Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

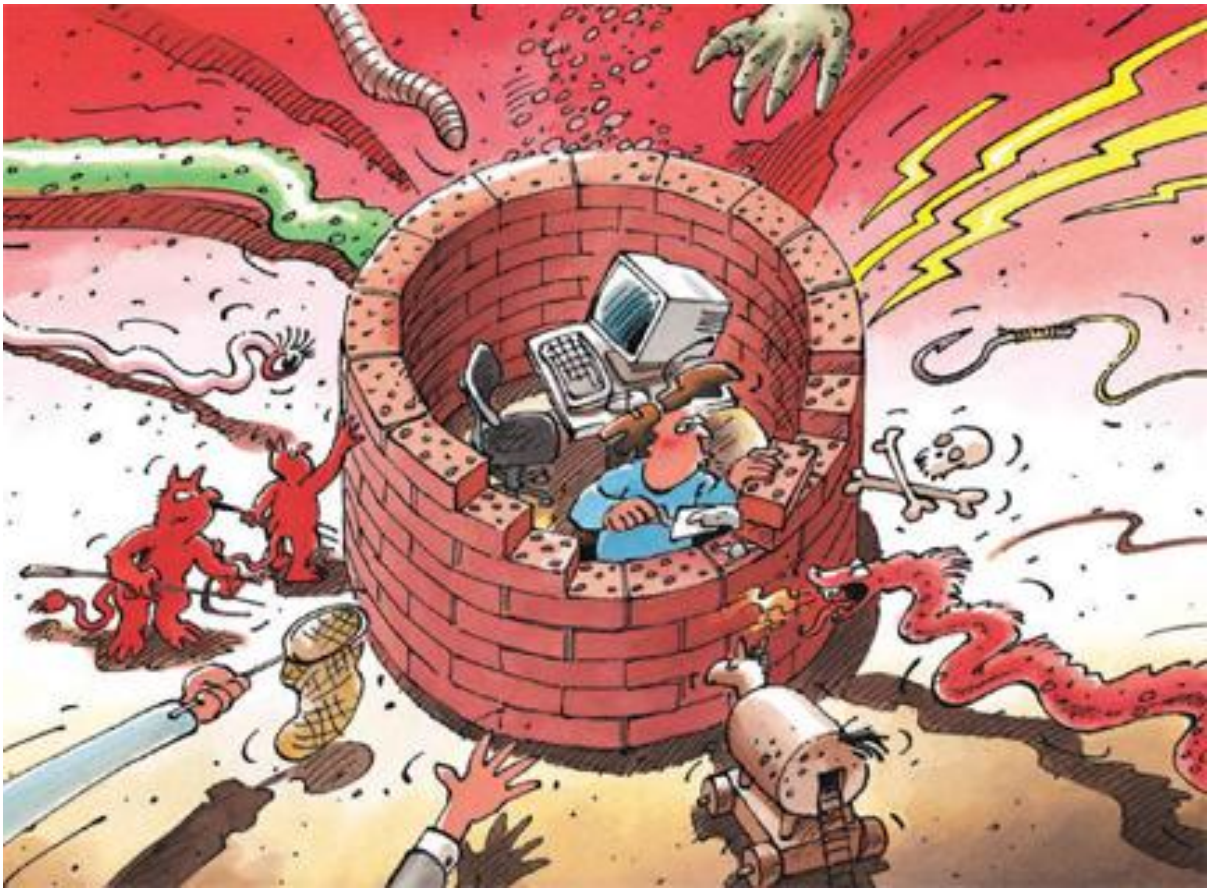
Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

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 2011/II (luglio – dicembre)



Indice

1 Cardini dell'edizione 2011/II

- **Attacchi a offerenti di servizi di certificazione e loro ripercussioni**

  Nel contesto di un attacco a DigiNotar, un servizio di certificazione olandese, sono stati emessi abusivamente oltre 530 certificati, fra di essi quelli per i domini di windowsupdate.com, che ospita la funzione di aggiornamento di tutti i prodotti Windows di Microsoft, come pure diversi domini di Google.

  ► Situazione attuale a livello internazionale: capitolo 4.1
  ► Tendenze / Prospettive: capitolo 5.5

- **Ciberattivismo**

  Nel corso degli ultimi mesi «Anonymous» ha nuovamente suscitato l'interesse dei media con operazioni nel ciberspazio. Ma chi ci cela in realtà dietro «Anonymous»? Secondo diverse dichiarazioni «Anonymous» non è un gruppo o un'organizzazione in senso stretto, ma piuttosto un atteggiamento di vita. Il sostegno non è vincolato a nessuna forma. Ogni attivista fa ciò che può e che ritiene giusto. Ciò può anche provocare che le azioni non raccolgano il sostegno di ampie cerchie del movimento e quindi dichiarazioni contraddittorie.

  ► Situazione attuale a livello internazionale: capitolo 4.3
  ► Tendenze / Prospettive: capitolo 5.2

- **«Buona» e «cattiva» sorveglianza in Internet**

  L'analisi del cavallo di Troia per il perseguimento penale (sovente designato indifferentemente «cavallo di Troia federale») effettuata dal «Chaos Computer Club» ha nuovamente attizzato le discussioni sulla sua utilizzazione non soltanto in Germania, ma anche in Svizzera. Inoltre a partire dal 1° dicembre 2001 Wikileaks ha iniziato a pubblicare numerosi documenti destinati a illustrare che le imprese private di sicurezza vendono soluzioni TIC a Stati con regime prevalentemente autocratico e senza coscienza dei diritti dell'uomo. Il dibattito di per sé vecchio che viene rilanciato poggia su un problema fondamentale di Internet, della società in rete e delle TIC. L'insorgenza di sempre nuove possibilità di comunicazione, di scambio di dati e di informazioni e di disponibilità sempre e ovunque comporta conseguenze: le misure di localizzazione e di procacciamento di informazioni e in via del tutto generale il lavoro delle autorità di sicurezza di uno Stato ne vengono complicati.

  ► Situazione attuale a livello internazionale: capitolo 4.7, capitolo 4.8
  ► Tendenze / Prospettive: capitolo 5.3

- **Phishing, truffe e ransomware in ascesa**

  Un nuovo fenomeno osservato in Svizzera dall'estate del 2011 sono le chiamate telefoniche di truffatori che si spacciano per collaboratori del servizio alla clientela di Microsoft e intendono così procurarsi l'accesso al computer. Negli ultimi 6 mesi è fortemente cresciuto anche il phishing, prevalentemente diretto nei confronti dei provider di posta elettronica e delle imprese di carte di credito. Per mantenere attivi possibilmente a lungo i siti Web fraudolenti i criminali sperimentano nuovi metodi che rendono difficile la disattivazione dei siti di phishing. All'inizio di novembre si è diffuso un software nocivo per effettuare estorsioni (ransomware) che pretende di provenire dal Dipartimento federale di giustizia e polizia.

  ► Situazione attuale a livello svizzero: capitoli 3.1, 3.2, 3.3, 3.4, 3.5

2 Introduzione

Il quattordicesimo rapporto semestrale (luglio - dicembre 2011) 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). Esso presenta un compendio degli avvenimenti in Svizzera e all’estero, illustra i principali sviluppi in ambito di prevenzione e presenta in sintesi le attività più importanti degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario (capitolo 6)** alla fine del presente rapporto. Le valutazioni di MELANI sono evidenziate di volta in volta dal loro colore.

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 2011. In merito il capitolo 3 tratta i temi nazionali, il capitolo 4 i temi internazionali.

Il **capitolo 5** contiene analisi approfondite e tendenze su temi di attualità.

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Chiamate telefoniche di truffatori che si spacciano per collaboratori del servizio alla clientela di Microsoft

Negli ultimi tempi si sono moltiplicate nel mondo, ma anche in Svizzera, le chiamate telefoniche di truffatori che si spacciano per collaboratori di Microsoft o di altre ditte di supporto TIC. Gli interlocutori si esprimono nella maggior parte dei casi in inglese e, stando alle loro indicazioni, provengono dagli USA, dall'Inghilterra o dall'Australia. In numerosi casi essi fanno riferimento a messaggi di errore presuntamente trasmessi dai computer dell'impresa contattata e da persone private. Le persone contattate telefonicamente sono ad esempio indotte ad avviare l'*Event-Viewer*[1] del loro computer, per mezzo del quale possono essere visualizzati tutti i suoi eventi e attività. In merito occorre sapere che anche un sistema che funziona perfettamente produce saltuariamente messaggi di errore. L'elenco dei messaggi visualizzato dall'Event-Viewer può addirittura essere molto lungo a seconda dell'età e della configurazione del computer, senza che il sistema presenti in linea di massima un problema. La chiamata del programma viene tipicamente sfruttata da questo interlocutore di «supporto» per rappresentare alla vittima uno scenario credibile, rispettivamente per infondergli timore. L'obiettivo del truffatore è di convincere la persona contattata a consentirgli di scaricare un programma di accesso a distanza del computer. Se lo scaricamento del programma viene autorizzato l'autore della chiamata dispone delle medesime possibilità di manipolare il computer come se fosse seduto direttamente di fronte ad esso (copia/modifica/cancellazione di dati, installazione di programmi, creazione di una «*porta sul retro*» per accedere nuovamente al sistema in un momento successivo ecc.).

Gli autori delle chiamate offrono talvolta anche la conclusione di un abbonamento di supporto, rispettivamente una garanzia, e richiedono in cambio l'indicazione di dati della carta di credito oppure un'altra forma di pagamento.

I truffatori si scelgono palesemente le vittime avvalendosi di elenchi accessibili al pubblico, come ad esempio il Registro svizzero di commercio o gli elenchi telefonici pubblici.

In linea di principio va constatato che Microsoft non effettua mai senza preannuncio o senza esservi stata sollecitata chiamate telefoniche di supporto per eliminare problemi del computer. Troverete ulteriori indicazioni su questo tema sul *blog* del responsabile in materia di sicurezza di Microsoft Svizzera[2].

Nell'ipotesi che l'autore della chiamata sia stato effettivamente autorizzato ad accedere al computer si raccomanda di fare ispezionare il computer da uno specialista e di farlo se del caso disinfestare. Ciò non garantisce tuttavia il rintracciamento di eventuale *software nocivo*, né la scoperta delle manipolazioni effettuate.

Il metodo più sicuro consiste nella cancellazione integrale del disco rigido e nell'installazione a nuovo del sistema operativo. È tra l'altro importante effettuare regolarmente un *backup* di

1 It. visualizzatore degli eventi, un programma di sistema Windows.

2 http://www.retohaeni.net/2011/07/microsoft-does-not-call-you/ (stato: 23 febbraio 2012).

tutti i dati essenziali su un media di memorizzazione esterno, affinché in caso di problemi del computer questi dati non vadano persi.

3.2 Hackeraggio dei conti di posta elettronica in aumento

Presso Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI si accumulano gli annunci di hackeraggio dei conti di posta elettronica. I criminali modificano tipicamente la password e altre indicazioni personali del conto (indirizzo e-mail alternativo, numero di telefono cellulare ecc.) affinché il titolare legale non vi possa più accedere. Vengono successivamente spediti messaggi a tutti i contatti o a contatti mirati della rubrica del conto. Si tratta in genere di richieste falsificate di aiuto, secondo le quali il mittente sarebbe bloccato da qualche parte all'estero dopo essere stato derubato di tutti i suoi soldi e del suo passaporto, ragione per la quale chiede l'invio di denaro.

From:
Date: Thu, 12 Jan 2012 11:07:37 +0100
To:
ReplyTo:
Subject: Re: Hallo

Ich hoffe du kriegst diese Nachricht rechtzeitig. Ich habe einen Ausflug nach Madrid in Spain gemacht und dabei wurde meine Tasche mit Reisepass, Bargeld, und meine Kreditkarten gestollen. Habe schon meine Bank informiert, aber die Arbeiten nicht so schnell wie ich es haben will. Kannst du mir ein bischen Geld borgen damit ich alles erledigen kann und zur recht komme. Ich gebe dir das Geld so schnell wie möglich zuruck.

Das Geld durch Western Union ist die beste möglichkeit. Lass mich wissen wenn du angaben zur meiner person brauchst (Name, Vorname ...) mich das Geld schiken zu können. Du kannst mich durch e-mail oder durch die Hotel Reception erreichen kann unter di nummer +34962 .

Ich warte auf deine Antwort.

Figura 1: Esempio di una e-mail inviata da un conto hackerato.

Oltre alle seccature per il destinatario esistono ulteriori inconvenienti per il titolare del conto di posta elettronica, perché non dispone più del controllo del proprio conto e non può più accedere alle e-mail e ai contatti. Ciò può essere disastroso e provocare situazioni estremamente sgradevoli nella vita reale nell'ipotesi che non sia stato effettuato un *backup* dei dati e dei contatti e che tutti i contatti di lavoro vengano intrattenuti mediante questo indirizzo di posta elettronica.

Tramite l'accesso al conto di posta elettronica di terzi sono ovviamente possibili numerose altre truffe. Numerose prestazioni di servizi in Internet possono essere raggiunte con la semplice immissione del nome di utente e della password. Se scorda la propria password l'utente può richiederne una nuova tramite il link «Ripristinare la password». La nuova password gli è inviata a mezzo e-mail. Se un aggressore riesce a inserirsi illecitamente sul conto e-mail, esso può servirsi di questo conto per accedere ai più diversi servizi della vittima e sfruttarli in maniera abusiva per proprio conto.

Indichiamo qui di seguito alcuni suggerimenti per ridurre a un minimo il danno in caso di evento:

1. Effettuate un *backup* dei contatti in modo da poter ripiegare su un indirizzo alternativo di posta elettronica in caso di evento. In questo modo è possibile avvertire i contatti possibilmente prima dell'arrivo di una e-mail di truffa.
2. Scelta accurata del provider di posta elettronica, soprattutto quando le e-mail sono utilizzate nell'attività professionale.

3. In caso di evento tentate immediatamente di riprendere il controllo del conto. In alcuni rari casi l'indirizzo alternativo di posta elettronica non viene modificato: in questa ipotesi è possibile inviare una password sostitutiva a questo indirizzo di posta elettronica. Se però anche l'indirizzo alternativo è stato modificato occorre avviare un *Recovery Process*. A tale scopo la maggior parte dei provider di posta elettronica mettono a disposizione un formulario di Recovery. Qui di seguito pubblichiamo un elenco non esauriente degli offerenti usuali di posta elettronica:

Google	https://www.google.com/accounts/recovery/
Hotmail / Live	https://account.live.com/resetpassword.aspx
Yahoo	https://edit.europe.yahoo.com/forgotroot
GMX	http://www.gmx.com/forgotPassword.html

La miglior cosa comunque consiste nel prevenire un'intrusione sul proprio. Osservate in merito le nostre raccomandazioni sull'utilizzo delle password[3]. Vale inoltre il principio generale secondo il quale nessun serio offerente di prestazioni di servizi vi chiederà via e-mail di indicargli la password. Pertanto non cliccate mai sul link di una e-mail per accedere al sito di un provider, di un fornitore di servizi finanziari, di un'impresa di carte di credito ecc.. Leggete inoltre le nostre informazioni in merito al *phishing*[4]. Osservate sempre prudenza quando un sito Web vi chiede la password (cfr. capitolo 3.3.)

Non si tratta più soltanto di adottare un atteggiamento critico nei confronti delle e-mail di persone sconosciute, ma di lasciarsi guidare dalla prudenza anche quando si conosce il mittente. Nel caso di eventi inusitati – soprattutto quando si tratta di denaro – MELANI raccomanda di raggiungere la persona telefonicamente, di porre domande alle quali solo questa persona può rispondere, di accertare la sua identità oppure di discutere con conoscenti comuni la credibilità della storia.

Non si dovrebbero neppure aprire sventatamente gli allegati e cliccare sui link di mittenti conosciuti – soprattutto se l'e-mail sembra impersonale, rispettivamente se nessuna caratteristica personale del mittente è riconoscibile nel testo.

