Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

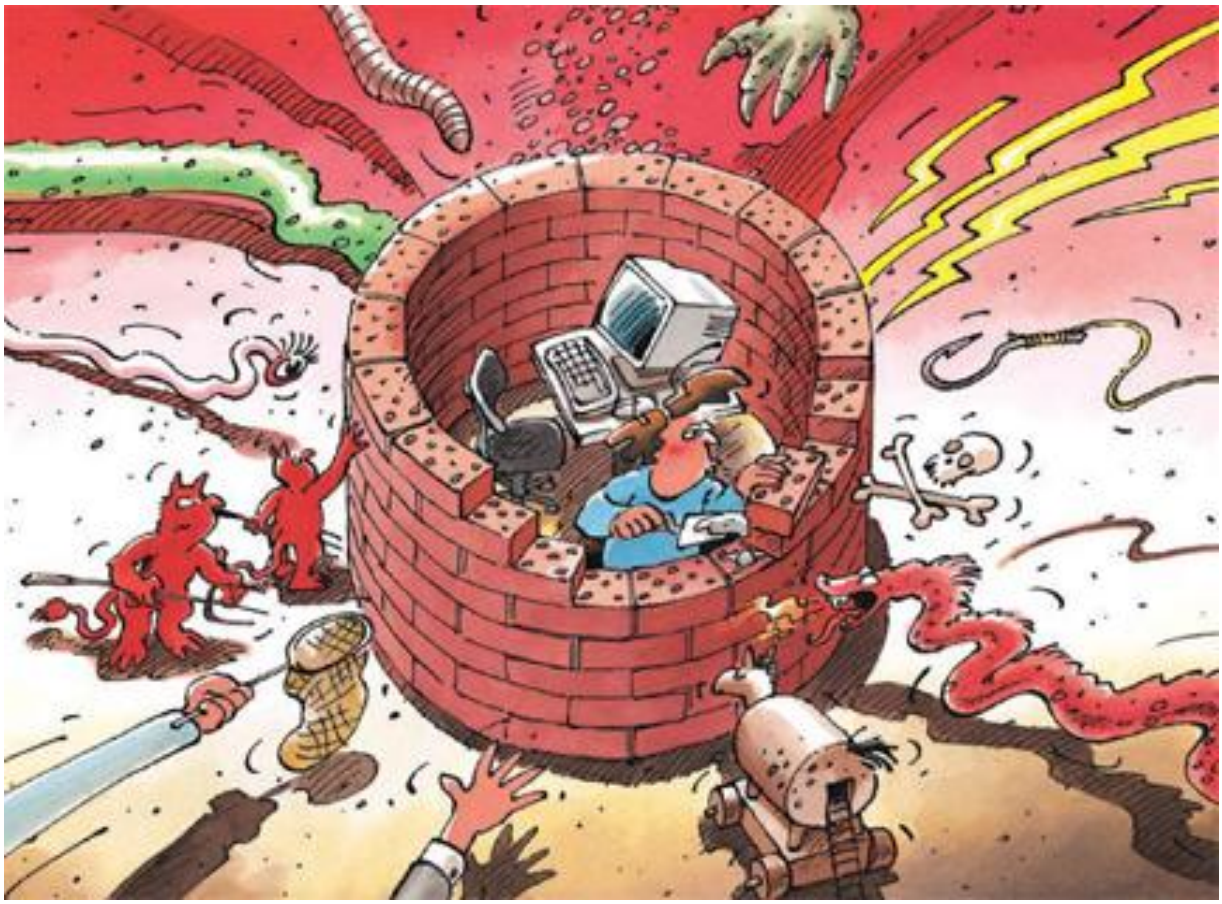
Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

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 2012/II (luglio – dicembre)



Indice

1 Cardini dell'edizione 2012/II 3

2 Introduzione 4

3 Situazione attuale dell'infrastruttura TIC a livello nazionale 5

3.1 Phishing – tendenze attuali 5
3.1.1 Attacchi combinati di phishing e voice-phishing 5
3.1.2 Anche siti di phishing con indirizzi https 5
3.1.3 Aumento degli e-mail di phishing anche senza sito di phishing 6
3.1.4 Primi domini svizzeri soppressi da MELANI su Switch 7

3.2 Fatture false con software nocivo 7
3.3 Impianti di comando aperti sulla rete – anche in Svizzera 8
3.4 Avaria dei semafori nel Cantone di Vaud 10
3.5 Avaria presso Ricardo 10
3.6 Attacco DDoS a Inside Paradeplatz 11
3.7 Regalo di Apple o una potenziale truffa? 12
3.8 Phone Phreaking – vecchie soluzioni alla riscossa 13
3.9 Secondo esercizio paneuropeo «Cyber Europe 2012» – Nuova partecipazione della Svizzera 15

4 Situazione attuale dell'infrastruttura TIC a livello internazionale 16

4.1 Conflitto informatico nel Vicino Oriente – Aggiornamento 16
4.1.1 Gauss: incontro tra cavallo di Troia del banking online e software di spionaggio 16
4.1.2 Shamoon: Spionaggio e sabotaggio presso compagnie petrolifere e gasiere 17
4.1.3 Hacktivismo nel contesto del Vicino Oriente 17

4.2 Attacchi DDoS – Motivazioni, autori e vittime 19
4.2.1 Attacchi DDoS alle banche US 19
4.2.2 Attacco DDoS a un fornitore tedesco di energia elettrica 20
4.2.3 Attacco DDoS ai server del Governo svedese e a banche svedesi 21
4.2.4 Attacchi all'infrastruttura DNS 21

4.3 Vulnerabilità presso i terminali PoS 22
4.4 Attacchi alle istituzioni dell'UE 23
4.5 Inaugurazione del CERT dell'Unione europea e del Centro europeo per la lotta alla criminalità informatica (EC3) 23
4.6 Apriti sesamo: serrature elettroniche negli alberghi 24
4.7 Apparecchiature collegate alle rete di telefonia mobile – grande varietà e poca consapevolezza della sicurezza 25
4.8 App Stores 25
4.9 Obbligo di comunicazione dei casi di hackeraggio e di controllo della rete – Pro e contro 27

5 Tendenze / Prospettive 28

5.1 Lacune dei browser – Strategia a due browser e altre possibilità 28
5.2 Panoramica delle strategie informatiche 29
5.3 Regolamentazione vs. libertà – Come rendere sicuro Internet? 30
5.4 Tracce in Internet – Quali dati rivelano gli utenti quando visitano un sito Web 31
5.5 Dati di imprese terze sui siti delle imprese – Un problema di sicurezza? 33
5.6 Fiducia nella Supply Chain 34

6 Glossario 36

1 Cardini dell'edizione 2012/II

- **Phishing in avanzata**
  Il phishing classico, ossia l'invio di e-mail che inducono la vittima a fornire dati personali, è in avanzata. Gli aggressori si sono concentrati soprattutto sulle carte di credito. Ai numerosi phishing di fattura piuttosto semplice ai danni delle carte di credito si è peraltro aggiunto un nuovo modus operandi che nel secondo semestre del 2013 è stato diretto anche contro gli utenti di e-banking svizzeri.
  ► Situazione attuale in Svizzera: capitolo 3.1

- **DDoS – attacchi massicci contro diverse banche US**
  Gli attacchi alla disponibilità di siti Web, i cosiddetti attacchi di Distributed Denial of Service (DDoS), rientrano fra i maggiori pericoli cui sono esposte le reti. Dal settembre del 2012 vengono annunciati attacchi in parte massicci contro diverse banche americane. Anche altri attacchi alla disponibilità hanno fatto titolo.
  ► Situazione attuale in Svizzera: capitolo 3.6
  ► Situazione attuale a livello internazionale: capitolo 4.2

- **Conflitto informatico nel Vicino Oriente – Aggiornamento**
  Nel quadro delle ricerche relative al software nocivo «Flame» la ditta russa produttrice di antivirus Kaspersky Lab ha scoperto un nuovo software nocivo denominato «Gauss». Nel caso di «Gauss» si tratta del primo caso conosciuto di software sofisticato, destinato presumibilmente allo spionaggio di Stato, che presenta le caratteristiche tipiche di un cavallo di Troia in ambito di banking online. La maggior parte delle apparecchiature infettate si trova in Libano, seguite da Israele e dai Territori palestinesi.

  La compagnia petrolifera saudita Saudi Aramco è stata paralizzata dalle infezioni provocate da un software nocivo. Poco tempo dopo anche il produttore qatariano di gas RasGas ha dovuto isolare la propria rete aziendale. Sebbene manchi una conferma ufficiale, numerosi esperti ritengono che RasGas sia stato colpito dallo stesso software nocivo. Diversi esperti occidentali sospettano che dietro vi sia anche l'Iran (le cui esportazioni di energia sono state sottoposte a forti pressioni dalle sanzioni internazionali), allo scopo di impedire un incremento della produzione di petrolio e di gas negli Stati arabi.
  ► Situazione attuale a livello internazionale: capitolo 4.1, capitolo 4.2

- **Dipendenza dalle TIC nella vita quotidiana – sempre e ovunque**

  Già da alcuni anni non solo i computer o i server sono il bersaglio di attacchi informatici. Ogni sistema informatico può finire nel mirino degli hacker. Lo scassinamento di una porta d'albergo protetta elettronicamente non è che uno di numerosi esempi. La dipendenza della società odierna dalle TIC presenta moltissime sfaccettature.
  ► Situazione attuale in Svizzera: capitolo 3.4
  ► Situazione attuale a livello internazionale: capitolo 4.3, capitolo 4.6

- **Regolamentazione vs. libertà – Come rendere sicuro Internet?**
  Per ora Internet non è sottoposto a una regolamentazione statale e può essere ampiamente disciplinato come spazio libero per il tramite di standard tecnici e di direttive amministrative (le cosiddette «polizie»). Esiste d'altra parte una forte coalizione di Paesi che si adoperano a favore di una regolamentazione di Internet per estendere il loro potere statale di controllo sul cyberspazio e intendono rafforzare la propria sovranità.
  ► Situazione attuale a livello internazionale: capitolo 4.9
  ► Tendenze / Prospettive: capitolo 5.3

2 Introduzione

Il sedicesimo rapporto semestrale (luglio – dicembre 2012) della Centrale d’annuncio e d’analisi per la sicurezza dell’informazione (MELANI) espone le principali tendenze nel campo dei pericoli e dei rischi che accompagnano le tecnologie dell’informazione e della comunicazione (TIC). Presenta un compendio degli avvenimenti in Svizzera e all’estero, illustra i principali sviluppi in ambito di prevenzione ed espone in sintesi le principali attività degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (termini *in corsivo*) sono riunite in un **glossario** alla fine del presente rapporto **(capitolo 6)**. Le valutazioni di MELANI sono di volta in volta evidenziate in un riquadro.

