendale e designa il processo tra l'introduzione sul mercato, rispettivamente il completamento di un bene negoziabile e il suo ritiro dal mercato.
Malicious Code	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di

	Troia, nonché le Logic Bombs.
Memoria ad accesso casuale (RAM)	La Random Access Memory (RAM) è una memoria di informazione utilizzata soprattutto nel caso dei computer come memoria di lavoro, generalmente sotto forma di moduli di memoria.
mTAN	La variante Mobile TAN (mTAN) o smsTAN consta dell'integrazione del canale di trasmissione SMS. Il numero di transazione (TAN) è inviato sotto forma di SMS.
Open Source	Open Source è una gamma di licenze per software il cui testo sorgente è accessibile al pubblico e la cui licenza ne promuove lo sviluppo ulteriore.
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.
PHP Code	PHP è un linguaggio script che viene principalmente utilizzato per l'allestimento di pagine Web dinamiche e di applicazioni Web.
PIN	Un numero di identificazione personale (PIN) o numero segreto è un numero con il quale ci si autentifica nei confronti di una macchina.
Point of Sales (POS)	Un terminale POS (in Svizzera terminale EFT/POS) è un terminale online per il pagamento senza contanti presso un punto di vendita («point of sale»).
Proprietario	L'aggettivo proprietario significa che qualcosa si trova in proprietà. Esso viene utilizzato con riferimento allo hardware e al software, per distinguerli dallo hardware e dal software liberi.
Protocollo NTP	Il Network Time Protocol (NTP) è uno standard di sincronizzazione degli orologi sui sistemi di computer per il tramite di reti di comunicazione basate su pacchetti.
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 (Re-	Il software di manutenzione a distanza (in inglese:

mote Access)	Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
Rete bot	Un insieme di computer infettati da Malicious Bot. Essi possono essere interamente comandati a distanza da un aggressore (il proprietario della rete bot). A seconda delle dimensioni, una rete può constare di poche centinaia fino a milioni di elaboratori infettati.
Roaming	Il concetto di roaming o di transito proviene originariamente dal settore della rete radio GSM. Il roaming GSM usuale consiste nella possibilità per un utente di telefonia mobile di ricevere ed effettuare autonomamente chiamate sulla propria rete domestica via un'altra rete estranea, di inviare e ricevere dati o di accedere ad altre reti di telefonia mobile.
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.
Scriptcode / Javascript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo Web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i browser.
Servizio abusi	Servizio di un provider al quale possono essere effettuate comunicazioni su eventi sul settore di rete del provider.
Servizio di anonimizzazione	Servizio, come ad esempio TOR, con il cui ausilio è possibile utilizzare un indirizzo IP estraneo per celare la propria identità.

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.
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche gli e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
Spear phishing	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
SQL Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L'aggressore tenta di introdurre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
Stream	Con il termine di flussi di dati (in inglese: data streams) si designano in ambito di informatica le successioni di serie di dati di cui non si può prevedere la fine.
Tecnologia over-the-air	L'interfaccia aerea designa la trasmissione di dati mediante onde elettromagnetiche attraverso il media aria (over the air, abbreviato in OTA).
UPnP	L'Universal Plug and Play (UPnP) serve all'attivazione di apparecchiature di qualsiasi produttore (apparecchiature radio, router, stampanti, impianti domestici di controllo) attraverso una rete basata su IP, con o senza controlli centrali mediante un Residential Gateway.
User Agents	Un User Agent è un programma cliente grazie al quale si può utilizzare un servizio de rete.
User Datagram Protocol (UDP)	UDP è un protocollo di rete minimo e senza connessioni che fa par-te della suite di protocolli di trasporto della famiglia di protocolli Internet. Il compito di UDP è di far pervenire all'applicazione corretta i dati trasmessi via Internet.