3.3 Una cartolina per le feste per derubare le password

L'invio e il ricevimento di cartoline postali elettroniche è fortemente diffuso nei periodi festivi. Tuttavia non tutte le cartoline postali elettroniche inviate sono serie. Durante il periodo natalizio sono stati osservati due casi particolarmente professionali di truffa rivolti direttamente a vittime svizzere.

Nel primo caso sono stati inviati a nome di Swisspostcard[5] e-mail il cui mittente era conosciuto dai destinatari e che dovevano indurli a cliccare su un link. Al destinatario veniva millantato il ricevimento di una cartolina postale natalizia, scaricabile dal sito Web unsereweihnachtskarten.com.

---

3 http://www.melani.admin.ch/themen/00166/00172/01005/index.html?lang=de (stato: 23 febbraio 2012).

4 http://www.melani.admin.ch/themen/00103/00203/index.html?lang=de (stato: 23 febbraio 2012).

5 Tramite Swisspostcard (un servizio della Posta svizzera) si possono confezionare cartoline postali elettroniche. Swisspostcard provvede successivamente alla loro stampa fisica e al loro invio a mezzo percorso postale regolare al destinatario desiderato.

```
-------- Original-Nachricht --------
Datum: Mon, 26 Dec 2011 07:02:29 -0800
Von:
An:
Betreff: Du hast eine Weihnachtskarte erhalten!

Lieber,

Du hast eine Weihnachtskarte von "einem anonymen Absender" erhalten.

Was kannst Du tun?
Gehe zu: http://www.unsereweihnachtskarten.com?e=

Nachdem Du die Weihnachtskarte empfangen und gelesen hast, kannst du darauf antworten. Wenn du
eine Weihnachtskarte versenden möchtest, gehe zur genannten Webseite.


Viel Spaß,

Julia Emmrich
Unsereweihnachtskarten.com

Swiss Post International
swisspostcard.ch
```

Figura 2: Esempio di e-mail di phishing che millanta al destinatario il ricevimento di una cartolina postale natalizia.

Effettuando un clic sul link si apriva in sottofondo la pagina originale di Swisspostcard. In primo piano veniva però visualizzato un formulario sul quale il destinatario doveva immettere i propri dati di login e la password per poter scaricare la sua cartolina postale natalizia personale. I dati di accesso immessi venivano trasmessi direttamente ai truffatori, che accedevano immediatamente al conto di posta elettronica. Ai contatti figuranti nella rubrica venivano poi subito inviate e-mail di *phishing* del medesimo genere per raggiungere un effetto di circolo vizioso.

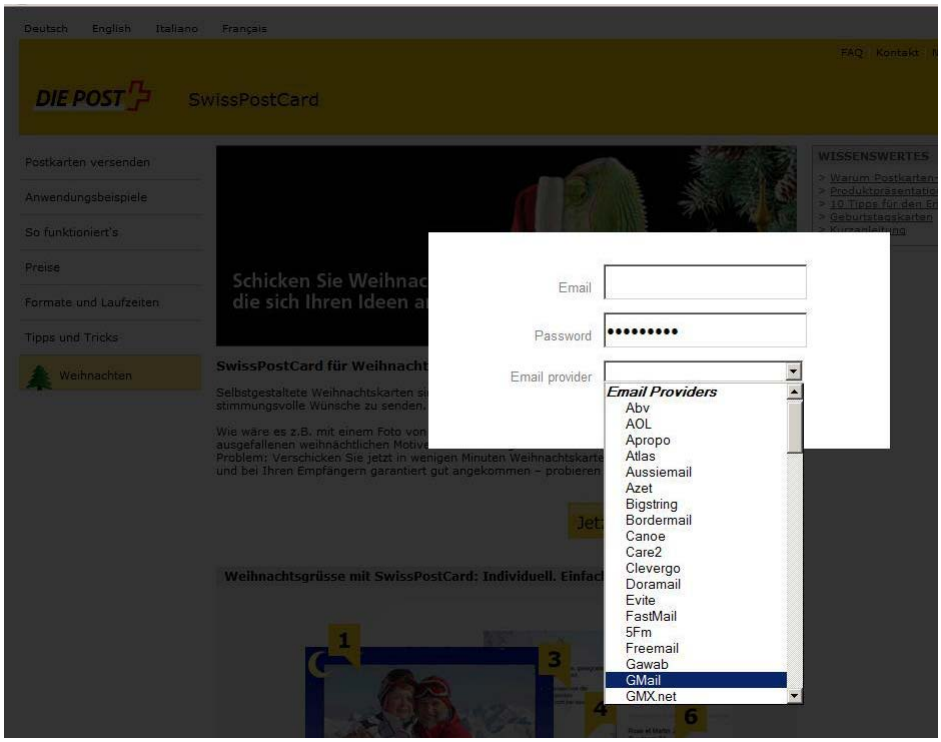


Figura 3: Sito di phishing che carica in sottofondo il sito di Swisspostcard e richiede in primo piano l'immissione dei dati di accesso al conto di posta elettronica.

Una settimana dopo gli aggressori hanno tentato nuovamente il medesimo trucco. Questa volta tuttavia le e-mail di *phishing* non sono state inviate a nome di Swisspostcard, bensì di Fleurop.

Nel primo caso è stato possibile allestire una statistica del numero di attacchi. In totale 25'939 persone hanno cliccato sul link e 4'148 di esse hanno chiamato a più riprese la pagina, circostanza che dovrebbe fornire l'indicazione che esse hanno perlomeno tentato di immettere i dati di login e la password. Ciò corrisponde a una percentuale del 16 per cento circa. Non sappiamo nondimeno se queste persone abbiano poi effettivamente indicato i loro dati di login e la loro password.

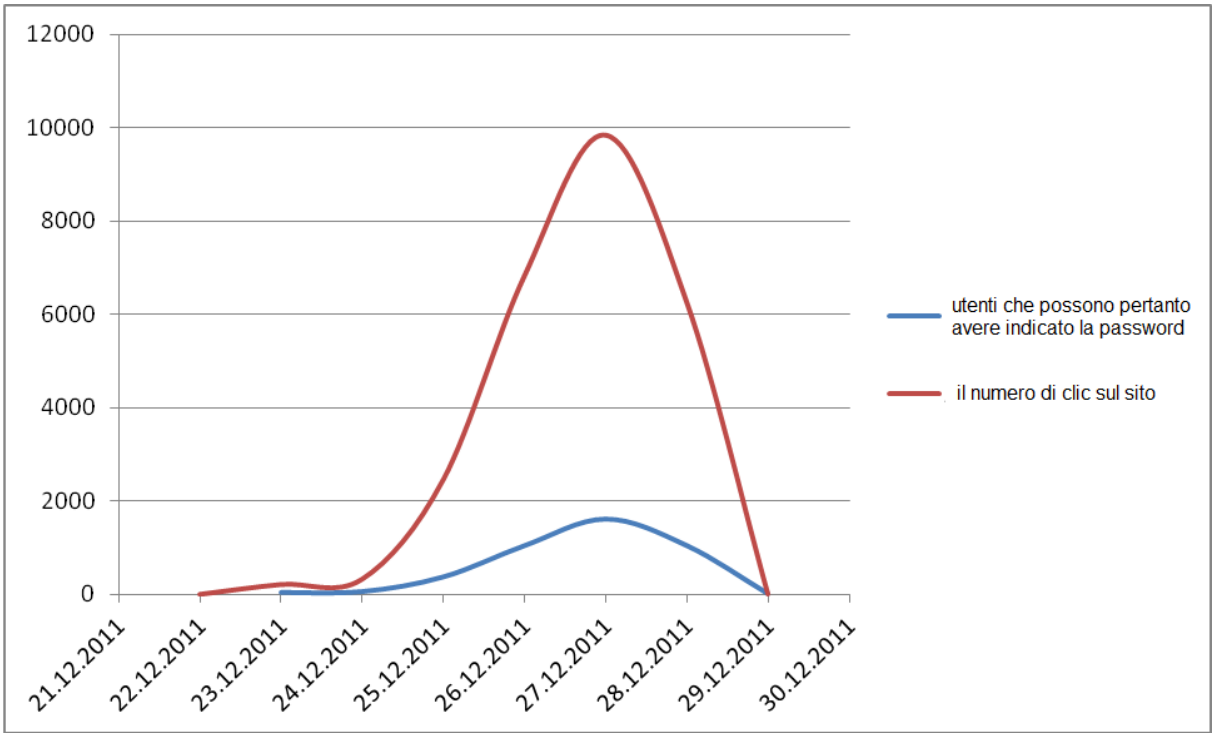


Figura 4: Accessi al sito di phishing «unsereweihnachtskarten.com». La linea rossa descrive il numero di clic sul sito. La linea blu descrive gli utenti che hanno chiamato reiteratamente il sito e possono pertanto avere indicato i loro dati di login e la password.

Tra il 22 e il 24 dicembre 2011 si sono verificati soltanto attacchi singoli, circostanza sicuramente riconducibile al Natale, il 25 dicembre il loro numero è aumentato rapidamente per raggiungere un massimo il 27 dicembre. Il 29 dicembre il sito ha poi potuto essere eliminato dalla rete.

Non si tratta quindi più soltanto di adottare un atteggiamento critico nei confronti delle e-mail di persone sconosciute, ma di lasciarsi guidare dalla prudenza anche quando si conosce il mittente. In particolare si dovrebbe sempre usare prudenza quando un sito Web richiede la password.

3.4 Attacchi di phishing: tecnicamente ottimizzati

Le organizzazioni statali, le imprese private e i provider combattono i tentativi di phishing. La rimozione dei siti di phishing è nella maggior parte dei casi ben collaudata. Nel frattempo pertanto ogni sito di phishing può praticamente essere rimosso in tempo utile, fermo restando che per «tempo utile» viene definita una durata compresa tra pochi minuti e un giorno intero. I criminali sperimentano pertanto nuovi metodi per rendere possibilmente difficile ai servizi corrispondenti la rimozione dei siti di phishing.

Nel caso ad esempio del tentativo di phishing descritto nel capitolo 3.3 il link è stato specialmente generato per ogni vittima ed era valido una sola volta. Dal profilo concreto in ogni link l'indirizzo e-mail è stato codificato in *base64*. Nell'ipotesi che il link iniziale venga cliccato due volte appare un messaggio di errore. Anche sulla pagina iniziale viene affisso soltanto un messaggio di errore. Ciò rende difficile lo spegnimento dei domini perché il servizio competente non ha reagito in assenza di prova attiva di terzi, dacché credeva in buona fede che dietro questo dominio non si celasse alcun sito di phishing. È quanto traspare chiaramente dalla seguente risposta del registro ufficiale:

Hello Sir,

Thank you for your email today and attention to this matter. After review we see that the subdomain you provided is not currently resolving to a phishing site at this time. If you have any further evidence of this domain being in breach of our registration agreement, please respond with it and we are happy to provide you with further assistance.

Thank you,

[redacted] Abuse Team

Figura 5: Risposta dell'ufficiale del registro alla richiesta di MELANI di bloccare i domini del sito di phishing.

Un'ulteriore variante utilizzabile è l'implementazione del filtraggio IP (p. es. georestrizioni). In seguito al filtraggio un sito phishing è raggiungibile soltanto da determinati settori IP. I visitatori con indirizzi IP diversi ricevono un messaggio di errore. Chi richiama il sito Web utilizzando un indirizzo IP "bloccato" ha quindi l'impressione che il sito sia già stato rimosso dalla rete.

In merito occorre sapere che la maggior parte delle pagine di phishing si nascondono in siti assolutamente normali ospitati su server Web compromessi. Diversamente dal caso in cui il dominio viene utilizzato esclusivamente per scopi criminali, sia il proprietario che il provider di hosting hanno la possibilità di cancellare il sito Web. Dato che i provider in genere verificano online i siti e non ricercano i siti fraudolenti nella struttura delle directory del server, il messaggio di errore *«404 Not Found*» costituisce per il provider un indizio sicuro dell'avvenuta rimozione del sito da parte del proprietario.

3.5 Ora anche in Svizzera: software nocivo che blocca il PC ed esige un pagamento

All'inizio del mese di novembre si è diffuso in Svizzera un *software nocivo* che bloccava i computer a fini di estorsione. A tale scopo appariva una finestra con un messaggio proveniente apparentemente dal Dipartimento federale di giustizia e polizia (DFGP). Il messaggio nella finestra invitava l'utente del computer a versare 150 franchi perché sul suo computer si trovava materiale pedopornografico e altro materiale illegale. Questa comunicazione non proveniva ovviamente da un'autorità svizzera.

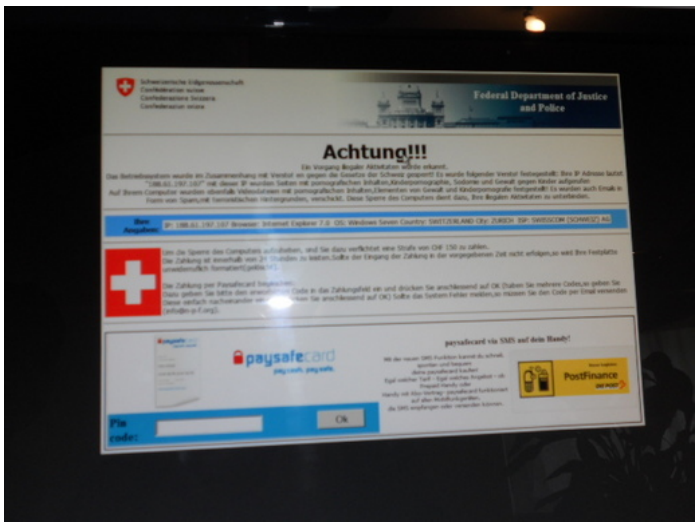


Figura 6: Schermata di un computer infettato da Ransomware.

Fin dai mesi di marzo e aprile 2011 è in circolazione un *software nocivo* che visualizza sui computer infettati una comunicazione proveniente apparentemente dall'Ufficio federale germanico della polizia criminale. La comunicazione in questione esigeva il pagamento di una multa di 100 euro perché sul computer infettato erano state rintracciati dati illegali. In caso di mancato pagamento il computer veniva bloccato e il *disco rigido* formattato. Anche in altri paesi sono state osservate versioni corrispondenti – adeguate al singolo Paese – di questo *Ransomware*.

In caso di apparizione di questa o di simili comunicazioni MELANI raccomanda di analizzare il computer con un *Live-CD* antivirus aggiornato oppure di rivolgersi a una ditta specializzata di computer. Nell'ipotesi di un'infezione si dovrebbero inoltre sostituire le password utilizzate sul computer in questione.

3.6 Politico(i) nel mirino degli hacker

Nel corso del secondo semestre si sono verificati su Internet alcuni eventi che hanno riguardato direttamente o indirettamente la politica svizzera o i partiti. I politici per l'appunto sono figure pubbliche e offrono quindi anche maggiormente il fianco agli attacchi.

In questo senso nel contesto delle elezioni al Consiglio federale del 14 dicembre 2011 è stata diffusa su Twitter una comunicazione, apparentemente a nome del consigliere nazionale Andrea Caroni, secondo la quale Eveline Widmer Schlumpf era stata rieletta , tutto questo prima che fosse noto il risultato ufficiale dell'elezione. Sebbene non avesse niente a che fare con questo account, l'onorevole Andrea Caroni dovette convincere l'opinione pubblica di non celarsi dietro questo *Tweet*. Poco dopo l'onorevole Andrea Caroni ha aperto personalmente un account Twitter e inviato notizie su questo tema. Questo esempio illustra che in Internet ognuno può assumere qualsiasi ruolo e fare qualsiasi dichiarazione a partire da tale ruolo.

Il 3 agosto 2011 il sito Web dell'UDC è stato nuovamente paralizzato da un attacco alla disponibilità. I siti Web dei partiti di Governo erano già stati paralizzati nel novembre del 2009, alla vigilia della votazione del 29 novembre 2009 sull'iniziativa popolare federale «Contro l'edificazione di minareti». Gli altri partiti di Governo non sono però stati toccati da questo evento.