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

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti della seconda metà del 2012. Il capitolo 3 tratta i temi nazionali e il capitolo 4 i temi internazionali.

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

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Phishing – tendenze attuali

Il *phishing* classico, ossia l'invio di e-mail che inducono la vittima a fornire dati personali, è in avanzata. Gli aggressori si sono concentrati soprattutto sulle carte di credito. Ai numerosi episodi di phishing di fattura piuttosto semplice ai danni di carte di credito si è peraltro aggiunto il cosiddetto *voice-phishing*, che nel secondo semestre del 2013 è stato diretto anche contro utenti di e-banking svizzeri. Diversamente dal *software nocivo* utilizzato in ambito di e-banking, simili attacchi necessitano di una semplice infrastruttura e possono essere effettuati anche da persone senza particolari doti tecniche. Per questo nella maggior parte dei casi basta un computer e/o un telefono.

3.1.1 Attacchi combinati di phishing e voice-phishing

Dall'autunno del 2012 si osserva un nuovo modus operandi in ambito di phishing. In questo contesto vengono inviate e-mail in cui si fa credere che l'istituto finanziario ha installato un nuovo sistema di sicurezza per meglio proteggere il conto e-banking. Sempre secondo queste e-mail un collaboratore della banca si metterebbe in contatto telefonico con la vittima per discutere e completare questo nuovo processo. A questo scopo, oltre ai dati personali, la vittima è invitata a fornire anche il proprio numero di telefono.

Successivamente la vittima – e si tratta in questo caso di una novità in Svizzera – viene chiamata telefonicamente dai truffatori e, con il pretesto di migliorare la sicurezza, indotta a indicare la password e il secondo elemento di sicurezza. In merito la vittima viene invitata a immettere un codice nel lettore di carte e a comunicarne il risultato all'aggressore. Grazie a questi dati il truffatore può effettuare il login sul conto di e-banking ed eseguire il pagamento. Se ai fini dell'esecuzione del pagamento viene richiesta la cosiddetta *firma della transazione* il processo viene ripetuto e anche tale firma viene richiesta dal truffatore secondo le medesime modalità. La chiamata telefonica è effettuata di volta in volta in maniera professionale e sovente anche in dialetto svizzero-tedesco.

3.1.2 Anche siti di phishing con indirizzi https

A lungo si è ipotizzato che gli aggressori utilizzassero anche siti di phishing dotati di cifratura (siti https). Nell'autunno dell'anno in rassegna si è infine provveduto, nel caso di diverse ondate di phishing, a inserire link a siti cifrati. Gli URL che iniziano con la sequenza https:// *(hyper text transfer protocol secure)*, stanno a significare che le informazioni immesse sul sito Web corrispondente sono trasmesse in maniera cifrata.

Non è stato tuttavia utilizzato un *certificato* specifico, ma si è semplicemente fatto capo a un *certificato* di un sito Web hackerato. Non si può parlare di una tendenza vera e propria, tanto è vero che si è trattato di casi isolati.

Figura 1: Sito Web protetto da cifratura

3.1.3 Aumento degli e-mail di phishing anche senza sito di phishing

Come già rilevato nell'ultimo rapporto semestrale MELANI[1] i truffatori attivi tramite phishing tentano di accedere ai dati delle vittime anche senza sito classico su un server Web. In merito si sono affermati due diversi metodi: il primo consiste nell'allegare all'e-mail un sito di phishing sotto forma di formulario HTML. All'apertura la pagina HTML è costruita localmente sul computer del destinatario. Se i formulari vengono compilati e si preme il pulsante «Avanti» i dati sono trasmessi «direttamente» all'aggressore.

Il secondo metodo è ancora più semplice: in questo caso il formulario è semplicemente integrato nelle e-mail. Non è necessario nient'altro all'infuori dell'indirizzo di posta elettronica scelto per la truffa. Gli aggressori sfruttano inoltre il fatto che per ogni e-mail può essere definito uno speciale indirizzo di risposta, diverso dall'indirizzo visibile del mittente. L'indirizzo visibile può corrispondere a quello ufficiale di un istituto finanziario; si vede dove l'e-mail è stata effettivamente spedita soltanto dopo aver premuto il pulsante «Rispondi».

[1] MELANI, Rapporto semestrale 2012/1, capitolo 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 28.2.2013).

Von: [redacted]Bank <info[redacted].ch> Gesendet: [redacted]
An: Priorität: normale
Betreff: Aktualisieren Sie Ihre Account-Informationen1 Typ: Text

Sehr geehrte Kundin, sehr geehrter Kunde

Die [redacted] legt grossen Wert auf die Sicherheit im internet Banking.
Die Technologie des [redacted] wird deshalb laufend an die neusten Anforderungen angepasst.

Jetzt informieren wir Sie ьber unsere Softwareaktualisierung gegen Scams und phishing.

Mit der zunehmenden scams und phishing uber internet haben wir uns entschieden unseren kunden zu helfen.

Um Unsere Software zu aktualisieren, senden SIE please This information unten, Nur [redacted] Haben E-Mail an uns Die untenstehenden Informationen.

1) Ihr Name und Vorname:
2) Konto-Nr:
3) [redacted] Vertrag Nummer:
4) Geburtsdatum:
5) Wohnadresse,ort,postleitzahl:
6) Telefon Nummer(Mobil & Home):
7) Email:

Wir freuen uns,sie zu unseren Kunden zдhlen zu dьrfen und grьssen Sie freundlich.

[redacted]
Switzerland.

Von: Datum: [redacted]
An: [redacted]bankag@freemail.hu Text
Cc: Priorität: normale
Betreff: Re: Aktualisieren Sie Ihre Account-Informationen1

> Sehr geehrte Kundin, sehr geehrter Kunde
>
> Die [redacted] legt grossen Wert auf die Sicherheit im internet Banking.
> Die Technologie des [redacted] wird deshalb laufend an die neusten
> Anforderungen angepasst.
> Jetzt informieren wir Sie ьber unsere Softwareaktualisierung
> gegen Scams und phishing.
> Mit der zunehmenden scams und phishing uber internet haben wir uns
> entschieden unseren kunden zu helfen.
> Um Unsere Software zu aktualisieren, senden SIE please This information
> unten, Nur If you [redacted] Haben E-Mail an uns
> Die untenstehenden Informationen.
>
> 1) Ihr Name und Vorname:
> 2) Konto-Nr:
> 3) [redacted] Vertrag Nummer:
> 4) Geburtsdatum:
> 5) Wohnadresse,ort,postleitzahl:
> 6) Telefon Nummer(Mobil & Home):

Figura 2: E-mail di phishing con indirizzo di risposta predisposto. L'e-mail sembra provenire dall'indirizzo di una banca svizzera, ma la risposta è inviata a un servizio gratuito di posta elettronica in Ungheria.

Per l'aggressore entrambi questi metodi presentano il vantaggio di non aver bisogno di un server Web hackerato o specialmente predisposto sul quale collocare il proprio sito di phishing, che potrebbe essere disattivato in tempi relativamente brevi non appena intercettato dalle autorità preposte alla sicurezza o dai provider di hosting.

3.1.4 Primi domini svizzeri soppressi da MELANI su Switch

Per lottare contro l'abuso di indirizzi Internet svizzeri e prevenire gravi pericoli per gli utenti di Internet è stato introdotto un nuovo articolo nel quadro della revisione dell'ordinanza del 6 ottobre 1997 concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT, RS *784.104*; in vigore dal 1° gennaio 2010). Secondo questa nuova disposizione il gestore del registro «.ch» (SWITCH) è tenuto a bloccare un nome di *dominio* e a sopprimerne l'attribuzione a un server di nomi se un ente per la lotta contro la cibercriminalità riconosciuto dall'Ufficio federale delle comunicazioni (UFCOM) ha presentato una richiesta di blocco del nome di dominio o se sussiste il sospetto fondato che questo nome sia utilizzato illegalmente. Questo sia per evitare che si acceda con metodi illegittimi a dati degni di protezione (*phishing*), sia per evitare che per il tramite di questi domini venga distribuito software nocivo (*malware*). SWITCH può ovviamente fare capo autonomamente a queste misure per tutelarsi dai pericoli e mantenerle in vigore per 5 giorni. SWITCH si è avvalso a più riprese di questa possibilità, in particolare per proteggere i visitatori di siti Web hackerati. La stessa Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) ha dovuto fare ricorso a questa competenza.