La consigliera nazionale Chantal Galladé è invece stata confrontata con un problema completamente diverso. Dato che non aveva rinnovato tempestivamente il proprio dominio

chantal-gallade.ch, tale dominio è stato acquistato da un terzo che vi ha poi collocato pubblicità. Ogni tentativo di prendere contatto con il nuovo titolare è fallito; non è pervenuta alcuna risposta. Nel frattempo la signora Galladé ha registrato un altro dominio[6]. Sul vecchio dominio non figura più alcuna pubblicità ed è ora in vendita.

Un altro esponente politico ha mostrato la propria carta d'identità alla telecamera nel corso di un'intervista televisiva. Un ignoto ha confezionato una «copia» dell'ID a partire da uno screenshot e successivamente tentato di utilizzare questa immagine come comprova dell'identità per l'allestimento di un profilo presso un portale di dating per omosessuali. Il portale di dating ha preso contatto con il politico per sapere se avesse effettivamente aperto un simile profilo. Al suo diniego il profilo è stato immediatamente cancellato. Grazie all'ottimo e attento lavoro del portale di dating il problema ha potuto essere eliminato sul nascere.

3.7 Hackeraggio di massa dei Webshop

Nell'agosto del 2011 MELANI ha constatato un incremento delle *infezioni di siti Web* nel caso dei Webshop, fra i quali anche numerosi Webshop svizzeri. Ne sono stati toccati i Webshop che hanno utilizzato il software osCommerce.

Gli attacchi sono stati perpetrati attraverso un'*interfaccia Admin* non sufficientemente protetta. Nel caso delle versioni più vecchie si era rinunciato in modo predefinito a un controllo classico degli accessi. Invece della password, il repertorio del *pannello di amministrazione* veniva rinominato utilizzando un nome oscuro, e/o proteggendo la cartella con un documento htaccess. .htaccess (in inglese: hypertext access) è un file di configurazione nel quale possono essere effettuate parametrizzazioni specifiche alla directory. Purtroppo numerosi utenti hanno tralasciato di modificare questi parametri di base. Per accrescere la sicurezza è stato successivamente integrato nella versione 2.2RC2 un controllo di acceso dell'amministrazione. Un'implementazione incorretta ha tuttavia avuto per conseguenza che questa protezione su un Webserver Apache poteva essere aggirata in maniera relativamente semplice effettuando *manipolazioni degli URL*.[7] Per l'aggressore era quindi facile effettuare il login nell'amministrazione e installarvi qualsiasi *codice*. Questa situazione è stata sfruttata intensamente nel luglio/agosto 2011. Gli shop hackerati sono poi stati utilizzati per collocare *infezioni di siti Web*. Secondo una comunicazione sul canale TIC e tecnica di gulli.com gli aggressori hanno compromesso circa 90'000 shop online[8].

Nel caso specifico è stato possibile proteggere l'intero repertorio admin mediante l'inserimento di un file *.htaccess*. Questo controllo di accesso è effettuato dal Webserver stesso ed è indipendente dal prompt di login e dal software shop. Una guida dettagliata è stata pubblicata da heise.de[9]. In genere occorre aggiornare allo stato più recente non soltanto il software del server, ma anche le applicazioni installate – in questo caso il software del Webshop – e si devono installare tutti gli aggiornamenti di sicurezza disponibili.

---

6 http://www.tagesanzeiger.ch/zuerich/region/Warum-Chantal-Gallad-fuer-Bikinis-wirbt/story/15004208 (stato: 23 febbraio 2012).

7 http://www.oscommerce.info/confluence/display/OSCOM23/%28A%29+%28SEC%29+Administration+Tool+Log-In+Update (stato: 23 febbraio 2012).

8 http://www.gulli.com/news/16740-zahlreiche-online-shopping-websites-kompromittiert-2011-08-01 (stato: 23 febbraio 2012).

9 http://www.heise.de/security/artikel/Schnellhilfe-fuer-osCommerce-Admins-1323536.html (stato: 23 febbraio 2012).

3.8 Siti Web falsificati di agenzie immobiliari reclutano agenti finanziari

Dopo una truffa ai danni dell'e-banking il denaro derubato deve essere «riciclato». A tale scopo ci si avvale frequentemente di *agenti finanziari*, reclutati ad esempio per il tramite di borse di impieghi. Sulla rete si collocano però anche siti speciali che pretendono di essere siti di imprese e offrono una rubrica «Posti vacanti» o simile. Nel caso di queste attività si tratta sempre della stessa cosa: denaro proveniente da fonti ignote deve essere accettato e trasferito su determinati conti. Si rinvia di volta in volta a questi «Posti vacanti» mediante messaggi *spam*.

In Svizzera si osserva attualmente un caso particolarmente audace e ostinato di reclutamento di agenti finanziari. Concretamente si utilizzano le indicazioni di imprese iscritte al Registro di commercio, ma che non sono presenti su Internet. I siti Web pubblicati a nome di queste ditte si spacciano per imprese che effettuano operazioni immobiliari in Ticino e sono alla ricerca di rappresentanti regionali per trasferire gli averi della clientela. I siiti hanno un aspetto estremamente professionale. Essi rappresentano in genere una copia 1:1 del sito Web esistente. Nella fattispecie si pone il problema che la motivazione criminale non è evidente come nel caso dei siti Web di *phishing*. Normalmente i siti Web criminali sono rapidamente disattivati dai provider. In questo caso è tuttavia molto difficile indurre il provider a chiudere questo sito Web. Ammesso che ci si riesca non passa molto tempo finché un sito Web identico è attivato sotto un altro dominio. Sembra che un gruppo di criminali si sia specializzato nel mantenere attivi il più a lungo possibile questi siti Web e nel reclutare il massimo numero possibile di agenti finanziari.

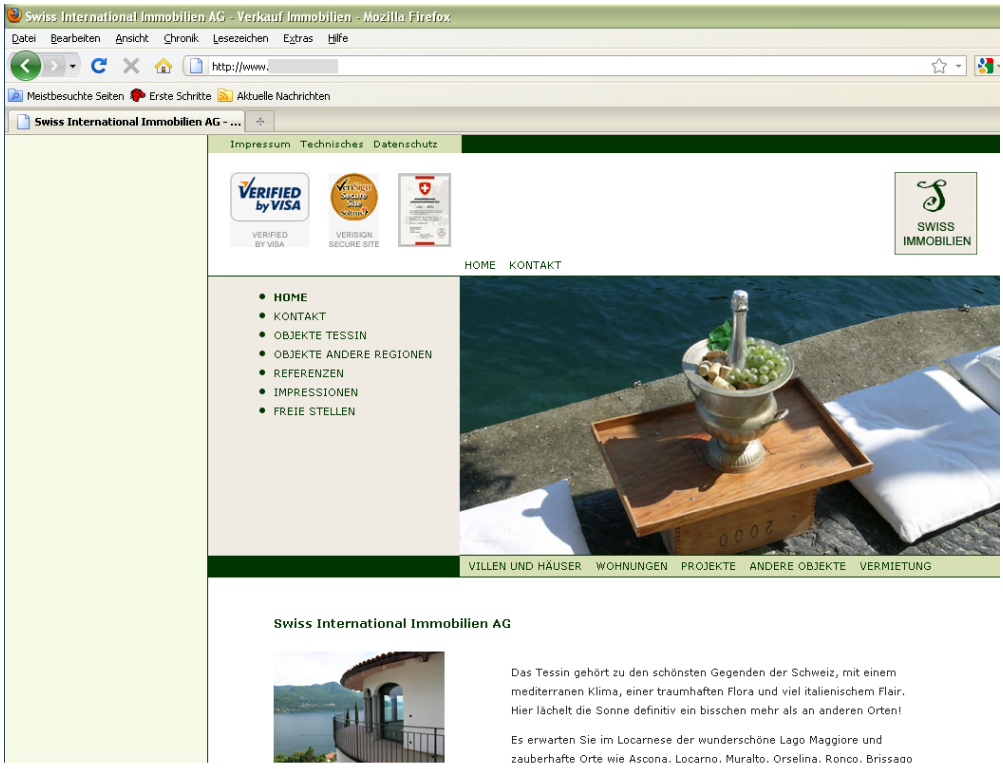


Figura 7: Esempio di sito di reclutamento di agenti finanziari.

Simili offerte sono poste in circolazione non soltanto per il tramite di e-mail e di siti Web appositamente predisposti, ma anche su diversi siti Internet che propongono serie offerte di lavoro. Si raccomanda di usare la massima prudenza quando il denaro ricevuto (volutamente o per errore) deve essere versato a persone sconosciute mediante trasferimento di contante. In ogni caso occorre accogliere con prudenza le offerte che prospettano utili

sproporzionatamente elevati. Anche in Internet vige il principio secondo il quale non è possibile fare legalmente molti soldi senza un lavoro corrispondente. I propri conti bancari non dovrebbero mai essere messi a disposizione di terzi.

3.9 Sistemi di controllo con connessione Internet – È necessaria una speciale consapevolezza della sicurezza

I motori di ricerca sui siti Web fanno parte della quotidianità di ogni utente di Internet. Era invece poco noto finora che esistessero anche motori di ricerca di *server*, *router*, *firewall*, stampanti e altre apparecchiature collegate a Internet. «SHODAN» è un siffatto motore di ricerca, che esiste già da alcuni anni ma che di recente è venuto al centro della ribalta: questo dopo che furono pubblicati i risultati delle inchieste sui sistemi *SCADA* collegati a Internet. Nel quadro della loro inchiesta i ricercatori dell'università di Cambridge intendevano valutare quantitativamente i *sistemi* industriali *di controllo* con collegamento Internet facilmente vulnerabili. Le ricerche[10] dovevano sfatare il mito secondo il quale i sistemi industriali di controllo non sono collegati a Internet e non costituiscono pertanto una fonte di inquietudini quanto alla sicurezza delle infrastrutture sensibili. I ricercatori hanno scoperto dozzine di sistemi vulnerabili Siemens Simatic collegati a Internet (nel mirino di Stuxnet), sistemi *SCADA,* nonché *Building Management Systems* (BMS).

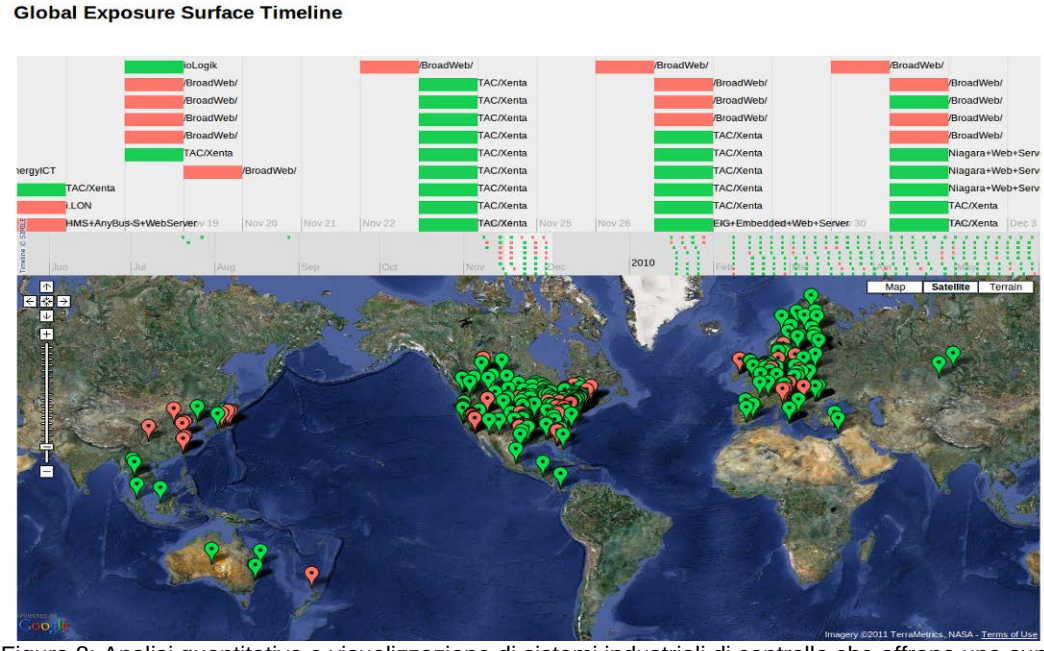


Figura 8: Analisi quantitativa e visualizzazione di sistemi industriali di controllo che offrono una superficie di attacco (fonte: Eireann Leverett)[11]. Sono segnalati in rosso i sistemi con un exploit conosciuto.

In Svizzera queste ricerche complementari hanno consentito di scoprire 34 sistemi vulnerabili. Si tratta nella maggior parte dei casi di applicazioni utilizzate nei *Building Management Systems*. Nel caso di questi impianti di controllo ci si è semplicemente scordati di modificare le password standard. Era quindi possibile accedere a questi impianti e controllarli integralmente. Nel quadro di questa verifica MELANI ha constatato che i sistemi

10 http://www.wired.com/images_blogs/threatlevel/2012/01/2011-Leverett-industrial.pdf (stato: 23 febbraio 2012).

11 http://cryptocomb.org/2011-Leverett-industrial.pdf (stato: 23 febbraio 2012).

vulnerabili non facevano parte di infrastrutture sensibili, ma riguardavano principalmente aziende, come alberghi e uffici.

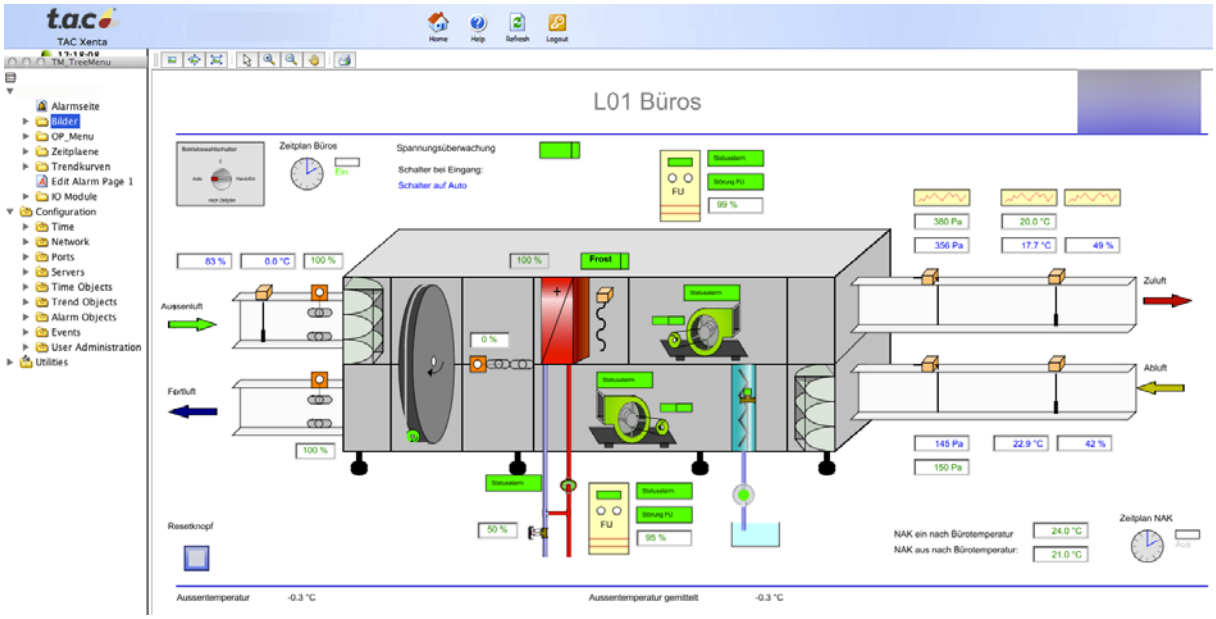


Figura 9: Esempio di un'applicazione del produttore TAC (ora Schneider Electric Buildings Germany GmbH) per il comando di edifici.

Gli obiettivi potenziali non sono considerati sensibili, ma il fatto che all'atto dell'installazione di un *Building Management System* (BMS) con collegamento Internet non venga modificata la password per difetto costituisce una grave violazione delle prescrizioni di base in materia di sicurezza informatica. La possibilità ad esempio di accedere alle reti di riscaldamento e di climatizzazione di un'azienda terza e di manipolarle potrebbe provocare gravi problemi a determinate circostanze. Inoltre il collegamento parziale e le possibilità di accesso ad altre applicazioni amministrative, come software di fatturazione e simili, schiude ulteriori probabilità di abuso. In linea di massima tutti i sistemi industriali di controllo non dovrebbero essere collegati a Internet. Nell'ipotesi dell'assoluta necessità del collegamento questo modo di procedere esige una particolare prudenza. Una valutazione dettagliata figura nel capitolo 5.1.

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Attacco al servizio olandese di certificazione

Secondo i dati attualmente disponibili, nel contesto di un attacco a DigiNotar, un *servizio di certificazione* olandese, sono stati emessi abusivamente oltre 530 *certificati*. Fra di essi figurano ad esempio certificati per domini di servizi di intelligence: gli aggressori hanno potuto emettere di volta in volta *certificati* di www.sis.gov.uk, www.cia.gov e www.mossad.gov.il. Sono stati emessi abusivamente *certificati* anche per altri domini, tra i quali windowsupdate.com, che ospita la funzione di aggiornamento di tutti i prodotti Windows di Microsoft come pure diversi domini di Google.

DigiNotar è il servizio emittente di *certificati* (Certificate Authority, CA), che garantiscono l'identità dei siti Web e assicurano la comunicazione cifrata. In caso di falsificazione di siffatti *certificati*, si può ad esempio ritenere di accedere al sito Web desiderato, mentre si è in realtà collegati con l'infrastruttura dell'aggressore. L'aggressore può in tal modo modificare il

percorso dei dati, intercettare dati cifrati e anche fornire dati falsi. Nel caso dell'attacco a DigiNotar sono stati messi in circolazione unicamente *certificati* falsificati, che sono però considerati affidabili dai browser e dai computer. In questo senso ad esempio può essere decodificato un collegamento cifrato a un conto Webmail oppure falsificato un aggiornamento di Windows. Tuttavia il solo *certificato* falsificato non basta. Il collegamento deve passare attraverso un *server* appositamente predisposto. Sembra che DigiNotar abbia scoperto l'attacco fin dal 19 luglio 2011; a fine agosto Google ha poi scoperto attacchi *Man-in-the-Middle* ai suoi servizi di posta elettronica, rendendoli poi pubblici.

Poco tempo dopo Microsoft ha pubblicato per i suoi sistemi operativi a partire da Windows XP e per Internet Explorer aggiornamenti che negano la fiducia ai *certificati di origine* della CA compromessa DigiNotar e la iscrivono nell'elenco degli emittenti non affidabili. Anche altri produttori di browser come Mozilla (Firefox) e Google (Chrome) hanno nel frattempo contrassegnato come non validi nei loro programmi i *certificati* emessi da DigiNotar.

Secondo quanto pubblicato in un rapporto intermedio dell'impresa di sicurezza[12] incaricata dell'inchiesta, dalla valutazione dei dati emerge che i falsi *certificati* sono stati anche effettivamente utilizzati. Circa 300'000 *indirizzi IP* hanno ad esempio utilizzato il *certificato* Google falsificato. Secondo il rapporto questi *indirizzi IP* possono essere attribuiti nella misura del 99% a computer iraniani. Per poter intercettare e decodificare questi dati l'aggressore ha altresì dovuto effettuare un'interazione diretta sul percorso dei dati, ovvero presso il provider. Un hacker iraniano ha preteso nel frattempo di esserne l'autore e di avere attaccato altri emittenti di certificati. Per il momento non è possibile affermare se gli attacchi provengano effettivamente da questo hacker oppure se dietro di essi si celi un attore statale con intenti di spionaggio.

L'attacco di hackeraggio contro DigiNotar ha provocato l'insolvenza dell'impresa. Secondo quanto afferma la sua società madre Vasco l'attività della filiale verrà interrotta e la ditta sarà liquidata. Il Governo dei Paesi Bassi ha assunto immediatamente dopo la pubblicazione dell'evento il controllo degli affari operativi di DigiNotar. Oltre ai propri *certificati* DigiNotar emetteva infatti come sub-CA *certificati* per la «PKI Overheid» dello Stato olandese e ci sono indizi che i sistemi utilizzati a tale scopo sono anch'essi compromessi. Il certificato di origine «PKI Overheid» non è stato tuttavia ritirato perché ciò avrebbe potuto provocare avarie di comunicazione dei sistemi di computer che dipendono da collegamenti cifrati. Non si è d'altra parte potuto provare l'emissione di certificati abusivi per il tramite di questa infrastruttura. Tutti i *certificati* «PKI Overheid» emessi come sub-CA da DigiNotar sono stati comunque sostituiti a titolo cautelare con nuovi certificati di altre sub-CA.

In un altro caso un hacker ha preteso di essere penetrato nei sistemi dell'emittente di certificati GlobalSign. L'emittente belga di certificati ha allora staccato i propri server dalla rete per una settimana e avviato una verifica. Da questa verifica è emerso che lo hacker non era penetrato nei sistemi utilizzati per l'emissione dei certificati, bensì su un server che mette a disposizione i siti aziendali pubblici per il Nordamerica. Secondo le indicazioni fornite da GlobalSign su di esso non si trovavano applicazioni Web, né dati dei clienti[13].

---

12 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html (stato: 23 febbraio 2012).

13 http://www.zdnet.de/news/41558800/globalsign-comodohacker-hat-die-falschen-systeme-erwischt.htm (stato: 23 febbraio 2012).

L'utilizzazione sicura di *sistemi crittografici* con chiavi pubbliche (la cosiddetta crittografia «Public Key») va di pari passo con la sicurezza dei corrispondenti *Certification Service Provider* (CSP) e Public-Key-Infrastructure (PKI)[14]. Di riflesso la sicurezza dei CSPs e delle PKIs ha sempre costituito un tema che ha occupato i tecnici della sicurezza. L'interesse è incentrato su due scenari: la falsificazione di *certificati* (per il tramite di vulnerabilità a livello di resistenza alle collisioni delle funzioni crittografiche hash utilizzate[15]) oppure l'uso abusivo di certificati di firma di codice. Nel secondo caso – come illustrato dal verme informatico Stuxnet – un siffatto certificato consente ad esempio di introdurre nel sistema operativo *malware* sotto forma di software per driver con firma digitale. Ora però gli attacchi recenti ai CSPs hanno evidenziato che anche la compromissione di CSP in vista dell'emissione di falsi certificati costituisce una minaccia reale. In merito gli hacker sembrano puntare maggiormente sulla fonte, risparmiandosi così il percorso molto più faticoso attraverso la procedura crittografica di per sé sicura.

4.2 SCADA – Software nocivo, attacchi e vulnerabilità

I Supervisory Control And Data Acquisition Systems sono utilizzati per la sorveglianza e il controllo di processi tecnici. (p. es. approvvigionamento energetico e idrico). In origine questi sistemi avevano poche analogie con le TIC usuali: erano isolati dalle reti di computer, utilizzavano hardware e software proprietari e comunicavano attraverso protocolli propri con l'elaboratore centrale. Nel corso degli ultimi anni l'ampia disponibilità di apparecchiature comparativamente più convenienti e dotate di interfacce sul protocollo Internet ha introdotto forti cambiamenti in questo settore. Il vantaggio proveniente dall'impiego di TIC usuali e più economiche è ottenuto al prezzo dell'esposizione in genere dei sistemi *SCADA* alle medesime minacce che ci sono note da Internet: si apre la strada a malware e aggressori.

Symantec scopre «Duqu», un software nocivo con riferimenti a Stuxnet

Il 14 ottobre 2011 si è venuti a conoscenza di un *software nocivo* denominato «Duqu», destinato a spiare i computer delle imprese e degli sviluppatori di sistemi industriali di controllo (sistemi *SCADA*). I dati derubati in questo modo possono essere utilizzati per attacchi successivi ai sistemi industriali di controllo. Le componenti di base (driver) di questo nuovo *software nocivo* si basano su componenti del già noto *software nocivo* Stuxnet[16]. Diversamente da Stuxnet il nuovo software nocivo non dispone tuttavia di una routine di diffusione, né di componenti SCADA, per manipolare ad esempio i sistemi di controllo. Per rimanere per quanto possibile irreperibile, il *software nocivo* si attiva soltanto 15 minuti dopo la sua installazione. Dopo 36 giorni il software nocivo si elimina dal sistema infettato, circostanza che ne rende ulteriormente difficile il reperimento. Sono state osservate diverse varianti di «Duqu». Per la sua installazione è stato utilizzato in un caso il certificato derubato di una ditta taiwanese; anche questa circostanza costituisce un parallelo con Stuxnet. Le altre varianti non erano apparentemente munite di firma digitale.

---

14 In questo senso i CSPs, rispettivamente le PKIs, costituiscono il tallone d'Achille della crittografia «Public Key».

15 Questo punto è p. es. approfondito nelle «Considerazioni tecnologiche: resistenza alle collisioni e rottura delle funzione crittografiche hash» del 4 agosto 2010: http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de (stato: 23 febbraio 2012).

16 Cfr. Rapporto semestrale MELANI 2010/2, capitolo 4.1, link: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (stato: 23 febbraio 2012).

Le funzioni del *software nocivo* comprendono la registrazione dei dati immessi sulla tastiera, l'analisi delle informazioni di rete e la memorizzazione del contenuto dello schermo. Queste informazioni vengono trasmesse all'aggressore nascoste in un file immagine non appariscente. In linea di massima tuttavia la funzione non è vincolata al software nocivo e può essere variata a piacimento dall'aggressore. «Duqu» comunica in maniera cifrata con un *server di comando* provvisto di un *indirizzo IP* indiano al quale il computer infettato fornisce i dati raccolti e dal quale riceve nuovi ordini. Una variante sarebbe già in circolazione dal mese di dicembre 2010, mentre varianti più recenti risalgono al periodo settembre/ottobre 2011. «Duqu» sarebbe stato reperito sui computer di sette o otto imprese europee, fra le quali anche un *indirizzo IP* in Svizzera.

Presunti attacchi all'approvvigionamento idrico

Un presunto attacco elettronico al sistema di approvvigionamenti idrico di Springfield/Illinois negli USA ha suscitato ampie discussioni nelle cerchie specializzate. Si presume che un aggressore sia riuscito a penetrare nel sistema di controllo dell'approvvigionamento idrico e a distruggervi una pompa attivandola e disattivandola ripetutamente. Sembra che nel periodo precedente il difetto alla pompa si siano verificati accessi alla rete dell'impianto a partire da un computer con *indirizzo IP* in Russia, circostanza che ha ulteriormente alimentato i pettegolezzi. Alcuni giorni dopo l'FBI e il Department of Homeland Security (DHS) hanno smentito i rapporti sull'attacco a Springfield. Non esisterebbe alcun indizio di ciberattacco. Le affermazioni contenute nel corrispondente rapporto della centrale di osservazione del terrorismo dell'Illinois e pervenute al pubblico e sulle quali poggiavano le speculazioni erano basate su dati grezzi non confermati. Non esisterebbero indizi di furto dei dati di accesso al sistema, né indizi di un'effrazione. Gli accessi a partire dalla Russia sarebbero il fatto di un tecnico autorizzato, in viaggio in Russia a quel momento, che aveva contattato la rete dell'impianto mediante un accesso (regolare) a distanza. La pompa avrebbe già da tempo presentato problemi, attivandosi e disattivandosi ripetutamente, prima di cessare definitivamente di funzionare.

Probabilmente motivato dall'annuncio del caso menzionato qui sopra, il 18 novembre 2011 un hacker è penetrato nell'impianto di approvvigionamento idrico di South Houston/Texas e ha pubblicato come prova *screenshot* del sistema di controllo dell'impianto. Nel caso in questione una persona con lo pseudonimo «pr0f» ha rivendicato questo attacco con un messaggio sul sito pastebin.com: «È giunto il momento di mostrare che i sistemi sensibili non possono essere collegati a Internet. Non dobbiamo preoccuparci di una presunta grande ciberguerra, ma piuttosto degli attori solitari che per i più diversi motivi e senza grandi conoscenze informatiche potrebbero attaccare simili sistemi sensibili».

Hackeraggio negli anni 2007 e 2008 di satelliti US di osservazione

Secondo un rapporto di Bloomberg Businessweek[17] si sono constatati negli anni 2007 e 2008 diversi attacchi a due satelliti US di osservazione. Questi satelliti sono utilizzati per osservazioni della terra e del clima, come pure per lavori di cartografia. Al momento degli attacchi gli aggressori avrebbero assunto durante più minuti il controllo dei satelliti. I dettagli degli attacchi non sono noti. È ad esempio ipotizzabile che dei dati siano stati falsificati. In teoria sarebbe stato possibile guidare i satelliti e addirittura provocarne la caduta.

---

17 http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (stato: 23 febbraio 2012).

Scrupoli in materia di sicurezza riguardo alla rete del Boeing Dreamliner

Secondo un rapporto della FAA[18] sussistono scrupoli in materia di sicurezza riguardo al cablaggio della rete del nuovo Dreamliner di Boeing. Sembra che la rete per i passeggeri – che consente tra l'altro di accedere a Internet durante il volo – sia fisicamente collegata alla rete di controllo e di navigazione dell'aeromobile, che controlla le funzioni rilevanti ai fini della sicurezza.

La stessa Boeing ha affermato che il documento della FFA trarrebbe in inganno e che la rete passeggeri non è interamente collegata alle altre reti. Si tratta di una combinazione di separazione fisica e di software *firewall*, come pure di altre soluzioni che non sono discusse pubblicamente. Si potrebbero invero scambiare dati tra reti, ma i meccanismi di protezione installati dovrebbero impedire in tutte le circostanze, che i servizi Internet dei passeggeri possano accedere alle reti di controllo e navigazione.

Un collegamento fisico tra la rete dei passeggeri e la rete di controllo dell'aeromobile renderebbe il sistema di controllo vulnerabile agli attacchi degli hacker. La stessa Boeing ha riconosciuto il problema e intende sperimentare e implementare una nuova soluzione.

La problematica di principio dei sistemi *SCADA* si situa prevalentemente nella loro storia: originariamente si trattava di sistemi proprietari autonomi e separati ai quali si poteva al massimo accedere dall'esterno a scopi di manutenzione tramite un *modem dial-up* del produttore. Per via di corrispondenza questi sistemi non dispongono di funzioni di protezione contro gli attacchi elettronici. In tempi recenti tuttavia i sistemi *SCADA* sono stati viepiù collegati in rete, utilizzano protocolli e tecnologie standard, sono in parte raggiungibili tramite Internet e possono talvolta anche essere reperiti con l'ausilio di speciali motori di ricerca (cfr. motore di ricerca SHODAN al capitolo 3.9). Stuxnet ha evidenziato che da solo un sistema separato non può garantire alcuna sicurezza. Finché sarà possibile trasferire i dati a sistemi separati, ad esempio tramite una chiavetta USB, sussisterà la possibilità di insinuarvi *software nocivo*. La presenza sui media di Stuxnet ha suscitato anche presso numerosi esperti di sicurezza l'interesse per la tecnica industriale di condotta e per i sistemi *SCADA*. Da allora sono state identificate diverse lacune di sicurezza in simili prodotti. È stato tra l'altro scopeto un metodo che consente di comandare a distanza i sistemi e di scaricare, rispettivamente caricare qualsiasi file, introdurvi e avviarvi *codici*, nonché di introdurvi dati falsi ai quali i controlli reagiscono in maniera corrispondente.

4.3 Anonymous

Il 27 luglio 2011 la polizia britannica ha arrestato sulle isole scozzesi Shettland il presunto portavoce dei gruppi di hacker «Anonymous» e «LulzSec». Si tratta nella fattispecie di un giovane diciannovenne. In numerosi Stati, fra i quali gli USA, l'Inghilterra, l'Olanda, la Spagna, la Turchia sono già stati arrestati altri membri del movimento di protesta su Internet. Questi arresti provocano di volta in volta attacchi ai siti Web dei corpi di polizia o dei Governi corrispondenti. È quanto è successo anche nel quadro di un'azione coordinata delle polizie italiana e ticinese all'inizio dello scorso mese di luglio, quando in Italia furono arrestati 15 presunti attivisti e in Ticino un cittadino italiano ventiseienne, considerato la testa della cellula italiana di Anonymous. Il collettivo Anonymous aveva tra l'altro attaccato le ditte italiane Eni, Finmeccanica e Unicredit. Nel mirino di Anonymous sono finiti anche le Poste italiane, il Senato, la Camera dei deputati e il sito Web del Governo del presidente del Consiglio

[18] Federal Aviation Administration, autorità federale dell'aviazione degli USA, http://www.faa.gov (stato: 23 febbraio 2012).