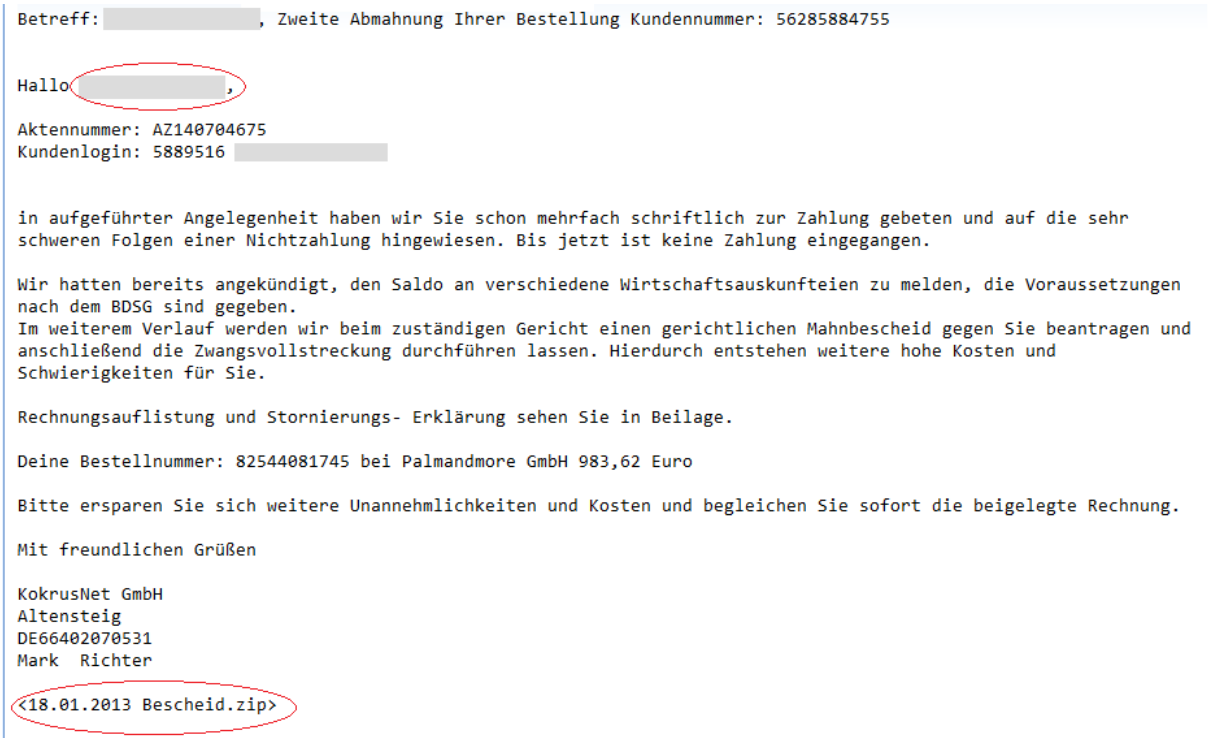
Nel dicembre del 2012 è stato annunciato a MELANI un sito di phishing con indirizzo Internet svizzero. Il dominio è stato creato esclusivamente in un intento di phishing e non si trattava invece – come in numerosi altri casi – di un sito Web hackerato sul quale i truffatori collocano normalmente il sito di phishing in un sottorepertorio. MELANI ha deciso di prorogare di altri 30 giorni il blocco di 5 giorni ordinato da SWITCH e di fare eseguire simultaneamente una verifica dei detentori. Dato che essi non hanno fornito alcuna risposta il dominio è stato definitivamente soppresso.

3.2 Fatture false con software nocivo

Da alcuni mesi sono viepiù in circolazione e-mail inviate da un falso mittente che si riferiscono di volta in volta a un'ordinazione, una fornitura o una fattura (fittizia). MELANI riceve ogni settimana annunci simili. Preannunciando diffide, i costi che ne risulterebbero e possibili procedure giudiziarie i mittenti tentano di creare un retroscena di minaccia tale da indurre i de-

stinatari ad aprire gli allegati per ottenere ulteriori informazioni. In questi casi tuttavia gli allegati contengono unicamente software nocivo, spesso contenuto in un file ZIP.

Per quanto riguarda i casi noti a MELANI, le e-mail sono state inviate in maniera mirata, nel senso che l'intestazione conteneva il nome e il cognome del destinatario. L'invio personalizzato delle e-mail di truffa sembra gradualmente affermarsi perché in tal modo si fa leva sulla fiducia.



Betreff: , Zweite Abmahnung Ihrer Bestellung Kundennummer: 56285884755

Hallo ,

Aktennummer: AZ140704675
Kundenlogin: 5889516

in aufgeführter Angelegenheit haben wir Sie schon mehrfach schriftlich zur Zahlung gebeten und auf die sehr schweren Folgen einer Nichtzahlung hingewiesen. Bis jetzt ist keine Zahlung eingegangen.

Wir hatten bereits angekündigt, den Saldo an verschiedene Wirtschaftsauskunfteien zu melden, die Voraussetzungen nach dem BDSG sind gegeben.
Im weiterem Verlauf werden wir beim zuständigen Gericht einen gerichtlichen Mahnbescheid gegen Sie beantragen und anschließend die Zwangsvollstreckung durchführen lassen. Hierdurch entstehen weitere hohe Kosten und Schwierigkeiten für Sie.

Rechnungsauflistung und Stornierungs- Erklärung sehen Sie in Beilage.

Deine Bestellnummer: 82544081745 bei Palmandmore GmbH 983,62 Euro

Bitte ersparen Sie sich weitere Unannehmlichkeiten und Kosten und begleichen Sie sofort die beigelegte Rechnung.

Mit freundlichen Grüßen

KokrusNet GmbH
Altensteig
DE66402070531
Mark Richter

<18.01.2013 Bescheid.zip>

Figura 3: Esempio di fattura falsa con intestazione personalizzata e software nocivo allegato (Bescheid.zip).

3.3 Impianti di comando aperti sulla rete – anche in Svizzera

La sicurezza degli impianti industriali di comando non viene tematizzata dai soli esperti di sicurezza, ma sempre più anche dai media[2]. Secondo l'Industrial Control System *CERT* (ICS-CERT) statunitense, che ha pubblicato un avvertimento[3] corrispondente lo scorso mese di ottobre, sono in aumento gli attacchi a simili sistemi. Il retroscena dell'avvertimento è che viene offerto un numero sempre maggiore di strumenti che consentono agli aggressori di rintracciare e penetrare all'interno di questi sistemi. In merito non sono necessarie speciali nozioni. Lo strumento più conosciuto è indubbiamente il motore di ricerca «SHODAN», in funzione già da alcuni anni, che scandaglia Internet alla ricerca di sistemi *SCADA* di cui abbiamo già parlato in precedenza[4]. Grazie a questo motore di ricerca l'ICS-CERT è stato in grado di rintracciare oltre 500 000 sistemi. Oltre a SHODAN esiste anche l'Every Routable IP Project (ERIPP).

---

2 http://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/report-februar-102.html (stato: 28 febbraio 2013).

3 http://ics-cert.us-cert.gov/index.html (stato: 28 febbraio 2013).

4 MELANI, Rapporto semestrale 2011/2, capitolo 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 28 febbraio 2013).

A ciò fanno riscontro numerosi gestori di impianti industriali di comando che si sono finora focalizzati principalmente sulla stabilità funzionale e meno sulla sicurezza rispetto alle manipolazioni. Ciò può anche derivare dal fatto che molti di essi non sanno neppure se i loro sistemi siano effettivamente collegati a Internet. Inoltre parecchi produttori programmano password universali con codice fisso per poter accedere ai sistemi anche in caso di perdita dei dati di accesso. Queste password d'emergenza hanno il vantaggio di consentire l'esercizio stabile delle apparecchiature anche in caso di perdita della password, ma costituiscono anche un vettore di attacco. Un altro caso è stato reso noto al pubblico nell'agosto del 2012 da Justin W. Clarke, un ricercatore nel campo della sicurezza. Clarke ha individuato nel sistema operativo proprietario Rugged OS, utilizzato nelle centrali elettriche o in ambito di sorveglianza del traffico, una *chiave RSA* segreta a codice fisso. Se questa chiave fosse nota il traffico cifrato di rete potrebbe essere decriptato e intercettato. L'ICS-CERT ha pubblicato un avvertimento in merito[5].

Un'ulteriore problematica è stata identificata da Phil Kernick, un esperto australiano nel campo della sicurezza. Praticamente in tutti gli eventi concernenti i sistemi *SCADA* analizzati da Kernick era implicato un software nocivo, non tuttavia diretto specialmente contro i sistemi SCADA. Si trattava ad esempio di *malware* convenzionali ai danni dell'e-banking. Queste infezioni hanno minato la stabilità dei sistemi, di tanto in tanto soggetti a crash. Ciò può avere gravi ripercussioni per i sistemi SCADA. Ne è generalmente all'origine il fatto che le reti di controllo e Office non sono separate in modo netto. Anche la possibilità di collegare schede di memoria USB o computer mobili estranei (p. es. da parte di collaboratori o di partner contrattuali esterni) è sovente problematica perché mancano le necessarie politiche di utente e/o ostacoli tecnici.

In linea di massima si dovrebbero collegare macchine a Internet soltanto quando è indispensabile al loro esercizio. Questi sistemi dovrebbero ovviamente essere sufficientemente protetti da un firewall a forti password. Per impedire la trasmissione di malware dai computer d'ufficio ai sistemi SCADA entrambe le reti devono essere separate.

Da quando MELANI ha reso conto nel suo rapporto semestrale 2011/2 delle modalità di individuazione in Svizzera dei sistemi SCADA vulnerabili grazie al motore di ricerca SHODAN, sono stati rintracciati siffatti sistemi anche nel corso dell'anno in rassegna. Non erano protetti da password o lo con una password che avrebbe dovuto essere modificata alla messa in esercizio. Questi obiettivi potenziali non vanno generalmente classificati come delicati, ma il fatto che all'atto dell'installazione di un sistema di comando con collegamento a Internet non venga modificata la password per difetto costituisce una grave violazione dei principi fondamentali di sicurezza informatica. La possibilità ad esempio di accedere alla rete di riscaldamento o di condizionamento dell'aria di un esercizio terzo e di manipolarla potrebbe provocare gravi problemi in determinate circostanze.