Berlusconi. In risposta agli arresti gli attivisti su Internet hanno derubato, secondo le loro proprie indicazioni, materiale dati dai *server* della ciberpolizia italiana CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) e lo hanno collocato su Internet. Alle autorità dello Stato compete la protezione e la conservazione delle infrastrutture TIC critiche. Uno scritto secondo il quale si trattava nella fattispecie di un'azione di rappresaglia è stato invero respinto come non autentico dal gruppo «Anonymous». Ci dovrebbe comunque essere una certa correlazione.

Sempre nel luglio del 2011 gli attivisti su Internet hanno indicato di essere penetrati in un *server* della NATO e di aver copiato numerosi documenti da un *server*. A titolo di prova sono stati pubblicati due documenti PDF degli anni 2007 e 2008. Un'ulteriore azione è stata costituita dalla pubblicazione di 25'000 serie di dati contenenti i nomi, gli indirizzi e le date di nascita di poliziotti austriaci. Questa azione era stata tra l'altro motivata dall'introduzione in Austria, nel mese di aprile 2011, dell'obbligo della conservazione dei dati.

Il maggior scalpore è stato sicuramente quello provocato dall'attacco a fine anno ai dati dei clienti della ditta statunitense Strategic Forecast (Stratfor). La ditta Stratfor è specializzata in analisi internazionali di sicurezza e procura ai propri clienti rapporti su questioni geopolitiche di attualità in ambito di sicurezza come il terrorismo, le sovversioni politiche o i cambiamenti di Governo nei singoli Paesi. Nel corso dell'attacco degli hacker sono stati tra l'altro derubati fondi di e-mail, dati di utente, password e informazioni sulle carte di credito. Uno degli obiettivi dell'azione sarebbe stato di versare denaro a organizzazioni caritative grazie ai dati di carte di credito derubati e quindi di ripartire «oltre 1 milione di dollari a enti di pubblica utilità». Sembra che non siano stati effettuati pagamenti non autorizzati con le carte di credito derubate. Gli attivisti avrebbero reso un cattivo servizio alle organizzazioni di beneficenza perché simili pagamenti provocano infatti dispendio amministrativo da tutti i lati. Dopo aver inizialmente rivendicato l'azione sotto la denominazione «LulzXmas», è poi circolata su Internet una smentita di Anonymous e poi nuovamente una smentita della smentita. Nel quadro di un ulteriore contributo i veri motivi dell'attacco sono stati indicati nella pubblicazione dei contatti dei servizi segreti e dell'industria degli armamenti.

Sotto la designazione «Anonymous» si riuniscono attivisti su Internet di tutto il mondo, per dimostrare a favore di un Internet libero e contro i controlli da parte dello Stato. Sebbene «Anonymous» abbia ripetutamente ribadito di essere un collettivo di attivisti di pari livello, alcune persone vanno considerate le forze trainanti del movimento. Alcune di esse dovrebbero in un certo qual senso essere utenti esperti che schiudono possibilità alla grande massa e danno loro una spinta. Queste posizioni possono se del caso essere assunte – anche sul breve termine – da qualsiasi persona. Un'analisi della struttura dei membri figura nel capitolo 5.2.

4.4 Un attore presumibilmente statale ha spiato per anni i sistemi di computer nel mondo intero, fra di essi anche l'ONU a Ginevra e il CIO

Il 3 agosto 2010 l'impresa di sicurezza McAfee ha pubblicato informazioni relative a un attacco coordinato ai danni di diverse imprese, autorità e organizzazioni. A causa di una configurazione errata l'impresa di sicurezza ha potuto rintracciare su un computer di controllo degli aggressori *file log* sui quali erano registrate le attività di accesso a partire dal 2006. L'analisi di questi file ha fornito illazioni su chi era stato attaccato dagli aggressori e sulla singola durata di questi attacchi. Secondo le informazioni fornite dall'impresa di sicurezza McAfee la scoperta di questo attacco farebbe parte dei maggiori attacchi di spionaggio finora conosciuti. Sempre secondo queste informazioni dal 2006 sono state spiate sistematicamente 72 imprese, organizzazioni e Governi, fra i quali anche la sede dell'ONU di

Ginevra e la sede principale del Comitato internazionale olimpico (CIO) di Losanna. La maggior parte delle reti attaccate si situano comunque negli USA. Si tratta di imprese di comunicazione satellitare, di diverse imprese di sicurezza e anche di un'impresa di produzione di pannelli solari. Non sono stati indicati nomi concreti di imprese. D'altra parte sarebbero anche stati colpiti servizi governativi degli USA, del Canada, dell'India, del Vietnam e di Taiwan. Per quanto riguarda il genere delle informazioni derubate si dispone unicamente delle dichiarazioni dell'impresa di sicurezza, secondo la quale le «informazioni derubate possono costituire un'immensa minaccia economica se si trovano nelle mani sbagliate»[19].

Per questa operazione gli aggressori hanno fatto capo ai metodi tradizionali di infezione come e-mail mirate e link predisposti. Le vittime hanno ricevuto e-mail confezionate su misura da indirizzi di mittente falsificati. Non appena il destinatario cliccava sul link veniva caricato e installato un *software nocivo*. Veniva inoltre stabilito un canale verso il server di controllo.

Nella fattispecie si pensa a un attore statale perché le informazioni derubate non possono praticamente essere messe in vendita da criminali. Il fatto poi che il server di controllo sia mal protetto sulla rete mostra ad esempio che gli aggressori non sono perfetti nella protezione della loro infrastruttura oppure che non si preoccupano affatto o poco si preoccupano della loro protezione perché sono disponibili sufficienti alternative. Questo attacco di spionaggio evidenzia ancora una volta un interesse persistente per dati e informazioni e che la pressione sui dati sensibili aumenta ogni giorno. Occorre partire dall'idea che sono in costruzione ulteriori reti di spionaggio, che altre reti sono già state allestite e sono possibilmente attive, ma non sono ancora state rintracciate.

In questo senso si continua a inviare e-mail mirate. È quanto evidenzia ad esempio un attacco mirato ai danni di gruppi d'armamento nel luglio del 2011. In questo caso gli aggressori hanno inviato ai collaboratori dei gruppi d'armamento e-mail redatte in maniera professionale che reclamizzavano una conferenza dell'associazione statunitense della tecnica aerea e spaziale AIAA. Il documento presuntamente classificato come «segreto» invitava i destinatari a inviare entro il 30 luglio contributi per l'imminente conferenza[20]. E-mail con riferimenti a conferenze sono particolarmente predilette dagli aggressori.

Va considerato che l'obiettivo degli attacchi di spionaggio economico non debbono essere soltanto grandi gruppi attivi a livello internazionale, ma anche piccole e medie imprese innovative.

Ogni volta si presume la presenza della Cina dietro questi attacchi, circostanza che è però sempre stata contestata dal Governo cinese. In realtà è difficile stabilire univocamente la paternità di un attacco, perché la sua unica traccia è nella maggior parte dei casi un *indirizzo IP*. Il fatto che un *indirizzo IP* provenga dalla Cina non costituisce una prova che l'aggressore provenga dalla Cina. È ad esempio relativamente facile affittare in un Paese qualsiasi *server* per il tramite dei quali eseguire gli attacchi, server destinati a mascherare il luogo di provenienza dell'attacco. Quand'anche l'attacco provenisse effettivamente dalla Cina non sarebbe ancora chiaro chi ne sarebbe l'autore. Secondo un articolo del Wall Street Journal i servizi segreti degli USA avrebbero localizzato 20 gruppi cinesi di hacker dai quali

19 http://www.spiegel.de/netzwelt/web/0,1518,778126-8,00.html (stato: 23 febbraio 2012).

20 http://www.heise.de/security/meldung/Gezielte-Angriffe-auf-Ruestungskonzerne-dauern-an-1282837.html (stato: 23 febbraio 2012).

proverrebbero la maggior parte dei ciberattacchi contro gli USA.[21] Anche se secondo il rapporto 12 di questi gruppi sarebbero sostenuti dall'Esercito popolare di liberazione cinese, sarebbe comunque difficile fornire la prova che gli attacchi sono stati effettivamente commissionati dallo Stato. Tale prova è poi resa ancor più difficile dal fatto che più Stati sono in grado di lanciare operazioni di spionaggio di maggiori dimensioni sulle reti.

4.5 Diversi attacchi di hacking

Anche nel corso del secondo semestre si sono verificati o sono stati resi pubblici diversi attacchi di hacking e di spionaggio. Pubblichiamo qui di seguito un elenco non esauriente di esempi:

Attacco di spionaggio alla camera di commercio US

Come riportato dal Wall Street Journal degli hacker cinesi avrebbero installato almeno sei «porte sul retro» sulla rete di computer della camera di commercio US. È probabile che per questo tramite l'organizzazione mantello dell'economia statunitense a Washington sia stata spiata sistematicamente per più mesi. La lacuna di sicurezza è stata scoperta e colmata fin dal mese di maggio del 2010, ma l'evento è stato reso pubblico soltanto nel secondo semestre del 2011[22].

Nuovo attacco ai servizi online di Sony

Dopo l'attacco ai danni dei dati dei clienti di Sony dello scorso semestre gli hacker sono nuovamente riusciti, nell'ottobre del 2011, a penetrare nella rete dei conti di utente dei servizi online di Sony PlayStation Network (PSN) e Sony Entertainment Network (SEN). L'attacco è riuscito in 93'000 casi. Questi dati di conto sono stati bloccati, mentre questa volta i dati di carte di credito non sarebbero stati in pericolo. Diversamente dal primo attacco in questo caso Sony non è stata attaccata direttamente: si è tentato di accedere ai conti con l'ausilio di informazioni sulle password procurate altrove. La spiegazione è semplice: numerose reti di computer utilizzano la medesima password per numerosi servizi, se non addirittura per tutti i servizi. I titolari degli account sono stati informati a mezzo e-mail e hanno dovuto passare attraverso un processo di autentificazione per poter nuovamente liberare il loro conto. Nell'ipotesi dell'effettuazione di acquisti fraudolenti sulla rete Sony, l'impresa rimborserebbe il denaro: è quanto dichiarato da Sony.

Gli hacker attaccano le reti sudcoreane

Nel corso di un attacco di hacking nella Corea del Sud sono stati derubati i dati di circa 35 milioni di utenti di Internet. Come comunicato dalle autorità del Paese a fine luglio le violazioni sono state effettuate sulla piattaforma online e sulla rete sociale Cyworld a partire da computer con *indirizzo IP* in Cina. Fra i dati procurati illegalmente figurano tra l'altro numeri di telefono e di assicurazione sociale, come pure indirizzi di posta elettronica e

---

21 http://online.wsj.com/article_email/SB10001424052970204336104577094690893528130-lMyQjAxMTAxMDEwMjExNDIyWj.html; rapporto integrale dell'Office of the National Counterintelligence Executive: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (stato: 23 febbraio 2012).

22 http://www.spiegel.de/netzwelt/netzpolitik/0,1518,805052,00.html (stato: 23 febbraio 2012).

password. La polizia sudcoreana ha dichiarato che le indagini dureranno probabilmente parecchi mesi[23].

4.6 Disattivazione della rete bot «*DNS*-Changer»

In seguito a un'infezione con il *software nocivo* «*DNS*-Changer» il *sistema DNS* dei computer colpiti è stato manipolato in maniera tale che il *browser Web* degli utenti venisse deviato inosservatamente su siti manipolati alla chiamata di siti Web popolari.

L'11 novembre 2011 gli amministratori criminali di questa *rete bot* sono stati arrestati dall'FBI. I *server DNS* manipolati dei criminali sono stati sostituiti con *server DNS* funzionanti correttamente e gestiti dall'FBI affinché non siano più possibili ulteriori manipolazioni.

Questi *server* dovevano essere disattivati l'8 marzo 2012, ma l'FBI ha poi prorogato il termine transitorio fino al 9 luglio 2012. A partire da questa data i computer infettati non potranno più risolvere alcun nome di dominio, né potranno quindi più chiamare nessun sito Web. A seconda del genere di utilizzazione del computer ciò potrà comportare gravi problemi.

SWITCH[24] e le autorità tedesche hanno pertanto approntato un test online grazie al quale si può verificare in maniera semplice se il proprio computer è stato infestato dal *software nocivo* «*DNS*-Changer»[25].

Secondo le informazioni in possesso di MELANI l'FBI avrebbe identificato nel corso di una settimana 20'500 *indirizzi IP* nella sola Svizzera. Ciò non significa che altrettanti sistemi siano infettati, perché nella maggior parte dei casi si tratta di *indirizzi IP* dinamici. È comunque possibile che parecchie migliaia di PC in Svizzera siano infettati dal *software nocivo* «*DNS*-Changer».

4.7 Cavallo di Troia per il perseguimento penale

L'8 ottobre 2011 il «Chaos Computer Club (CCC)»[26] ha reso noto di essersi procurato un cavallo di Troia per il perseguimento penale delle autorità tedesche. Questo cavallo di Troia consente agli investigatori in Germania la cosiddetta sorveglianza alla fonte delle telecomunicazioni. Le telefonate su Internet, le cosiddette *conversazioni Voice-over-IP* (VoIP), possono così essere intercettate prima della loro codificazione presso il chiamante o dopo la loro decodificazione presso il destinatario.

Nel corso della discussione questo cavallo di Troia è stato sovente designato indifferentemente «cavallo di Troia federale» e quindi equiparato erroneamente ai programmi di spionaggio dell'intelligence e a un grande attacco di ascolto selvaggio. Le basi legali dei diversi generi di impiego non vanno però confuse o scambiate.

Il CCC ha esaminato il Cavallo di troia per il perseguimento penale e rimproverato alle autorità che le sue funzioni non sono limitate alla registrazione delle conversazioni, ma

---

23 http://www.tagesanzeiger.ch/digital/internet/Hacker-greifen-suedkoreanische-Netzwerke-an/story/31054597 (stato: 23 febbraio 2012).

24 http://www.dns-check.ch (stato: 23 febbraio 2012).

25 http://www.dns-ok.de/ (stato: 23 febbraio 2012).

26 http://www.ccc.de (stato: 23 febbraio 2012).

offrono anche la possibilità di leggere dati sul computer e di trasmetterli. In questo senso è ad esempio possibile leggere contenuti del *Web browser* con l'ausilio di screenshot. Una possibilità di acceso a distanza consentirebbe inoltre di scaricare qualsiasi funzione. Il CCC ha criticato anche la codificazione: le comunicazioni in uscita sono *cifrate soltanto in maniera simmetrica*, mentre nel caso delle comunicazioni in entrata la codificazione è totalmente assente. Ciò svolge un ruolo particolare perché i dati e i comandi sono apparentemente disbrigati per il tramite di *server* esteri e non di *server* tedeschi. Il cavallo di Troia comporterebbe inoltre lacune di sicurezza che potrebbero in linea di massima essere sfruttate da terzi per accedere a loro volta al computer sorvegliato.

Anche in Svizzera si è discusso dopo questo evento dell'impiego di cavalli di Troia per il perseguimento penale. La polizia giudiziaria federale ha fatto uso in quattro casi di cavalli di Troia: tre volte nella lotta contro il terrorismo e una volta contro la criminalità organizzata. Il Cantone di Zurigo ha utilizzato almeno una volta cavalli di Troia contro trafficanti di droga[27]. Alla notizia dell'impiego di questi cavalli di Troia il Partito pirata svizzero ha sporto una querela per l'utilizzazione di software di spionaggio nella lotta contro il terrorismo e la criminalità organizzata. Il Ministero pubblico della Confederazione ha deciso nel frattempo di non accogliere la querela[28].

Già prima dell'avvento dell'era di Internet le autorità di perseguimento penale potevano intercettare le conversazioni telefoniche delle persone sospette in presenza di un'autorizzazione del giudice nel caso concreto. Gli offerenti di servizi di telecomunicazione sono tenuti per legge a rendere possibile una simile sorveglianza alle autorità di perseguimento penale[29].

Con la diffusione delle tecnologie alternative di comunicazione si pongono nuove sfide alle indagini delle autorità di perseguimento penale. Dato che in ambito di telefonia su Internet (p. es. Skype) la trasmissione delle conversazioni non è più effettuata da un offerente classico di servizi telefonici e la comunicazione percorre in maniera cifrata le linee, la sorveglianza è possibile soltanto presso le apparecchiature finali. Nella procedura penale è consentito servirsi di mezzi ausiliari tecnici per effettuare la sorveglianza[30]. Nel caso della telefonia su Internet si può trattare di un programma introdotto nel computer della persona mirata che capta successivamente le comunicazioni prima della loro codificazione e le trasmette alle autorità di perseguimento penale.

È una questione controversa sia dalla dottrina giuridica che dalla politica[31] se le attuali[32] basi legali in Svizzera siano sufficienti per questo genere di sorveglianza. Non giova certamente alla chiarificazione di questa tematica il fatto che nelle discussioni si mescolino continuamente perseguimento penale e servizi di intelligence, come pure sorveglianza telefonica e perquisizioni online. Occorre da un canto trattare singolarmente dal profilo giuridico le diverse entità e misure e, d'altro canto, limitare a livello di utilizzazione il

---

27 http://www.nzz.ch/nachrichten/politik/schweiz/trojaner_im_fall_stauffacher_eingesetzt_1.12994241.html (stato: 23 febbraio 2012).

28 http://www.aargauerzeitung.ch/schweiz/anzeige-der-piratenpartei-zu-spionage-software-bleibt-ohne-folgen-115718001 (stato: 23 febbraio 2012).

29 Cfr. legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) e pertinente ordinanza del 31 ottobre 2001 ((OSCPT): http://www.admin.ch/ch/i/rs/c780_1.html (stato: 23 febbraio 2012) http://www.admin.ch/ch/i/rs/c780_11.html (stato: 23 febbraio 2012).

30 Art. 280 del Codice di diritto processuale penale svizzero: http://www.admin.ch/ch/i/rs/312_0/a280.html (stato: 23 febbraio 2012).

31 In Svizzera l'utilizzazione di software di sorveglianza è possibile unicamente nel quadro del perseguimento penale; essa non è invece autorizzata in ambito di agenzie di intelligence.

32 Il Codice di diritto processuale penale svizzero è in vigore soltanto dal 1.1.2011; in precedenza ogni Cantone e anche la Confederazione avevano il proprio Codice di procedura penale.

complesso di funzioni del software agli interventi autorizzati ed escludere una modifica delle funzioni, rispettivamente un abuso dei metodi impiegati. Poco importa se un software di intercettazione utilizzato per registrare conversazioni VoIP sia ad esempio in grado (e abbia il diritto) di effettuare screenshot e di accedere alla posta elettronica. La cosa diviene problematica soltanto se non si può escludere che terzi non autorizzati ricevano i dati rilevati e possano per giunta effettuare manipolazioni del software utilizzato. La sicurezza deve avere la massima priorità nell'impiego dei mezzi corrispondenti.

Occorre infine constatare che sia gli ostacoli a una sorveglianza telefonica «normale» che gli ostacoli a un'eventuale sorveglianza della telefonia su Internet sono importanti: in Svizzera la sorveglianza può essere effettuata soltanto in base a un'autorizzazione del giudice nel caso di determinati gravi reati e se «le operazioni d'inchiesta già svolte non hanno dato esito positivo oppure se altrimenti le indagini risulterebbero vane o eccessivamente difficili»[33]. Qui il principio di proporzionalità deve essere preso in considerazione come nel caso di ogni intervento sui diritti fondamentali.

4.8 Pubblicato da Wikileaks il commercio di software di sorveglianza e di analisi forense

Dal 1° dicembre 2011 Wikileaks pubblica unitamente ai media partner del mondo intero documenti destinati a illustrare che il mercato di soluzioni TIC di sicurezza, di sorveglianza e di analisi forense non fiorisce soltanto con le autorità governative degli Stati democratici, ma anche grazie al commercio con i cosiddetti Stati illegittimi. La maggior parte di questi documenti sono opuscoli di vendita, presentazioni ufficiali e liste di prezzi di circa 100 imprese del settore delle soluzioni globali di sicurezza, come pure della sicurezza e della forensica TIC, fra le quali DigiTask e Siemens in Germania, FoxIT nei Paesi Bassi, Dreamlab Technolgies SA in Svizzera e Hewlett Packard negli USA.

Dopo la caduta di diversi regimi nello spazio arabo sono divenuti pubblici documenti che illustrano l'esistenza perlomeno di offerte nelle quali queste imprese offrono i loro prodotti agli ex potentati. Dopo la caduta del regime egiziano è divenuto pubblico che il gruppo anglo-tedesco Gamma aveva offerto i propri prodotti al regime Mubarak. Nel caso della Libia il regime di Gheddafi avrebbe fatto capo alle soluzioni TIC della ditta francese Amesys per il proprio «Public Safety System and Passport Network».[34] Anche in Siria viene presumibilmente utilizzato software di sorveglianza di ditte TIC occidentali. Oltre al software della ditta tedesca Utimaco – che collega i collegamenti telefonici intercettati con i computer del suo centro di sorveglianza – viene anche utilizzato il software della ditta statunitense NetApp per l'archiviazione della posta elettronica. Proverrebbe invece dalla ditta francese Qosmos la tecnica di sorveglianza delle reti di comunicazione. I produttori non avrebbero mai fornito direttamente la Siria[35].

Nel caso della presente «rivelazione» Wikileaks e diversi gruppi per il rafforzamento della libertà di informazione argomentano altresì che questo genere di trasferimento di tecnologia a sistemi illegittimi non è soltanto moralmente ed eticamente riprovevole, ma che l'aiuto fornito alla sorveglianza e quindi la repressione della popolazione in questi Paesi ha anche avuto un prezzo in vite umane. Si stigmatizza inoltre in maniera generale la vendita di simili

---

33 Art. 269 del Codice di diritto processuale penale svizzero: http://www.admin.ch/ch/i/rs/312_0/a269.html (stato: 23 febbraio 2012).

34 http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html (stato: 23 febbraio 2012).

35 http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html (stato: 23 febbraio 2012).

prodotti alle autorità di perseguimento penale, ai servizi di intelligence e ai militari occidentali. Nel suo editoriale Wikileaks espone chiaramente che l'impiego di siffatte soluzioni TIC di sorveglianza e il mercato che ne risulta sono in linea di massima urtanti e che in merito mancano del tutto disposizioni legali corrispondenti per controllare simili «armi a base di dati». Le imprese menzionate da Wikileaks sono attive nel settore della forensica TIC, della *Lawful Interception* e della cosiddetta *Data Retention* (cfr. anche il capitolo 5.3).

È interessante il fatto che fra i documenti menzionati sotto la denominazione «Spy Files» figurino unicamente offerenti occidentali. Le imprese asiatiche in ascesa che offrono programmi di sorveglianza capillare e di valutazione in ambito di intelligence o in genere di sicurezza interna e che si sono specializzate in identificazione degli utenti, in misure di censura e in sorveglianza delle reti sociali e dei collegamenti HTTPS non sono menzionate. Nel caso di questi newcomer sul mercato della sicurezza ci si fanno pochi scrupoli a vendere software di sorveglianza agli Stati interessati, indipendentemente dal loro regime interno.

4.9 Strategie ed esercizi

Nuova strategia UE per la sicurezza delle reti

L'Unione europea ha annunciato per l'anno prossimo una «grande strategia europea per la sicurezza delle reti europee». In una lettera ai ministeri competenti degli Stati membri sono anzitutto individuate le «capacità di sicurezza». In questo settore l'UE dovrebbe ancora dare un'accelerata politica. L'UE assegna inoltre un ruolo chiave per la propria strategia[36] all'Agenzia europea per la sicurezza delle reti e dell'informazione ENISA[37].

Esercizio trasversale ai Länder di gestione delle crisi nel settore delle TIC in Germania

Il 30 novembre e il 1° dicembre 2011 il Ministero federale dell'interno, in particolare unitamente ai Länder di Amburgo, Turingia, Sassonia, Assia e Bassa Sassonia, ha esercitato per la prima volta il confronto a livello federale con una crisi consecutiva a un ciberattacco. Nel corso di questo esercizio denominato LÜKEX-Übung (Länder Übergreifende Krisenmanagement-Übung/EXercise), esercizio che si svolge ogni due anni all'insegna di tematiche diverse, è stata allenata l'interazione di più settori colpiti a livello federale con gli stati maggiori di crisi dei Länder e con imprese selezionate. L'esercizio di quest'anno era basato su una situazione d'esercizio fittizia che ha messo a confronto gli stati maggiori dello Stato centrale e dei Länder con tutta una serie di eventi dannosi nell'amministrazione e nelle imprese economiche partecipanti (tra l'altro attacchi *spam* massici, programmi nocivi, nonché un sovraccarico intenzionale dei sistemi). All'esercizio hanno partecipato complessivamente 2'500 persone e 12 Länder.

L'esercizio è stato incentrato sulla concertazione Stato federale/Länder in ambito di analisi delle cause degli attacchi TIC, nonché in ambito di misure di prevenzione a livello politico e amministrativo. È stato inoltre esercitato il coordinamento di misure di protezione della popolazione e delle reti delle imprese e delle amministrazioni, come pure l'interazione di organizzazioni pubbliche e di organizzazioni non pubbliche a livello di Stato federale e di Länder. L'esercizio verrà valutato nei prossimi mesi in maniera dettagliata da tutti i

[36] http://www.heise.de/security/meldung/Neue-EU-Strategie-fuer-Sicherheit-in-den-Netzen-angekuendigt-1394814.html (stato: 23 febbraio 2012).

[37] http://www.enisa.europa.eu (stato: 23 febbraio 2012).

partecipanti. L'obiettivo è di raggiungere un miglioramento della pianificazione delle crisi e degli iter di gestione[38].

La Svizzera e in particolare i rappresentanti della cancelleria federale e della strategia nazionale per la protezione della Svizzera contro i rischi cibernetici hanno partecipato all'esercizio LÜKEX in qualità di osservatori. In Svizzera vengono eseguiti esercizi strategici di condotta analoghi a LÜKEX. Il tema del prossimo esercizio di questo genere sarà anch'esso un ciberattacco contro la Svizzera. Per questo tramite il Consiglio federale intende collaudare la strategia di difesa contro un simile attacco e in particolare il suo concetto di attuazione. L'esercizio comprenderà quattro parti e si svolgerà dal settembre 2012 al maggio 2013. Esso è destinato agli stati maggiori di crisi dei dipartimenti e agli altri organi dell'Amministrazione federale che sono convocati in caso di evento[39].

Cyber Atlantic

Figura 10: Logo Cyber-atlantic 2011

Il primo esercizio di Cybersecurity tra l'UE e gli USA è stato eseguito a Bruxelles il 3 novembre 2011. L'esercizio TableTop di un giorno «Cyber Atlantic 2011» ha esaminato la modalità di funzionamento della collaborazione tra UE e USA nel caso di attacco alle strutture critiche di informazione. In questo ambito sono stati simulati gli scenari *Advanced Persistent Threat (APT)* e un attacco a un sistema *SCADA* nel settore dell'energia. L'esercizio ha coinvolto oltre 20 Paesi, 16 dei quali vi hanno partecipato attivamente. Esso è parte di una convenzione UE-USA nel settore della cibersicurezza, conclusa al vertice UE-USA di Lisbona del 20 novembre 2010[40]. La Svizzera ha partecipato in qualità di osservatore al Cyber Atlantic 2011, raccogliendovi preziose esperienze in ambito di coordinamento internazionale in caso di cibereventi.

5 Analisi approfondite e tendenze

5.1 SmartGrid e domotica

Come già menzionato nei capitoli 3.9 e 4.2 i sistemi *SCADA* (Supervisory Control and Data Acquisition) sono soprattutto utilizzati per il comando di centrali elettriche e per sistemi di trasporto, ma anche in misura sempre maggiore nelle abitazioni, negli edifici aziendali e negli

38 Comunicato stampa del Ministero tedesco degli interni: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/12/luekex.html?nn=109632 (stato: 23 febbraio 2012).
Un compendio di esercizi anteriori: https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/IT-Krisenreaktionszentrum/Uebungen/Beispiele/beispiele_node.html (stato: 23 febbraio 2012).

39 http://intranet.bk.admin.ch/aktuell/media/03238/index.html?lang=de&msg-id=43517 (stato: 23 febbraio 2012).

40 http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011 (stato: 23 febbraio 2012).

alberghi per il comando del riscaldamento, la climatizzazione e delle tapparelle. Negli impianti moderni il controllo può essere effettuato anche per il tramite di tablet e smartphone e di app corrispondenti. È ovvio il desiderio di poter utilizzare il comando non soltanto sulla rete protetta di casa, al riparo dei propri quattro muri, ma anche ovunque via Internet. Il telecomando è sensato soprattutto nel caso degli appartamenti di vacanza, per attivare ad esempio lo scaldaacqua prima dell'arrivo, per regolare piacevolmente la temperatura dell'appartamento oppure semplicemente per controllare a distanza lo spegnimento della cucina e di tutte le luci e il buon funzionamento del riscaldamento.

Anche in questo caso occorre porre attenzione alla sicurezza. I sistemi sono direttamente collegati a Internet e sono in linea di massima esposti ai medesimi pericoli dei sistemi di computer. Come descritto nel capitolo 3.9, nel caso dei sistemi di comando degli alberghi e delle aziende con accesso al Web si è semplicemente scordato di modificare la password standard. Era così possibile accedere a questi impianti e controllarli integralmente. Ciò che sembra innocuo di primo acchito può avere conseguenze molto vaste, come ad esempio quando in inverno si spegne il riscaldamento di una casa vuota oppure anche quando il sistema di allarme di casa è pilotato dalla domotica e può così essere disattivato.

In futuro saremo a contatto dei sistemi *SCADA* anche in altri settori. I rivolgimenti nel settore energetico, in vista per l'appunto dell'abbandono a lungo termine dell'energia nucleare, obbligano i fornitori di energia a ricercare possibilità di garanzia della stabilità energetica, anche se il fabbisogno di base proverrà sempre meno dalle centrali nucleari e sarà sempre più disponibile energia irregolare sotto forma di energia eolica e solare. Lo *SmartGrid* è destinato a fornire una soluzione a questo problema. Nel corso di una prima fase il consumo di energia sarà rilevato direttamente presso il consumatore per accrescere la stabilità del sistema. Questi dati saranno poi trasmessi a una centrale. Se oggi il consumo energetico si basa in gran parte su stime ed esperienze, sarà successivamente possibile determinarlo con maggiore precisione e quindi garantire una migliore stabilità del sistema. Se però questi dati pervengono nelle mani sbagliate o se un siffatto *SmartMeter* viene hackerato, si potrà analizzare in base ai dati di consumo di corrente se una persona è o no al proprio domicilio oppure manipolare la fattura di elettricità.

In una seconda fase è ipotizzabile che anche apparecchiature come la lavastoviglie e la macchina per lavare siano collegate e controllate da uno *SmartGrid*. Il consumatore finale segnalerà poi alla centrale che intende avviare la macchina per lavare. Questa segnalazione non è immediata, nel senso che la centrale di comando decide quale è il momento opportuno per avviare l'apparecchiatura corrispondente.

È chiaro che un simile sistema deve essere molto bene protetto perché a seconda delle circostanze manipolazioni errate possono provocare gravi interruzioni di corrente. Nella peggiore delle ipotesi l'intero approvvigionamento energetico può essere paralizzato.