Inoltre l'integrazione parziale e le possibilità di accesso ad altre applicazioni amministrative interne all'azienda, come il software di fatturazione e simili, apre la via ad ulteriori potenziali abusi. In linea di massima tutti i sistemi industriali di controllo non dovrebbero essere collegati a Internet. Qualora ciò fosse assolutamente indispensabile occorre particolare cautela con questo modo di procedere.

[5] http://ics-cert.us-cert.gov/pdf/ICS-ALERT-12-234-01.pdf (stato: 28 febbraio 2013).

3.4 Avaria dei semafori nel Cantone di Vaud

Il 16 luglio 2012 si sono verificati ostacoli al traffico e una coda chilometrica sulla tratta autostradale tra Losanna e Chexbres in seguito un'avaria informatica del sistema di controllo del traffico del Cantone di Vaud. Alle 16 il servizio di sorveglianza del traffico della polizia vodese aveva rilevato dei problemi tecnici. Poco tempo dopo il sistema non reagiva più e la segnaletica è rimasta bloccata sulle impostazioni di quel momento. Nella galleria del Flonzaley la corsia sinistra è rimasta bloccata e non ha più potuto essere liberata al traffico, circostanza che ha provocato una coda di 15 chilometri. Dopo l'intervento manuale da parte di un tecnico la situazione del traffico tra Losanna e Chexbres ha cominciato a migliorare lentamente a partire dalla 19:30. L'avaria informatica ha potuto essere risolta soltanto nella notte, verso l'1:40.

Era inoltre rimasta interrotta la trasmissione dell'allarme dalle gallerie delle autostrade vodesi. In caso di incendio o di incidente il sistema di emergenza in galleria non avrebbero funzionato. Le telecamere di sorveglianza hanno invero continuato a inviare immagini, ma non hanno potuto essere manovrate. Per questo motivo sono state piazzate forze di polizia nei punti nevralgici.[6]

Sebbene nella fattispecie si sia trattato di un incidente e non di un attacco, questo esempio illustra chiaramente le innumerevoli sfaccettature della dipendenza dalle TIC della società odierna. Anche nel caso della segnaletica in ambito di traffico stradale si ricorre sempre più a sistemi TIC per affrontare il costante aumento del traffico rispetto a un'infrastruttura immutata. Questi sistemi sono pensati in modo da poter essere disinseriti in caso di malfunzionamento o da commutare tutti i segnali su luce lampeggiante gialla. In questo senso è esclusa una situazione nella quale tutti i partecipanti al traffico hanno il segnale sul verde con la conseguenza quindi che si possano verificare incidenti.

3.5 Avaria presso Ricardo

Il 28 ottobre 2012 si sono verificati importanti problemi informatici presso la ditta di asta online Ricardo.ch. Un errore nella banca dati ha fatto sì che durante diverse ore un terzo circa dei clienti non abbia potuto presentare offerte. Ne è conseguito che i prodotti sono stati in maggior parte venduti a un prezzo nettamente inferiore al loro valore perché nonostante l'avaria le aste sono proseguite fino alla fine, ma non è più stato possibile presentate offerte. È noto che nel caso delle aste gli ultimi minuti sono i più lucrativi. Ricardo.ch ha successivamente chiarito che le offerte giunte a conclusione durante questa avaria «dovevano in ogni caso essere lasciate al compratore anche al prezzo raggiunto».

Due settimane dopo e probabilmente a seguito di diverse proteste da parte dei clienti la dichiarazione citata qui sopra è stata riveduta. Si è presunto che le offerte in questione siano state automaticamente prolungate, ciò che non è stato il caso ovunque. Ricardo.ch ha poi comunicato che in questi casi i venditori non erano in linea di massima vincolati al contratto e che potevano rivolgersi al servizio clientela[7]: Ricardo inoltre si è mostrato condiscendente, procedendo a maggiori rimborsi nei confronti dei venditori.

---

6 http://www.vd.ch/autorites/departements/dse/police-cantonale/medias/communiques-de-presse/articles/disfonctionnement-reseau-informatique-gerant-la-signalisation-routiere-sur-les-autoroutes-vaudois/ (stato: 28 febbraio 2013).

7 http://blog.ricardo.ch/2012/11/teilausfall-von-ricardo-ch-am-28-oktober-2012/ (stato: 28 febbraio 2013).

Come pressoché ogni impresa, anche ricardo.ch esclude la responsabilità per problemi tecnici. Il rischio compete nella maggior parte dei casi al cliente. In questo senso anche le condizioni generali di ricardo.ch prevedono che l'impresa è responsabile soltanto in caso di indisponibilità temporanea del sito Web consecutiva a grave negligenza o intenzionale, in caso di avaria di singole o di tutte le funzioni del sito Web oppure di malfunzionamento del sito Web. In particolare in caso di lieve negligenza ricardo.ch non è responsabile dei problemi tecnici a motivo dei quali le offerte e le controfferte non sono state elaborate o accettate oppure lo sono state con ritardo e in maniera errata[8]. In caso di incidenti, specialmente se vi è in gioco denaro, le condizioni generali sono in genere esposte alle pressioni del pubblico. In casi simili le imprese si mostrano flessibili, soprattutto a causa dei rischi per la loro reputazione.

3.6 Attacco DDoS a Inside Paradeplatz

Nell'arco di tre mesi il sito Web «Inside Paradeplatz» è stato paralizzato a due riprese da cosiddetti attacchi di *Distributed Denial of Service* (attacchi DDoS). Già nel mese di giugno il sito Web era finito nel mirino di sconosciuti che vi avevano indirizzato migliaia di richieste al secondo, rendendolo temporaneamente irraggiungibile. La stessa cosa si è ripetuta nel mese di settembre, con una durata tuttavia nettamente superiore a quella del primo attacco, che si era concluso dopo un giorno e mezzo. Parallelamente al secondo attacco è stato apparentemente compromesso il sito Web personale del gestore, sul quale è stata collocata un'*infezione drive-by*. Secondo il proprietario del sito web, nell'ipotesi che il sito fosse ricercato mediante Google o cliccato veniva visualizzato un avvertimento corrispondente.[9] Secondo le affermazioni del gestore si intendeva impedire che le informazioni fossero diffuse per il tramite di un altro canale. Questi fatti fanno presumere un attacco mirato. In un caso simile è molto complesso individuare l'origine dell'attacco perché le tracce sono camuffate.

Gli *attacchi DDoS* fanno parte dei maggiori pericoli ai quali sono esposte le reti. Il capitolo 4.2. elenca una serie di attacchi DDoS all'estero. Ciononostante questo attacco è evidente e non corrisponde agli attacchi DDoS usuali. Il fatto per l'appunto che sia stato oggetto di attacco anche il sito Web privato del gestore per collocarvi un'*infezione di sito Web* dà spazio a speculazioni. Il motivo addotto dal gestore, ovvero che tramite l'infezione del sito Web gli aggressori intendessero impedire che le informazioni fossero diffuse per mezzo di un altro canale, è solo in parte plausibile. Questo perché per impedire in maniera semplice la diffusione delle informazioni anche il sito privato poteva essere colpito con un attacco DDoS.

Un'altra speculazione in merito a questo attacco è quella secondo la quale gli aggressori volessero infettare in maniera mirata con software nocivo i computer di persone parte della cerchia del gestore per accedere alle informazioni. Nel caso delle persone facenti parte della cerchia del gestore è particolarmente grande la probabilità che esse accedano per prime al sito Web privato del gestore per esaminare per quale ragione il sito ufficiale non funzioni più.

[8] http://www.ricardo.ch/ueber-uns/Portals/ch-ueber-uns/Docs/downloads-pdf-de/AGB_DE.pdf (stato: 28 febbraio 2013).

[9] http://insideparadeplatz.ch/2012/08/28/inside-paradeplatz-im-visier-von-hackern/ (stato: 28 febbraio 2013).

3.7 Regalo di Apple o una potenziale truffa?

Nel mese di novembre 2012 è stato diffuso un messaggio SMS in cattivo tedesco secondo cui il destinatario aveva vinto un regalo da parte di Apple. In considerazione delle numerose segnalazioni giunte a MELANI sembra che questo messaggio SMS sia stato inviato su vasta scala. Il messaggio conteneva un codice di vincita e un link. I nomi di dominio erano sempre costruiti secondo il medesimo modello e contenevano di volta in volta *domini Top Level* «.cc»

Figura 4: Messaggio SMS con l'annuncio della presunta vincita.

Per ricevere l'iPhone 5 gratuito occorreva immettere sul sito Web indicato il codice ricevuto con il messaggio SMS. Dall'analisi è emerso che qualsiasi numero dava accesso al sito successivo. Questa sola circostanza rende il messaggio SMS dubbioso e fa presumere che l'intera campagna fosse unicamente un pretesto per indurre i destinatari a fare qualcosa.

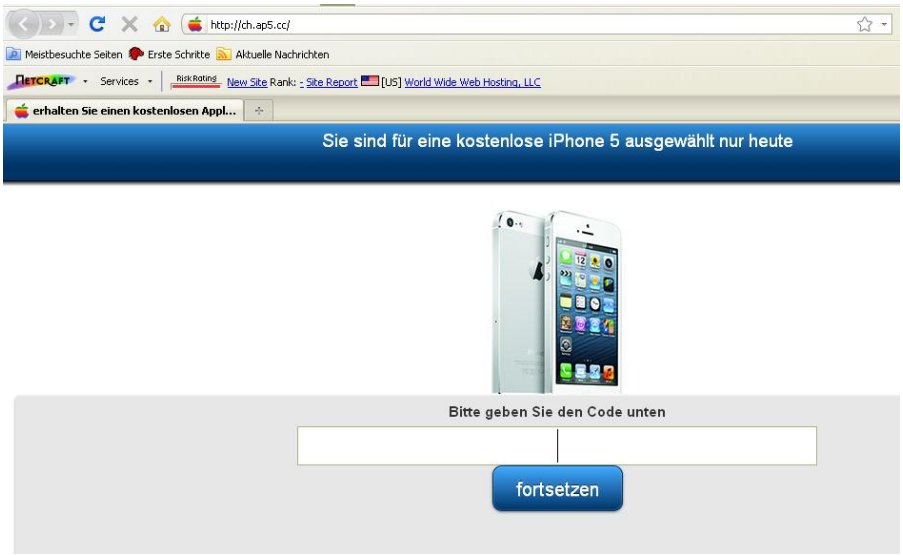


Figura 5: Sito sul quale doveva essere immesso il codice della presunta vincita.

Dopo l'immissione del codice di vincita si veniva dirottati sul sito Web di una ditta denominata «Ziinga». Questa ditta offre un cosiddetto shopping di intrattenimento («entertainment shopping»), in sostanza una piattaforma di aste. A chi giunge a questo sito vengono richiesti nome, cognome, indirizzo e-mail e sesso, come pure l'accettazione delle condizioni generali. Per la vittima tutto questo è plausibile perché crede ancora di avere vinto un iPhone. Con l'accettazione della CGA si conclude tuttavia un contratto platino di socio a 89.99 $ al mese.

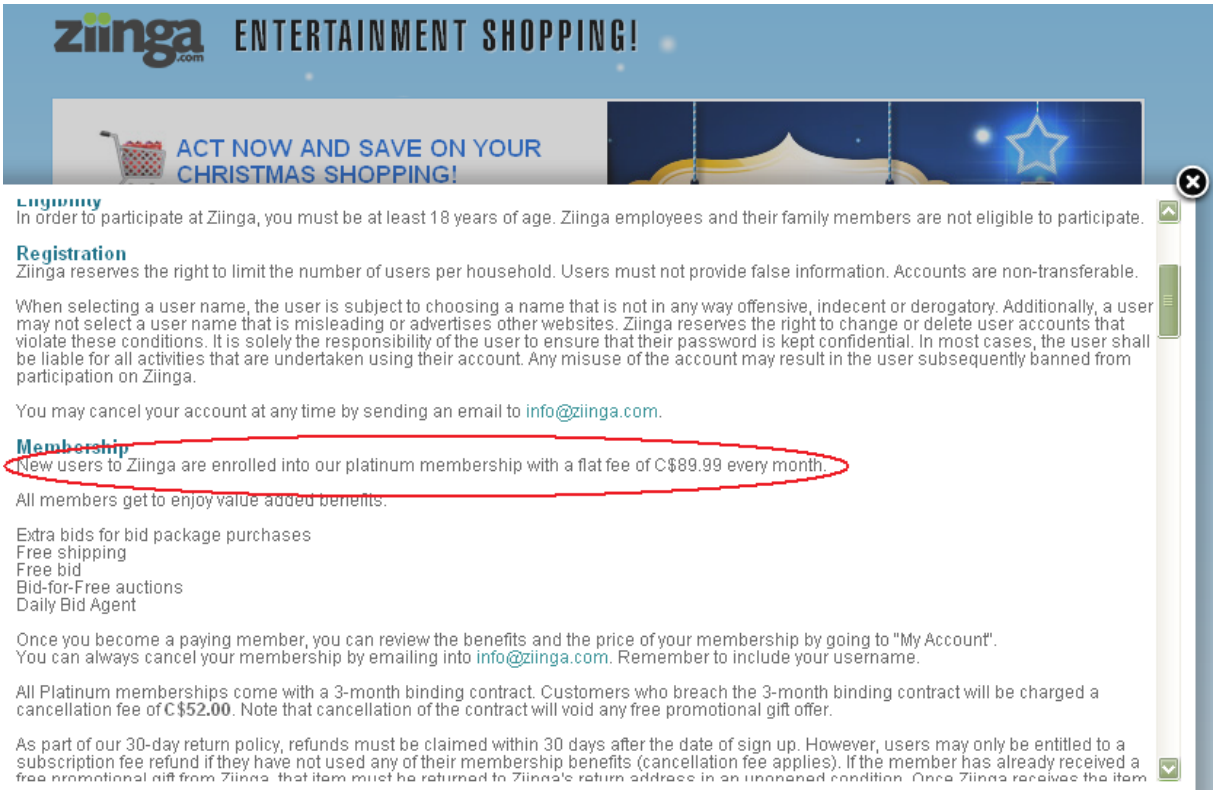


Figura 6: Condizioni generali di Ziinga (stato: 30. novembre 2012).

La società Ziinga è citata anche su Wikipedia. L'articolo è catalogato come «non neutrale», ma fornisce comunque alcune indicazioni. Anche il fatto oche i costi per l'adesione a membro non sono chiaramente visibile sul sito è stato criticato a più riprese[10]. La qualità di membro può successivamente essere disdetta in ogni momento, ma ciò esige un contributo di disdetta di £ 28 (risp. USD 52). In questo caso tuttavia Ziinga ha preso le distanze dall'invio del messaggio SMS e ha escluso un nesso con la propria società. Rimane tuttavia la questione di chi, a parte Ziinga, abbia interesse all'invio di messaggi SMS di questo genere. Non è ancora stato accertato chi abbia effettivamente inviato il messaggio, ma sui siti Web indicati non sono stati individuati software nocivi.

Un altro motivo dell'invio del messaggio SMS potrebbe essere stata la verifica della validità di numeri di telefonia mobile. Ogni link inviato era infatti unico e conteneva un codice che faceva concludere al numero di telefonia mobile corrispondente. Quando il destinatario cliccava il link veniva segnalato al mittente che il numero di telefonia mobile era in esercizio. Se la richiesta è inoltre abbinata all'immissione di un indirizzo e-mail, allora è addirittura possibile assegnare il numero di telefonia mobile a un indirizzo e-mail. Questi dati possono successivamente essere utilizzati in maniera mirata per attacchi phishing oppure essere rivenduti a cerchie interessate.

3.8 Phone Phreaking – vecchie soluzioni alla riscossa[11]

Le prime pratiche di *phreaking* risalgono ai tempi dell'apparizione dei servizi automatici di commutazione delle compagnie telefoniche e hanno raggiunto il loro apice tra gli anni Set-

[10] http://en.wikipedia.org/wiki/Ziinga#Controversy (stato: 28 febbraio 2013).

[11] Il presente articolo si basa su un rapporto di fedpol, l'Ufficio federale di polizia, messo gentilmente a disposizione di MELANI.

tanta e la metà degli anni Novanta. L'invenzione del phreaking è attribuita a una persona soprannominata «Cap'n Crunch». L'obiettivo era di accedere ai sistemi telefonici per in seguito ad esempio telefonare gratuitamente. Ne sono in particolare colpiti i raccordi telefonici della rete fissa e in tempi recenti anche i sistemi *VoIP* dei privati e i sistemi telefonici di imprese di qualsiasi dimensione. In caso di riuscita dell'attacco i sistemi telefonici possono essere utilizzati abusivamente per qualsiasi forma di truffa.

I criminali accedono in particolare ai sistemi di telefonia facendo capo a un software di manutenzione. Tale software è sovente protetto da un solo *PIN* standard. I criminali riescono comunque sempre ad hackerare anche sistemi telefonici ben protetti e oggetto di una buona manutenzione. Per millantare un'identità e rendere difficile l'inseguimento, i criminali fanno ad esempio capo al cosiddetto *spoofing*. Grazie allo spoofing è possibile camuffare il proprio numero e simulare un altro numero. La tecnica necessaria a questo scopo e i PIN standard possono essere trovati su Internet.

Nel caso del modus operandi più frequente si utilizzano cosiddetti numeri a valore aggiunto. I numeri a valore aggiunto sono prestazioni di servizi che vanno al di là della telefonia, ma sono pagate tramite l'abbonamento telefonico. Un esempio per quanto riguarda la Svizzera sono i numeri 0900. Nel caso di questa variante l'aggressore si procura in una prima fase l'accesso al sistema di telefonia di un'impresa. Ad avvenuto controllo i criminali possono allacciare i collegamenti dell'impianto telefonico a un numero a valore aggiunto che hanno creato. Affinché l'impresa non si accorga troppo rapidamente di ciò che sta accadendo gli attacchi sono effettuati all'infuori delle ore d'ufficio. Dato che nel caso di questa variante i criminali devono coprire numerosi raccordi telefonici dell'impresa colpita la probabilità che la truffa venga scoperta durante le ore d'ufficio è sensibilmente più elevata. L'attacco principale è sovente preceduto da attacchi minori. L'utilizzazione abusiva di numeri a valore aggiunto viene in genere effettuata nei Paesi dove è difficile perseguire i colpevoli.

Un'ulteriore variante riguarda i sistemi di pagamento online. Le carte a credito online sono smerciate da diversi servizi di vendita, come i chioschi e i distributori di carburante. I criminali millantano mediante *spoofing* il numero di servizio di un'impresa che emette carte a credito online e contattano per questo tramite singoli servizi di vendita. Il personale, ritenendo di essere collegato con un rappresentante dell'impresa che emette le carte, fornisce i codici e le informazioni delle carte a credito online. Gli averi sulle carte sono immediatamente incassati su Internet. Ciò rende impossibile impedire il danno. Per poter sfruttare questa forma di phone phreaking i criminali devono disporre di conoscenze insider. Da un canto deve essere noto il pertinente numero di servizio dell'impresa e, d'altro canto, i criminali devono conoscere i processi tecnici e avere dimestichezza con gli iter di supporto.