5.2 Anonymous – i vantaggi e gli inconvenienti della struttura aperta

Nel corso degli ultimi mesi «Anonymous» ha nuovamente provocato agitazione con diverse operazioni nel ciberspazio. Sull'elenco delle vittime figurano ditte illustri come Sony, la Bank of America, l'impresa di sicurezza Stratfor (cfr. il capitolo 4.3) oppure addirittura gruppi criminali come «Los Zetas», la mafia messicana della droga.

In Svizzera ha soprattutto suscitato scalpore l'«Operation Payback», nel cui ambito è stata tra l'altro oggetto di attacchi Postfinance dopo la chiusura dei conti di Julian Assange, il fondatore di Wikileaks. Ma chi si cela in realtà dietro Anonymous e questi attacchi? Secondo diverse dichiarazioni Anonymous non è un gruppo o un'organizzazione in senso stretto, che

dispone di uno statuto e alla quale si fa atto di adesione come membro e si versano contributi. Anonymous è piuttosto un'idea, rispettivamente un atteggiamento di vita[41]. Il sostegno non è vincolato a nessuna forma. Ogni «Anon» fa ciò che può e che ritiene giusto. Questa definizione comporta il vantaggio di ridurre il livello di inibizione a partecipare ad «Anonymous» e di poter sfruttare il momento di un'indignazione attuale nei confronti di un'impresa o nei confronti dello Stato prima che il partecipante alle azioni si faccia (possa farsi) troppi scrupoli sulle conseguenze. Questa struttura comporta d'altra parte anche pericoli, tra l'altro per il movimento stesso. Dato che tutti gli «Anon» decidono autonomamente ciò che ritengono giusto, è possibile che vengano annunciate o eseguite azioni che non corrispondono necessariamente al parere della maggioranza, se non al parere complessivo di Anonymous.

Il primo esempio in merito è costituito dall'annuncio che Anonymous avrebbe attaccato il 5 novembre 2011 Facebook con l'obiettivo che per il fatto di questo attacco «il maggior numero possibile di utenti abbandoni Facebook»[42]. L'annuncio ha suscitato grande scalpore sui media – ma il 5 novembre 2001 non è successo niente. Esso ha provocato ampi dibattiti sulla stampa, ma anche nelle schiere di Anonymous. In questi senso altri «Anon» hanno considerato il piano di attacco come come "immaginario" e ad opera di un combattente solitario, sebbene nell'ottica di Anonymous sussisterebbero senz'altro motivi per compiere una simile azione. Il nome dell'iniziatore è stato in definitiva pubblicato, circostanza che va indubbiamente considerata come la massima punizione in seno ad Anonymous[43].

Anche nel caso dell'attacco a Stratfor si sono accumulate rivendicazioni, smentite e smentite delle smentite. Dopo avere inizialmente rivendicato l'azione «LulzXmas» e avere invitato a effettuare versamenti a organizzazioni di beneficenza con i dati derubati delle carte di credito, è circolata su Internet una smentita a nome di Anonymous, che è stata successivamente smentita a sua volta. Nel contesto di un altro contributo i veri motivi dell'attacco sono stati indicati nella pubblicazione dei contatti dei servizi segreti e dell'industria degli armamenti[44]. Il caso Stratfor pone tuttavia in luce un altro aspetto: sotto la copertura di Anonymous potrebbero anche celarsi criminali con intenti meramente finanziari e senza grandi visioni. I dati delle carte di credito non sono stati utilizzati soltanto per trasferire presuntamente 1 milione di dollari a organizzazioni di beneficenza. Essi sono stati inoltre collocati sulla rete dove sono rimasti liberamente disponibili a tutti i criminali (e al resto del mondo) e hanno potuto essere utilizzati per qualsiasi scopo.

Il vincolo blando ad Anonymous sfocia in una serie di attacchi non coordinati e più o meno spettacolari. Dato che per motivi inerenti alla sua struttura non esiste adesione come membro ad Anonymous, né esistono un portavoce ufficiale e persone responsabili dell'intero movimento, ognuno può in linea di massima eseguire attacchi o pubblicare comunicazioni in nome di Anonymous. In questo senso dopo un attacco o dopo la pubblicazione di dati è ozioso dibattere se si tratti o no di Anonymous. Le rivendicazioni e le smentite vanno considerate alla medesima stregua.

41 http://www.format.at/articles/1131/524/303276_s1/format-chat-anonymous-mitglied-tvxor (stato: 23 febbraio 2012).

42 https://www.taz.de/!81221/ (stato: 23 febbraio 2012).

43 http://www.golem.de/1111/87543.html (stato: 23 febbraio 2012).

44 http://www.n-tv.de/technik/Hacker-Angriff-gibt-Raetsel-auf-article5086791.html (stato: 23 febbraio 2012).

5.3 «Buona» e «cattiva» sorveglianza in Internet

L'analisi del cavallo di Troia per il perseguimento penale (nel linguaggio corrente anche cavallo di Troia federale) effettuata dal «Chaos Computer Club» e la pubblicazione dell'insieme delle sue funzioni hanno nuovamente attizzato le discussioni in merito alla sua utilizzazione non soltanto in Germania, ma anche in Svizzera. Inoltre a partire dal 1° dicembre 2001 Wikileaks ha iniziato la pubblicazione di documenti destinati a illustrare che le imprese private di sicurezza vendono soluzioni TIC a Stati con regime prevalentemente autocratico e senza coscienza dei diritti dell'uomo. Molte di queste soluzioni rientrano nell'ambito della cosiddetta *Lawful Interception* e della forensica TIC e consentono alle singole autorità di intercettare e di registrare le comunicazioni su Internet e a mezzo telefonia mobile dei cittadini oppure di spiare i dati sui computer.

Il dibattito di per sé vecchio ora nuovamente rilanciato poggia su un problema fondamentale di Internet, della società in rete e delle TIC. L'insorgenza di sempre nuove possibilità di comunicazione, di scambio di dati e di informazioni e di disponibilità sempre e ovunque comporta conseguenze: le misure di localizzazione e di procacciamento di informazioni e in via del tutto generale il lavoro delle autorità di sicurezza di uno Stato ne vengono complicati. Nel caso ad esempio dell'intercettazione di una comunicazione Skype ordinata dal giudice questa evoluzione rende necessario l'impiego di soluzioni TIC, come l'installazione di programmi estranei sul computer della persona sospettata. Sono per l'appunto gli Stati che perseguono una politica di repressione nei confronti di chi la pensa diversamente che rafforzano il controllo centralizzato delle reti interne e dei loro collegamenti con l'estero a causa delle accresciute possibilità di comunicazione in patria e all'estero. In merito si utilizzano in parte i medesimi prodotti e soluzioni TIC impiegati negli Stati di diritto che funzionano apparentemente meglio. Ne è motivo il fatto che a livello tecnico Internet, i computer e le reti funzionano ovunque nel medesimo modo e che si possono utilizzare ovunque soluzioni TIC corrispondenti, a prescindere da dove si situano questi elementi TIC e dalle condizioni quadro legali predominanti.

Dal profilo giuridico, fatte salve determinate restrizioni in ambito di commercio di soluzioni crittografiche, i prodotti TIC non sottostanno a nessun controllo delle esportazioni. Un siffatto controllo non sarebbe neppure attuabile di fatto. Da un canto le soluzioni TIC basate su software, come quelle stigmatizzate da Wikileaks, sono quasi sempre cosiddetti *beni Dual-User* e, d'altro canto, constano di *codice* di programma – non sono quindi fisicamente disponibili – e possono essere spostate in ogni momento da un posto all'altro. Ironicamente un simile regime di esportazione può essere attuato a livello mondiale soltanto mediante un controllo totale di tutto l'Internet e dei suoi flussi di dati.

In considerazione del fatto che i più diversi processi si svolgono sempre più su Internet è chiaro che da parte delle autorità di sicurezza di un determinato Paese esista una domanda di soluzioni TIC nell'una o nell'altra forma. È soltanto in questo modo che possono adempiere ulteriormente il loro mandato nel quadro dello Stato di diritto. Non esiste una stretta linea di separazione che indichi a partire da quale momento, secondo la concezione occidentale, gli Stati utilizzano simili soluzioni in maniera illegittima. Ogni Stato è peraltro libero di emanare in questo campo, per la propria industria TIC, norme vincolanti sul commercio di soluzioni TIC che disciplinino chiaramente in quali casi siffatti prodotti possono essere utilizzati dalle proprie autorità. In Svizzera questi lavori sono stati avviati o sono già

stati conclusi nel quadro della revisione della legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni[45] (LCSPT) e di altre leggi in questo settore.

5.4 Sicurezza nell'era mobile – Come proteggo il mio smartphone?

Come illustrato dalle statistiche più recenti[46] la Svizzera dispone di circa quattro milioni di telefoni mobili, fra i quali 1.5 milioni di *smartphone*[47]. Due diversi sistemi operativi dominano il mercato a livello mondiale e in Svizzera: iOS di Apple, con una quota di mercato di quasi il 50%, e Android di Google con una quota di pressoché il 27 %. Questi due sistemi operativi sono anche quelli maggiormente diffusi in ambito di tablet.

In questo contesto è possibile constatare una sempre maggiore convergenza tra sistemi operativi per apparecchiature mobili e sistemi operativi «classici» per *desktop*. È quanto testimoniano il nuovo sistema operativo «Mountain Lion» di Apple che comprende diverse funzioni di iOS oppure il nuovo «Windows 8» che disporrà della medesima interfaccia grafica nella versione *desktop* e nella versione mobile[48].

Queste statistiche evidenziano che ci troviamo in una fase di transizione, che porta dai sistemi *desktop* ai sistemi mobili. Quale ne è il significato ai fini della sicurezza? Un'analisi di iOS e di Android dovrebbe consentire di chiarirlo meglio:

- Il sistema operativo di Apple è un sistema proprietario che funziona unicamente sull'hardware di questa impresa. Finché il sistema iOS non sia stato manipolato[49], l'utente può installare soltanto applicazioni provenienti da iTunes Store oppure applicazioni[50] «in house» senza AppStore, se partecipa al programma «iOS Enterprise Program». Ognuno può sviluppare qualsiasi applicazione per il sistema iOS. Prima che possano accedere al mercato[51] le applicazioni devono però essere state preliminarmente analizzate e accettate da Apple. Successivamente esse sono direttamente firmate da Apple e offerte su iTunes Store. L'utente non può tuttavia vedere i diritti attribuiti a un'applicazione.
- Il sistema Android poggia invece su una piattaforma *Open-Source* con kernel Linux che può girare sullo hardware di qualsiasi produttore. Il principale punto di diffusione delle applicazioni è Google Play Store (prima chiamato Android Market[52]) – con un

---

45 http://www.admin.ch/ch/i/rs/c780_1.html(stato: 23 febbraio 2012).

46 http://weissbuch.ch/wb11press.html (stato: 23 febbraio 2012).

47 Lo smartphone è un telefono mobile che combina funzione avanzate, come ad esempio la connessione a Internet oppure l'elaborazione di dati personali con le funzioni di base di un telefono. L'altra categoria di moderni telefoni mobili è denominata «Feature Phones». Questi telefoni mobili dispongono soltanto di alcune funzioni complementari. Il loro sviluppo non è quindi così complesso come quello degli smartphone.

48 Sembra che il prossimo Windows 8 Metro abbia ormai perso il pulsante start, così caro agli utenti di Microsoft: http://arstechnica.com/microsoft/news/2012/02/discoverability-windows-8-and-the-disappearance-of-the-start-button.ars (stato: 23 febbraio 2012).

49 In ambiente iOS questa operazione viene denominata «Jailbreak».

50 Grazie al programma «iOS Developer Enterprise» una ditta può ad esempio sviluppare un proprio App Store: https://developer.apple.com/programs/ios/enterprise/ (stato: 23 febbraio 2012).

51 https://developer.apple.com/appstore/guidelines.html (stato: 23 febbraio 2012).

52 L'Android Market è stato modificato in Google Play il 7 marzo 2012

semplice clic l'utente può installare applicazioni da qualsiasi sito Web[53]. Anche nel caso di Android ognuno può sviluppare qualsiasi applicazione. Non esiste però alcun processo di verifica corrispondente a quello di Apple. Inoltre lo sviluppatore firma personalmente le applicazioni. L'utente finale ha la possibilità di prendere visione dei diritti dell'applicazione (tuttavia soltanto se perviene da Google Play Store al sito Web, perché tipicamente i diritti non sono visualizzati direttamente sull'applicazione dello *smartphone*).

Symantec ha recentemente pubblicato un rapporto[54] relativo alle modalità con le quali entrambi i sistemi operativi tentano di garantire la sicurezza dell'utente finale. Il rapporto esamina i seguenti cinque punti:

1. **Controllo tradizionale di accesso:** ad esempio l'utilizzazione di una password per accedere al telefono oppure la possibilità di bloccare l'accesso all'apparecchio dopo un determinato periodo di inattività.
2. **Provenienza delle applicazioni:** in merito si considera principalmente la *firma digitale*.
3. **Cifratura:** cifratura dei dati in caso di furto o di perdita dell'apparecchio.
4. ***Sandboxing*:** il tentativo di isolare le applicazioni in maniera che esse possano accedere soltanto ai processi dei quali abbisognano.
5. **Diritti delle applicazioni:** alle applicazioni sono attribuiti soltanto i diritti di cui necessitano assolutamente per adempiere le loro funzioni.

Secondo il rapporto le differenze tra entrambi i sistemi sono palesi. In sintesi il fattore maggiormente determinante va ricercato nella provenienza delle applicazioni. In merito esiste una differenza evidente tra entrambe le filosofie. Per quanto attiene alla sicurezza Apple assume la responsabilità delle applicazioni da installare[55]. Dal canto suo l'approccio *Open-Source* di Android consente all'utente di installare qualsiasi applicazione, senza tuttavia un grande controllo e limitazioni delle funzionalità, rispettivamente dei diritti necessari. Basta recarsi su Google Play per trovare fin dalla prima pagina giochi che esigono autorizzazioni completamente inutili per gli scopi dell'applicazione stessa. Rientrano fra di essi i diritti di invio e di ricevimento di SMS, di effettuare chiamate e di accedere ai dati personali memorizzati sull'apparecchio[56].

Un ulteriore aspetto risiede nel fatto che nel caso degli apparecchi mobili la protezione dal *software nocivo* differisce notevolmente da quella alla quale siamo abituati sui sistemi *desktop*. In futuro la protezione degli apparecchi mobili sarà interamente ripensata oppure le «vecchie» idee dei sistemi *desktop* dovranno essere implementate anche sugli apparecchi mobili.

---

53 Questa procedura è denominata «Sideloading».

54 http://www.symantec.com/podcasts/detail.jsp?podid=b-a-window-into-mobile-device-security (stato: 23 febbraio 2012).

55 In almeno un caso – quello del ricercatore statunitense Charlie Miller – è stato possibile disattivare la sicurezza dello App Store per pubblicare un'applicazione potenzialmente nociva: http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (stato: 23 febbraio 2012).

56 Un esempio interessante è quello di Uloops, un'applicazione per comporre brani musicali. Nella relativa descrizione gli sviluppatori indicano che l'applicazione ha accesso allo stato del telefono e all'identità. Essa può importare informazioni come l'ID interna del telefono, il modello, la marca, il nome dell'utente, la password e l'account di e-mail e quindi una grande quantità di dati personali: https://market.android.com/details?id=net.uloops.android&feature=featured-apps#?t=W251bGwsMSwxLDIwMywibmV0LnVsb29wcy5hbmRyb2lkIl0 (stato: 23 febbraio 2012).

- Antivirus:
  Nel caso dei sistemi mobili il sistema operativo non gestisce alcuna protezione antivirus. Per quanto riguarda iOS solo Apple potrebbe fornire una simile protezione perché l'antivirus dovrebbe poter accedere a tutte le applicazioni, ciò che non è però consentito alle applicazioni installate. In genere ciò è impedito dal *Sandboxing* e dall'attribuzione dei diritti. Su Android i soli programmi antivirus efficaci sono a pagamento. Ciononostante l'applicazione gratuita di Creative Apps è l'applicazione antivirus maggiormente diffusa. Secondo uno studio di AVTest[57] sembra che essa non abbia riconosciuto nessuno dei 172 *virus* verificati.
- Firewall:
  Per il momento non esistono studi che hanno analizzato i *firewall* sugli apparecchi mobili.
- Aggiornamento del sistema operativo e delle applicazioni:
  nel caso degli apparecchi con sistema operativo non modificato (ovvero senza *Jailbreak* o *ROM* modificata) soltanto Apple e alcuni produttori di hardware che implementano Android forniscono aggiornamenti regolari. La maggior parte dei produttori di hardware che utilizzano il sistema di Google non vi sono preparati. Sussistono pertanto eventuali lacune di sicurezza finché l'utente non ha acquistato un nuovo apparecchio.