Tramite i sistemi *VoIP* è altresì possibile effettuare cosiddetti attacchi *vishing* (cfr. in merito il capitolo 3.1).

Condizione imperativa del phone *phreaking* sono speciali conoscenze tecniche. Su Internet si possono invero trovare istruzioni dettagliate, ma si tratta sempre di saper reagire a nuove misure di sicurezza e di adeguare i modi di procedere in maniera corrispondente, ciò che implica in parte iter di programmazione. Per poter penetrare in sistemi di telefonia ben protetti e sicuri sono inoltre necessarie informazioni dettagliate sull'organizzazione, gli iter e i collaboratori dell'impresa, ciò che implica sovente conoscenze insider. Occorre peraltro partire dall'idea che in futuro il phone *phreaking* sarà sempre più facile e comprenderà ulteriori settori. Esiste ad esempio il pericolo che gli *smartphone* ne siano viepiù colpiti – anche l'hackeraggio di *smartphone* può essere designato come *phreaking*. I criminali sfruttano ad esempio il controllo del telefono mobile acquisito mediante hackeraggio per utilizzare servizi SMS soggetti a pagamento.

3.9 Secondo esercizio paneuropeo «Cyber Europe 2012» – Nuova partecipazione della Svizzera

Il 4 ottobre 2012 oltre 500 specialisti in informatica hanno partecipato al secondo esercizio «Cyber Europe 2012» esteso a tutta l'Europa. L'esercizio era incentrato sulla comunicazione e la coordinazione a livello nazionale ed europeo in vista del miglioramento della resistenza delle strutture critiche di informazione. «Cyber Europe 2012» ha costituito una pietra miliare nel rafforzamento della cooperazione, della prontezza a tutelarsi e della capacità di reazione nell'ipotesi di una crisi paneuropea della sicurezza informatica.[12]

Cyber Europe 2012 perseguiva tre obiettivi:

- un test dell'effettività e della scalabilità delle procedure standard che disciplinano la cooperazione delle autorità in Europa;
- un test della cooperazione tra settore pubblico e privato in Europa;
- l'individuazione di lacune e di sfide nel caso di gravi perturbazioni transfrontaliere di rete in Europa.

Hanno partecipato a questo esercizio i 29 Stati membri dell'UE e gli Stati dell'AELS (Associazione europea di libero scambio); 25 di questi Paesi (fra i quali anche la Svizzera) hanno partecipato attivamente all'esercizio, mentre i rimanenti quattro erano presenti come osservatori. All'esercizio hanno partecipato anche diversi organismi dell'UE. Vi hanno partecipato complessivamente 339 organizzazioni con in tutto 571 singoli attori. Conformemente a una raccomandazione e diversamente dall'esercizio precedente «Cyber Europe 2010» vi hanno partecipato questa volta anche attori del settore privato. Per quanto riguarda la Svizzera si è trattato di due imprese del settore delle telecomunicazioni e del settore finanziario. Nell'impianto destinato all'esercizio la collaborazione tra attori del settore pubblico e del settore privato era tuttavia limitata al livello nazionale, mentre il settore pubblico collaborava anche a livello transnazionale.

Lo scenario dell'esercizio era incentrato su ampie perturbazioni delle rete in Europa che colpivano i Paesi partecipanti. Esso partiva dall'ipotesi che gli aggressori si fossero uniti per sferrare un cyberattacco massiccio contro l'Europa, diretto anzitutto contro le prestazioni elettroniche di servizi con attacchi DDoS. Ne erano ad esempio toccati l'e-government e i servizi finanziari (e-banking ecc.). Queste perturbazioni della rete costituivano una sfida sia per i partecipanti del settore pubblico, sia per quelli del settore privato, ed esigevano una cooperazione transfrontaliera.

Grazie all'esercizio «Cyber Europe 2012» è stato possibile esaminare, comprendere e valutare gli attuali meccanismi europei di sostegno alla cooperazione nel settore della sicurezza informatica. L'esercizio ha inoltre rafforzato la collaborazione tra i partecipanti.

Esperienze e insegnamenti:

- tutti i Paesi partecipanti erano pienamente riuniti durante la fase di esercizio. Nel corso dell'esercizio si è assistito a numerose interazioni bilaterali e multilaterali a livello internazionale;
- con l'ausilio di tutta una serie di processi standard e di strumenti di comunicazione è stata possibile una buona valutazione della situazione nei diversi Paesi durante la simulazione della crisi di sicurezza informatica;

[12] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_DE_TRA.pdf (stato: 28 febbraio 2013).

- i processi standard hanno nondimeno evidenziato determinate vulnerabilità a livello di scalabilità in considerazione del forte numero di Paesi partecipanti;
- per raggiungere una capacità di reazione rapida ed efficace in tutta l'Europa occorre che i servizi competenti abbiano dimestichezza con i processi standard;
- in Svizzera i contatti con i partecipanti in provenienza dal settore privato sono bene affermati. Il grande numero di informazioni e il loro trattamento (handling) impongono tuttavia una certa sfida;
- per rendere possibile una cooperazione efficace e senza intoppi sono imprescindibili infrastrutture e strumenti di comunicazione adeguati, stabili e moderni;
- «Cyber Europe 2012» ha contribuito a istituire la fiducia tra i Paesi. È unicamente su questa base che si potrà fare capo proficuamente e tempestivamente a misure volte a ridurre i rischi in caso di crisi reale della sicurezza informatica. L'esercizio si è rivelato proficuo sia per le nuove relazioni sia per quelle già esistenti.

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Conflitto informatico nel Vicino Oriente – Aggiornamento

4.1.1 Gauss: incontro tra cavallo di Troia del banking online e software di spionaggio

Nel quadro delle ricerche relative al software nocivo «Flame»[13] la ditta russa produttrice di software antivirus Kaspersky Lab ha scoperto un nuovo software nocivo denominato «Gauss». Nel caso di «Flame» e «Gauss» fa specie il fatto che l'architettura, la struttura del modulo, il codice di base e le forme di comunicazione siano molto analoghe a quelle del *Command & Control Server*. In considerazione di queste affinità è evidente l'identità di origine di questi due software nocivi.

Dalle indicazioni risulta che Gauss è attivo dal settembre 2011 e ha potuto presumibilmente spiare decine di migliaia di computer prima della sua scoperta nel giugno del 2012. La maggior parte delle apparecchiature infettate si trova in Libano, seguite da Israele e dai Territori palestinesi.

Le funzioni di Gauss comprendono la lettura delle password su Internet, di indicazioni relative ai conti bancari online, di *cookie* e in particolare dei dati di configurazione del computer infettato. Il software nocivo è stato programmato in maniera tale da rendere possibile il procacciamento di dati nel contesto dei conti presso banche libanesi.

[13] In merito a «Flame» cfr. MELANI, Rapporto semestrale 2012/1, capitolo 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 28.2.2013).

Nel caso di «Gauss» si tratta del primo caso conosciuto di software sofisticato, destinato presumibilmente allo spionaggio di Stato, che presenta le caratteristiche tipiche di un cavallo di Troia in ambito di banking online. Diversamente dai cavalli di Troia noti in ambito di banking online utilizzato dai truffatori su Internet, le funzioni corrispondenti di Gauss non procurano alcun danno finanziario all'utente, ma spiano unicamente quali transazioni bancarie sono effettuate con il computer infettato.

4.1.2 Shamoon: Spionaggio e sabotaggio presso compagnie petrolifere e gasiere

Il 15 agosto 2012 i computer della rete d'ufficio della Saudi Aramco, la compagnia petrolifera dello Stato saudita, sono stati paralizzati da un'infezione con software nocivo. Il software, denominato «Shamoon», ha raccolto dati sui computer infettati e li ha trasmessi agli aggressori prima di cancellarli e di sovrascrivere il *Master Boot Record (MBR)*. In tal modo i computer infettati sono stati resi inutilizzabili e hanno necessitato di una nuova installazione. Secondo le indicazioni fornite dalla Saudi Aramco sono stati infettati oltre 30 000 computer della rete d'ufficio – l'infezione non ha però avuto alcun influsso sulla produzione di petrolio e sul relativo commercio. Tutte le apparecchiature infettate hanno potuto essere ripristinate.

Poco tempo dopo anche il produttore qatariano di gas RasGas ha dovuto staccare la propria rete aziendale dal mondo esterno. Sebbene manchi una conferma ufficiale, numerosi esperti ritengono che RasGas sia stato colpito da Shamoon.

La funzionalità di Shamoon qui descritta ricorda il software «Wiper»[14], all'origine di scompiglio in Iran. L'analisi di Shamoon consente tuttavia di concludere che non si è in presenza della medesima origine.
Gli oneri assunti per effettuare questo attacco non sono irrilevanti, ragione per la quale essi fanno apparire probabile la partecipazione di uno Stato o perlomeno il sostegno agli autori da parte di uno Stato. Diversi esperti occidentali presumono dietro a ciò anche sforzi dell'Iran (le cui esportazioni di energia sono state sottoposte a forti pressioni dalle sanzioni internazionali), volti a impedire un incremento della produzione di petrolio e di gas negli Stati arabi.

4.1.3 Hacktivismo nel contesto del Vicino Oriente

Nel secondo semestre del 2012, oltre ai due attacchi sensazionali menzionati qui sopra, si sono verificati anche diversi attacchi di minori dimensioni con riferimento al Vicino Oriente. Eccone una scelta:

- nel mese di agosto è stata hackerata per la seconda volta la piattaforma blog dell'agenzia di informazioni Reuters e una prima volta il conto Twitter @ReutersTech. Tutto questo di volta in volta nell'intento di diffondere propaganda e notizie false sugli avvenimenti in Vicino Oriente;

- sempre nel mese di agosto sono stato inviati in maniera mirata e-mail a dissidenti siriani esortandoli a scaricare un presunto programma di sicurezza denominato «Anti Hacker»

[14] In merito a «Wiper» cfr. MELANI, Rapporto semestrale 2012/1, capitolo 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 28.2. 2013).

per proteggersi da aggressori malintenzionati. Dietro quel programma di sicurezza si celava un software di spionaggio[15];

- un gruppo di hacker (autodichiarati) pachistani ha protestato nel mese di settembre contro il film controverso «Innocence of the Muslims», procedendo alla deturpazione (defacement) di diversi siti Web. A metà novembre questo gruppo ha in particolare poi anche messo nel mirino siti Web israeliani. A quel momento era ancora in atto l'«Operation Israel» di Anonymous. Questa operazione era stata lanciata dopo che il Governo israeliano aveva manifestato l'intenzione di tagliare i collegamenti di telecomunicazione con la Striscia di Gaza;

- Anonymous ha dichiarato la «guerra» al regime di Assad perché quest'ultimo ha interrotto i collegamenti Internet con l'estero[16];

- un gruppo di hacker ha preso possesso di diversi conti di utente del vice premier israeliano diffondendovi propaganda pro palestinese. Non si trattata apparentemente di una parte dell'«Operation Isreael» di Anonymous, bensì di un atto autonomo di solidarietà con la Palestina;

- in considerazione degli avvertimenti relativi a un importante attacco con software nocivo contro la polizia israeliana i computer della polizia sono stati staccati preventivamente da Internet per un certo periodo di tempo. In tal senso i funzionari sono stati sensibilizzati a non collegare alcuna apparecchiatura USB ai computer di servizio. Il sistema interno di computer della polizia è comunque rimasto in funzione tutto il tempo – solo il traffico e-mail con le autorità non è stato temporaneamente possibile;

- l'autorità internazionale dell'energia atomica (IAEA) ha annunciato un attacco nel corso del quale gli aggressori si sono procurati i dati personali di contatto di scienziati, poi pubblicati su Internet. Gli hacker hanno minacciato di pubblicare ulteriori informazioni sensibili nell'ipotesi che continuassero gli attacchi diretti contri scienziati nucleari iraniani – nel corso degli ultimi anni numerosi scienziati sono rimasti vittima di attentati in Iran, attentanti di cui il Governo iraniano attribuisce la responsabilità agli USA e a Israele;

- la spocietà Symantec, attiva nel settore della sicurezza, ha scoperto che il worm informatico «Narilam», che sembra soprattutto diretto contro imprese in Iran. Dall'analisi risulta ovvio che questo software nocivo non è destinato allo spionaggio, ma attacca in maniera mirata banche dati rilevanti dal profilo economico (p.es. banche dati di contabilità), dove modifica o sopprime serie di dati[17].

Si possono fare speculazioni sull'origine di questi singoli attacchi. Sarebbe comunque difficile fornire la prova che dietro di essi si celano organizzazioni statali, hacker patrioti o simpatizzanti di determinati gruppi e da chi gli autori hanno ricevuto quale sostegno.

---

15 https://www.eff.org/deeplinks/2012/08/syrian-malware-post (stato: 28 febbraio 2013).

16 http://www.youtube.com/watch?v=olZzqa6nwos; http://www.youtube.com/watch?v=xdmlPhWIAuw (stato: 28.2.2013).

17 http://www.symantec.com/connect/blogs/w32narilam-business-database-sabotage (stato: 28.2.2013).

4.2 Attacchi DDoS – Motivazioni, autori e vittime

Nel mondo informatico gli attacchi alla disponibilità dei siti Web, i cosiddetti attacchi di *Distributed Denial of Service (DDoS)*, possono perseguire differenti scopi. Ne abbiamo già trattato in precedenti rapporti semestrali[18]. Inizialmente gli attacchi venivano effettuati soprattutto come atti di vandalismo. Nel frattempo le motivazioni sono cambiate. Si osservano ad esempio attacchi DDoS come strumento di vendetta, di danneggiamento della concorrenza, di racket oppure per motivi politici. Se gli attacchi DDoS di minori dimensioni rimangono perlopiù nascosti e non ne perviene notizia al pubblico, si verificano sempre più attacchi DDoS di maggiori dimensioni volti a ottenere una grande attenzione (mediatica). I siti Web, rispettivamente i server Web, costituiscono in merito l'obiettivo preferito. Ma si può anche trattare di server di posta elettronica, di server *DNS*, di *router* e di *firewall* oppure di altri servizi di Internet. Gli attacchi alle banche US nel secondo semestre del 2012 hanno sicuramente dato il via a una nuova qualità di attacchi. Ma anche altri attacchi alla disponibilità hanno fatto titolo.

4.2.1 Attacchi DDoS alle banche US

Dal settembre del 2012 vengono annunciati attacchi in parte massicci contro diverse banche americane. Ne sono state ad esempio colpite Bank of America, Citigroup, Wells Fargo e diverse altre banche ancora. Finora non si ha avuto notizia di furti, ma nel caso delle banche citate si osservano in continuazione ostacoli nell'accesso ai siti Web.

Il volume di dati degli attacchi ha raggiunto talvolta oltre 60 GB/s. Dall'inizio degli attacchi si è presunto da più fonti che essi provenissero dall'Iran, non però da cerchie criminali, bensì che fossero il fatto di organi statali o che perlomeno fossero stati sostenuti o tollerati da organi di Stato. In questo senso anche un articolo del New York Times indica che secondo membri non designati nominalmente del Governo US dietro questi attacchi si celi l'Iran[19]. Finora tuttavia non è stata fornita la conferma di questa tesi. Per il momento solo il perdurare di questi attacchi e la difficoltà di limitarli fornisce un indizio della possibile esistenza di un nesso statale. Come indicato in questi casi è difficile fornire la prova e l'esperienza insegna che occorre usare prudenza perché da entrambi i lati sono in gioco forti interessi politici. L'Iran dal canto suo ha sempre respinto categoricamente l'accusa di partecipazione a questi attacchi.

Da diverse parti si presume che il motivo degli attacchi vada ricercato nell'embargo economico degli USA nei confronti dell'Iran e che essi vadano considerati come una misura di rappresaglia. Il gruppo Izz ad-Din al-Qassam Cyber Fighters, che ha rivendicato fin dall'inizio gli attacchi, ha indicato come motivazione la diffusione di video su Maometto[20]. Anche a questo proposito si specula che sotto la cappa dell'hacktivismo si celino altre motivazioni[21].

Gli attacchi sono stati perpetrati anche a partire da computer svizzeri. Nella maggior parte dei casi si trattava di server Web con una larghezza di banda relativamente ampia, apposi-

---

18 Cfr. anche HJB 2010/2, capitolo 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (stato: 28.2.2013).

19 http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=1& (stato: 28.2.2013).

20 http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 (stato: 28.2.2013).

21 http://blogs.techworld.com/war-on-error/2013/01/iran-v-usa---the-worlds-first-cyberwar-has-started/index.htm (stato: 28.2.2013).

tamente compromessi a questo scopo. I loro gestori sono stati informati in merito dalla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

Secondo le dichiarazioni delle banche US gli attacchi DDoS perdurano, ma non hanno nel frattempo gravi ripercussioni. Le avarie consecutive agli attacchi DDoS dovrebbero diminuire nelle prime settimane di gennaio, sebbene all'inizio dell'anno gli aggressori abbiano annunciato nuovi attacchi massicci. Gli osservatori considerano questa circostanza come una prova che nel frattempo gli istituti finanziari hanno migliorato con successo le capacità di difesa contro simili attacchi[22]. In questo senso la statistica del traffico delle 13 maggiori istituzioni US presenta nel gennaio del 2013 una disponibilità temporale del 97 per cento, mentre tale disponibilità era del 95 per cento durante la prima fase degli attacchi (1% di un giorno corrisponde a circa 15 minuti).

Nel caso di un attacco DDoS oltre ai preparativi tecnici vanno adottate misure organizzative e di comunicazione. Ciò che l'impresa comunica e le modalità di detta comunicazione costituisce indubbiamente un fattore decisivo. Una strategia di comunicazione può fungere da prima misura contro le ripercussioni di attacchi DDoS. Una comunicazione sventata può invece costituire la miccia di un attacco (rispettivamente di un nuovo attacco) DDoS. I rischi e le ripercussioni di una comunicazione a un ampio pubblico devono pertanto essere valutati in una fase avanzata.

Un secondo fattore decisivo è sicuramente la previdenza tecnica. È molto più semplice fare preparativi in una fase avanzata che non quando le infrastrutture dell'impresa sono sotto attacco. Ciò vale in particolare per le imprese la cui esistenza dipende in ampia misura da prestazioni di servizi o da vendite online. Nell'ipotesi normale il provider upstream dispone dell'esperienza e della possibilità di messa a disposizione di soluzioni corrispondenti per difendersi dagli attacchi DDoS.

È ovvio che le misure menzionate qui sopra valgono in particolare per le infrastrutture critiche di informazione. Lo scambio di informazioni è di estrema importanza se l'attacco DDoS riguarda un intero settore economico o è addirittura intersettoriale. Sarà così possibile impedire l'attacco o perlomeno attutirlo. MELANI garantisce un simile scambio di informazioni ai gestori di infrastrutture critiche in Svizzera.

4.2.2 Attacco DDoS a un fornitore tedesco di energia elettrica

I server Web dell'esercente tedesco delle rete di distribuzione di energia elettrica «50 Hertz Transmission» sono rimasti vittima di un attacco DDoS per parecchi giorni. L'impresa allaccia un terzo circa della Germania alla rete di energia elettrica. La distribuzione di energia elettrica non è stata tuttavia ostacolata in nessun momento perché gli aggressori non avevano preso di mira i sistemi di controllo (*SCADA*), ma «soltanto» i server Web dell'impresa. L'attacco ha parimenti colpito e distrutto la comunicazione a mezzo posta elettronica. 50 Hertz ha reagito staccando i server dalla rete.