L'utente finale è quindi posti davanti a una scelta difficile: affidarsi ad Apple e agire in un sistema chiuso[58] senza grandi «libertà» oppure optare a favore di un sistema *Open-Source* con tutti i suoi vantaggi e inconvenienti[59], caratterizzato dalla sua apertura e da poche restrizioni.

5.5 Attacchi a offerenti di servizi di certificazione e loro ripercussioni[60]

L'impiego sicuro di sistemi criptografici a chiave pubblica (cosiddetta criptografia a chiave pubblica) va di pari passo con la sicurezza dei CSP e delle PKI[61] corrispondenti. Di conseguenza la sicurezza dei CSP e delle PKI ha da sempre costituito un tema del quale si sono occupati i tecnici della sicurezza. Il loro interesse si è focalizzato su scenari basati sulla falsificazione dei certificati (a seguito di una debole resistenza alle collisioni delle funzioni hash criptografiche[62]) o sull'utilizzazione abusiva di certificati per la firma del codice. Nel secondo caso – come è stato mostrato dal verme informatico Stuxnet – un simile certificato

---

57 http://www.av-test.org/fileadmin/pdf/avtest_2011-11_free_android_virus_scanner_english.pdf (stato: 23 febbraio 2012).

58 Oltre ai vantaggi e agli inconvenienti dell'architettura iOS e del modello di mercato vanno menzionate eventuali sorprese, come ad esempio l'invio dei dati di posizionamento GPS. All'atto del backup i dati sono trasmessi ad Apple all'insaputa dell'utente: http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/ (stato: 23 febbraio 2012).

59 Anche in questo caso vanno presi in considerazione ulteriori fattori a parte l'architettura e il modello di mercato. Android lascia al provider la possibilità di modificare il sistema operativo o di installare applicazioni prima della vendita del telefono. Ciò vale ad esempio per l'applicazione Carrier IQ, preinstallata su alcuni apparecchi Android. Essa registra in ampia misura il comportamento dell'utente e lo comunica al provider: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/ (stato: 23 febbraio 2012).

60 Un estratto del rapporto specialistico omonimo è scaricabile dal sito: http://www.melani.admin.ch/dokumentation/00123/01132/index.html?lang=it

61 In questo senso i CSP e le PKI costituiscono il tallone d'Achille della criptografia a chiave pubblica.

62 Questo punto è stato ad esempio approfondito in *Considerazioni sulla tecnologia, Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen,* del 4 agosto 2010: http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de

consente ad esempio di introdurre nel sistema operativo malware sotto forma di software per driver firmato digitalmente. Tuttavia gli attacchi più recenti ai CSP hanno evidenziato che anche la compromissione di un CSP finalizzata all'emissione di certificati falsi costituisce una minaccia reale. Con l'ausilio di falsi certificati di server SSL/TLS è possibile sferrare attacchi *Man-in-the-Middle* (MITM) su vasta scala. A questo punto l'aggressore dispone del pieno controllo dei dati trasmessi, può decriptarli e leggerli.

Nell'ipotesi che – come nella fattispecie – siano stai emessi certificati falsi, occorre tenere conto dei seguenti punti:

- da una parte tutti i meccanismi attivi di revoca dei certificati fondati su liste di revoca (CRL e/o risposte dell'OCSP) non funzionano per questi certificati. Un certificato falso (ossia emesso in modo illegittimo) non è imperativamente bloccato e pertanto non è neppure riconoscibile come tale. In questo caso sarebbe necessario poter distinguere tra certificati autorizzati (ovvero emessi legittimamente) e certificati non autorizzati.
- d'altra parte è emerso che il modello di fiducia (centralizzato e gerarchizzato) basato sullo standard ITU-T X.509 è in linea di massima problematico. Se nell'ambito di questo modello vengono compromessi un CSP o una Root CA (autorità di certificazione radice) riconosciuta come attendibile, ne sono colpite tutte le entità che si riferiscono a questa CA (nel peggiore dei casi tutti gli utenti di Internet). Sotto il profilo della sicurezza tutti si trovano nella medesima barca e la probabilità che una Root CA sia compromessa è proporzionale alla lunghezza dell'elenco.

Al termine di queste osservazioni preliminari ci si chiede quali misure si possano adottare per prevenire al meglio gli attacchi MITM nelle condizioni date. Poiché esistono soltanto pochi approcci per prevenire tali attacchi, si dovrà tentare di rendere gli attacchi MITM possibilmente difficili e dispendiosi per gli aggressori. A tal fine, occorre stabilire se si possono apportare modifiche al modello di fiducia.

- Se non è possibile modificare il modello di fiducia, si raccomanda di lavorare con elenchi prevalentemente vuoti di Root CA attendibili, ovvero di selezionare solo determinate Root CA. Google usa questa possibilità già dalla versione 13 di Chrome, denominata «public key pinning». Se si intende generalizzare questo approccio estendendolo a un numero indefinito di domini, c'è l'opportunità di una connessione al Domain Name System (DNS).
- Se si possono apportare modifiche al modello di fiducia, vi sono in genere nuovi approcci da prendere in considerazione. Ad esempio un modello di fiducia nel quale la compromissione avrebbe soltanto ripercussioni locali. Un simile modello dovrebbe essere imperativamente distribuito e sostenere relazioni dinamiche di fiducia. I ricercatori dell'Università Carnegie Mellon hanno ad esempio mostrato che gli attacchi sono effettuati perlopiù a livello locale e che pertanto i falsi certificati si possono accertare facendo un confronto con i servizi notarili distribuiti geograficamente.

Come ogni sistema socio-tecnico anche il CSP presenta punti deboli e vulnerabilità che nell'ambito di un attacco possono essere indirizzate e sfruttate (in maniera più o meno mirata). I punti deboli e le vulnerabilità riguardano non tanto le procedure e i meccanismi criptografici utilizzati quanto le interfacce con i processi di rilascio e di emissione dei certificati. Come documentano gli attacchi più recenti, in questo ambito le aggressioni sono ipotizzabili e anche realizzabili. Volendo fare un'analogia con un falsificatore di banconote, diremo che questi può falsificare biglietti di banca oppure – ma si tratta di un'operazione più complicata e più dispendiosa – introdursi mediante effrazione in un'azienda che stampa le banconote e utilizzare abusivamente i macchinari installati per emettere banconote regolari. È evidente che la seconda possibilità è certamente più difficile da realizzare, ma in compenso maggiormente lucrativa. Un attacco analogo è riuscito nel settore delle PKI e con ogni probabilità attacchi simili saranno effettuati con successo anche in futuro. Vale dunque la pena di tenere conto di queste eventualità nelle considerazioni sullo sviluppo delle future PKI.

6 Glossario

.htaccess	.htaccess (in inglese: hypertext access) è un file di configurazione nel quale possono essere effettuate parametrizzazioni specifiche alla directory.
404 Error Page	Una pagina di errore è una pagina che viene visualizzata quando ad esempio si clicca un link a Internet non più funzio-nante o su un URL inesistente. La maggior parte dei browser visualizzano in questo caso la pagina standard fornita dal server Web. Le pagine di errore possono essere predisposte individualmente dal webmaster del sito.
AcceptPathInfo	Configurazione del Webserver Apache.
Advanced Persistent Threat	Questa minaccia provoca un danno molto ingente, che si ripercuote sulla singola organizzazione o su un Paese. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di notevoli risorse.
Agente finanziario	È un agente finanziario chiunque svolge legalmente l'attività di intermediario monetario e quindi anche operazioni di trasferimento finanziario. In tempi recenti questo concetto è utilizzato nel contesto delle transazioni finanziarie illegali.
Apache Webserver	Il server HTTP Apache è un prodotto Open Source e libero della Apache Software Foundation e il Webserver maggiormente utilizzato in Internet.
Attacco Man-in-the-Middle	Attacco Man-in-the-Middle Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in grado di seguire o di modificare lo scambio di dati.
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di acce-dere 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.

Base64	Base64 descrive una procedura di codificazione di file binari a 8 bit (p. es. programmi eseguibili, file ZIP) in una stringa di caratteri consistente unicamente di caratteri ASCII leggibili e indipendenti dal codepage.
Beni Dual Use	Dual Use (inglese per doppia utilizzazione) è un concetto utilizzato prevalentemente nel controllo delle esportazioni che caratterizza l'utilizzabilità di principio di un bene economico (p. es. di una macchina, ma anche di software e di tecnologia) sia a scopi civili che a scopi militari.
Blog	Un blog è un diario tenuto su un sito Web e quindi nella maggior parte dei casi visibile al pubblico, sul quale almeno una persona, il Web-logger o blogger (in forma abbreviata), registra annotazioni, elenca circostanze o mette per scritto riflessioni.
Bot / Malicious Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
Browser	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e Safari.
Building Management System	Un Building Management System (BMS) è un software per il cui tramite un edificio dotato di automatizzazione può essere visualizzato e pilotato. Rientra nelle funzioni usuali del Building Management System il comando della luce e della climatizzazione.
Certificate Authority (italiano: servizio di certificazione)	Un servizio di certificazione è un'organizzazione che rilascia certifi-cati digitali. Un certificato digitale è in un certo qual senso l'equivalente di una carta d'identità a livello di cyberspazio ed è destinato all'assegnazione di una determinata chiave pubblica a una persona o a un'organizzazione. Tale assegnazione è autenticata dal servizio di certificazione che provvede a tale scopo apponendovi la propria firma digitale.
Certificati di server SSL/TLS	Un certificato digitale è in un certo qual senso l'equivalente di una carta d'identità a livello di cyberspazio ed è destinato all'assegnazione di una determinata chiave pubblica a una persona o a un'organizzazione. Tale assegnazione è

	autenticata dal servizio di certificazione che provvede a tale scopo apponendovi la propria firma digitale.
Certification Service Provider (CSP)	Cfr. servizio di certificazione.
Certificato di origine	Certificato che serve a validare la vigenza di tutti i certificati subordinati.
Certificato digitale	Certifica l'appartenenza di una chiave pubblica (PKI) a un soggetto (persona, elaboratore).
Cifratura simmetrica	Diversamente dalla cifratura asimmetrica, nel caso di una cifratura simmetrica entrambi i partecipanti utilizzano la medesima chiave.
Code	Istruzioni di programma che definiscono i comandi che deve eseguire il computer.
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.
Data Retention	Data Retention (in italiano: conservazione dei dati) designa la memorizzazione di dati riferiti alle persone da parte o per conto del servizio pubblico, senza che i dati siano attualmente necessari.
Desktop	Un Desktop Computer, abbreviato in «Desktop», è un computer in forma di box, adeguato all'impiego come elaboratore di lavoro sulle scrivanie.
Dial-Up	Significa "selezione" e designa l'allestimento di una comunicazione con un altro computer tramite la rete telefonica.
DNS-System	Domain Name System. Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
Driver Software	Un driver per apparecchiature, sovente semplicemente denominato driver, è un programma di computer o un modulo di software che comanda l'interazione con le apparecchiature collegate.
Event-Viewer	Programma cha visualizza messaggi di errore e di servizio nel sistema operativo Windows.
Exploit	Un programma, uno script o una riga di codice

	per il tramite dei quali è possibile sfruttare le lacune dei sistemi di computer.
File log	Un file log contiene il protocollo automatico di tutte o di determinate azioni dei processi su un sistema di computer.
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere – ossia sul vostro computer.
Firmare / Firma / Firma digitale	Per firma digitale si intendono dati abbinati a informazioni elettroniche grazie ai quali è possibile identificare il firmatario, rispettivamente il creatore della firma, e l'integrità delle informazioni elettroniche firmate.
Georestrizioni	Limitazioni, ad esempio alla chiamata di siti Web, a motivo dell'appartenenza nazionale dell'indirizzo IP utilizzato.
Harddisk	Hard Disk (in italiano: disco rigido) è un media magnetico di memorizzazione della tecnica informatica che scrive dati sulla superficie di un disco ruotante.
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.
Interfaccia admin o Administrationspanel	L'interfaccia admin è un'interfaccia grafica per il cui tramite l'amministratore può effettuare configurazioni.
IP-Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
ITU-T X.509	X.509 è uno standard ITU-T della Public-Key-Infrastructure per l'allestimento di certificati digitali.
Jailbreak	Con il termine jailbreaking (dall'inglese evasione dalla prigione) si intende il superamento delle limitazioni di uso dei prodotti Apple per il tramite

	di un apposito software.
Lawful Interception	Lawful Interception (in italiano: sorveglianza della telecomunicazione) significa la possibilità per gli Stati di poter ad esempio sorvegliare il traffico telecomunicazioni della parola, di testi, di immagini e di film.
Live CD	Un Live CD contiene un sistema operativo bootable.
Malicious Code	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Toia, nonché le Logic Bombs. Vedi anche Malware.
Manipolazione dell'URL	Con l'ausilio di determinate manipolazioni dell'URL un server può essere indotto a visualizzare siti che sono di per sé bloccati.
Open Source	L'Open Source è una gamma di licenze di software il cui testo fonte è liberamente accessibile e che per il tramite della 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.
Public Key Infrastructure	Infrastruttura per la gestione e l'utilizzazione di certificati digitali.
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.
Recovery Process	Recovery (in italiano: ripristino dei dati) significa il ripristino dei dati originali dopo la loro perdita.
ROM	Read Only Memory Una memoria che consente unicamente la lettura dei dati, ma non la loro soprascrittura.
Root CA	Servizio centrale di certificazione.

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.
Sandboxing	Il sandboxing è una tecnica che genera sul computer un ambiente separato che può essere utilizzato per l'esecuzioni di programmi non affidabili.
Screenshot	Per screenshot (in italiano: copia della schermata) si intende nelle TIC la memorizzazione del contenuto grafico attuale dello schermo.
Server	Sistema di computer che offre ai clients determinate risorse, come ad esempio spazio di memoria, servizi (ad es. e-mail, Web, FTP ecc.) o dati.
Servizio di certificazione	Il servizio di certificazione è un'organizzazione che emette certificati digitali. Un certificato digitale è in qualche sorta l'equivalente di una carta di identità nel ciberspazio e serve ad attribuire una determinata chiave pubblica a una persona o a un'organizzazione. Questa attribuzione è autenticata dal servizio di certificazione, che la munisce della sua propria firma digitale.
Sistemi crittografici	Un sistema crittografico è un sistema utilizzato per la cifratura. Crittografia significa originariamente scienza di cifratura di informazioni.
Sistemi di controllo	Cfr. SCADA
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
SmartGrid	Si designa come «Smart grid» una rete (di corrente) intelligente nel cui ambito i dati di diversi apparecchi (tipicamente i contatori presso i consumatori) sono ritrasmessi all'esercente della rete e grazie alla quale, a seconda della sua struttura, si possono inviare comandi a questi apparecchi.
SmartMeter	Uno SmartMeter (in italiano: contatore intelligente) è un contatore dell'energia che mostra al singolo utente del collegamento il consumo effettivo di energia e il tempo effettivo di

	utilizzazione, dati che possono anche essere trasmessi all'impresa di approvvigionamento energetico.
Smartphone	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
SMS	Short Message Service Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
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.
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 intro-durre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
Tweet	Contributi della piattaforma di comunicazione Twitter.
USB	Universal Serial Bus Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo).
Virus	Un programma informatico capace di autoreplicarsi e provvisto di funzioni nocive, che si aggancia a un programma ospite o a un file ospite per diffondersi.
VoIP	Voice over IP Telefonia tramite il protocollo Internet (IP). I protocolli utilizzati con maggiore frequenza sono: H.323 e SIP.