Secondo quanto riferisce la stampa, per effettuare l'attacco sono stati utilizzati migliaia di *indirizzi IP* in Europa dell'Est e specialmente in Russia [23]. Non si sa se gli autori provengano da questa regione o vi abbiano soltanto affittato una rete bot, né sono chiari i motivi di questo attacco.

---

[22] http://www.bankinfosecurity.com/are-banks-winning-ddos-battle-a-5434 (stato: 28.2.2013).

[23] http://www.welt.de/wirtschaft/energie/article111369975/Russische-Hacker-attackieren-Stromnetzbetreiber.html (stato: 28.2.2013).

La pressione economica fa sì che i sistemi siano sempre più uniformi e che non soltanto singole componenti ma intere sottostazioni vengano comandate a distanza ed esercitate senza personale. Tuttavia nella maggior parte dei casi la rete amministrativa e la rete di comando sono tuttora sempre strettamente separate. La tecnologia di rete pressoché identica induce nondimeno sempre più a riunire la rete aziendale alla rete di comando per semplificare i processi amministrativi. Le diverse esigenze poste alle misure di sicurezza e le possibilità in questo campo vanno comunque sempre prese in considerazione.

Occorre inoltre considerare che nel caso appunto dei fornitori di energia elettrica non soltanto l'attacco ai sistemi di comando può avere ripercussioni sulla stabilità delle rete elettrica; anche i sistemi che forniscono informazioni per mantenere la stabilità della rete possono essere essenziali. Ora proprio questi sistemi sono sempre più collegati alla rete amministrativa, creando così un possibile punto di attacco.

4.2.3 Attacco DDoS ai server del Governo svedese e a banche svedesi

All'inizio del mese di ottobre si sono verificati attacchi DDoS contro diverse imprese e autorità svedesi. Ne sono stati vittima oltre alle banche i siti Web delle ferrovie di Stato svedesi Staatsbahn SJ, l'agenzia di informazione TT e i server della Difesa. Si presume che il motivo degli attacchi sia la richiesta di estradizione della Svezia nei confronti di Julian Assange. Soltanto tre giorni dopo i server svedesi sono stati nuovamente vittima di un attacco DDoS. Nel mirino degli aggressori figuravano la Banca centrale svedese, il Parlamento svedese e l'agenzia nazionale di informazione Säpo. Questi attacchi DDoS erano stati preannunciati da Anonymous. Ne era motivo una protesta contro la giustizia svedese che era intervenuta in precedenza contro piattaforme che consentono di scaricare film e altri contenuti tramite *BitTorrent*.

4.2.4 Attacchi all'infrastruttura DNS

Anche l'infrastruttura DNS è sempre più nel mirino degli attacchi. Il *Domain Name Systems (DNS)* rende possibile un'utilizzazione conviviale di Internet e dei suoi servizi perché al posto degli *indirizzi IP* si possono utilizzare i cosiddetti *URL* (p. es. www.melani.admin.ch). Al livello superiore della gerarchia figurano i server Root, che come istanza massima hanno la competenza delle informazioni concernenti i *Top-Level-Domains* (TLD, p.es. .com, .net, .ch). Oltre a questi server di nomi TLD sono in funzione presso ogni provider server DNS che effettuano la memorizzazione intermedia dell'informazione DNS di livello massimo e la mettono a disposizione dei (computer dei) loro clienti.

Tra il 3 e il 6 settembre 2012 la Deutsche Telekom ha dovuto affrontare un attacco massiccio a queste infrastrutture DNS. L'attacco ha potuto essere parato con successo. Non si sono osservate limitazioni nella risoluzione dei nomi.

All'inizio del 2013 anche SWITCH è stata vittima di un attacco alle infrastrutture DNS, che ha potuto anch'esso essere parato[24]. Non era la prima volta che si verificava un attacco all'infrastruttura TLD CH. Nel caso di questo «*DNS-Amplification Attack*» l'obiettivo non era soltanto l'infrastruttura CH. Essa costituiva unicamente un mezzo per attaccare un server Web negli USA. Nel caso del metodo di attacco «DNS-Amplification» qui descritto si sfrutta il fatto che

[24] Un rapporto esauriente su questo attacco seguirà nel Rapporto semestrale 2013/1.

in determinati casi il server di nomi risponde con grandi pacchetti a piccoli pacchetti di richieste. In teoria una richiesta di una lunghezza pari a 60 byte può determinare una risposta di una lunghezza di oltre 3000 byte. Queste grandi risposte sono poi dirette sugli obiettivi veri e propri. Grazie a questo trucco gli aggressori necessitano di un'infrastruttura di attacco di minori dimensioni (rete bot) per produrre un grande flusso di dati.

Gli attacchi DDoS fanno parte dei maggiori pericoli ai quali sono esposte le reti. In merito non aumenta tanto il numero degli attacchi quanto soprattutto la loro complessità. Si osserva parimenti un incremento degli attacchi ai protocolli DNS[25]. Nel suo blog SWITCH scrive che il protocollo DNS è quello attualmente soggetto a maggiori abusi per effettuare attacchi DDoS. Oggigiorno poi si utilizzano sempre più server DNS autoritari invece di server DNS accessibili pubblicamente come ne era il caso in precedenza[26].

4.3 Vulnerabilità presso i terminali PoS

Per quanto riguarda i terminali di carte di credito, i cosiddetti *PoS* (*Point of Sales),* gli aggressori si erano finora focalizzati sui metodi classici di *skimming*, che introducono un hardware supplementare sul terminale per leggere le strisce magnetiche e i *PIN*. Un simile modus operandi è stato applicato anche nei commerci svizzeri[27]. Una nuova lacuna di sicurezza, oggetto di una pubblicazione nel luglio del 2012 degli esperti tedeschi di sicurezza Thomas Roth e Karsten Nohl di SRLab, attira l'attenzione su un nuovo pericolo.

Gli esperti di sicurezza hanno scoperto una lacuna critica di sicurezza nel terminale di carte «Hypercom Artema Hybrid» del produttore Verifone. Il lettore di carte viene attaccato mediante un traboccamento della memoria tampone (buffer overflow) nello stack della rete, con la conseguenza che viene controllato il processore delll'applicazione. L'aggressore accede quindi al terminale attraverso la rete e può controllare il campo di immissione e il display e catturare il PIN e la striscia magnetica. L'aggressore potenziale non deve più procurarsi l'accesso diretto all'apparecchiatura. Basta l'accesso al terminale via *TCP/IP*. A tale scopo non è assolutamente necessario un accesso fisico alla rete aziendale corrispondente. L'aggressore può ad esempio procurarsi l'accesso introducendo un software nocivo nel computer di un collaboratore. La cosa è ancor più semplice quando il terminale delle carte è direttamente accessibile da Internet, ossia quando è provvisto di un *indirizzo IP pubblico*.

Si possono anche verificare attacchi locali attraverso il processore sulla porta seriale o sulla connessione JTAG. Nel caso di JTAG si opera al di sotto del livello software. L'accesso via JTAG avviene direttamente sul processore e quindi la lacuna di sicurezza non può essere completamente eliminata via un aggiornamento del software.[28]

La centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) è stata informata tempestivamente di questa lacuna di sicurezza e ha trasmesso questa informazione al-

[25] http://www.all-about-security.de/security-artikel/applikations-host-sicherheit/applikationen-web-services/artikel/14953-ddos-angriffe-bleiben-groesste-gefahr-fuer-netzwerke/ (stato: 28.2.2013).

[26] http://securityblog.switch.ch/2012/12/04/ddos-angriffe-durch-reflektierende-dns-amplifikation-vermeiden/ (stato: 28.2.2013).

[27] MELANI rapporto semestrale 2011/1, capitolo 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de (stato: 28.2.2013).

[28] http://www.golem.de/news/verifone-ec-kartenterminals-in-deutschland-gehackt-1207-93144.html (stato: 28.2.2013).

le imprese competenti in Svizzera per l'esercizio di questi terminali. Le imprese in questione hanno potuto adottare contromisure corrispondenti.

4.4 Attacchi alle istituzioni dell'UE

Secondo quanto afferma l'agenzia US di informazioni Bloomberg un gruppo di spie cinesi sarebbe penetrato nel sistema informatico del Consiglio dell'UE. Questo gruppo, denominato «Byzantine Candor», si sarebbe procurato e-mail di Herman Van Rompuy e di altri alti funzionari dell'UE. L'articolo dell'agenzia Bloomberg riporta inoltre che gli hacker erano in relazione con l'esercito cinese di liberazione del popolo e che tutta questa faccenda è stata scoperta grazie a un gruppo statunitense di professori universitari, di imprenditori e di esperti di sicurezza nel campo delle TIC. Oltre al Consiglio dell'UE sarebbero state vittima degli hacker almeno 20 imprese. Ciò che accomuna tutte queste vittime è il fatto di possedere tecnologie che potrebbero procurare alla Cina un vantaggio in termini di competitività. L'UE non si è espressa in merito a questi attacchi.

Bloomberg è del parere che Byzantine Candor sia soltanto uno dei numerosi esempi da designare sotto il nome di industria cinese dello spionaggio.

Nel corso dei due ultimi anni si sono riportati a più riprese eventi analoghi (cfr. in merito in particolare i rapporti MELANI 2011/1 und 2011/2)[29]; le presunte attività spionistiche di «Byzantine Candor» e le sue possibili relazioni con l'esercito cinese sono già state tematizzate nel dicembre del 2010 da diversi media, dopo che Wikileaks aveva pubblicato un corrispondente messaggio segreto US del 2008. Nel messaggio si descriveva che le attività di spionaggio in provenienza dalla Cina si erano moltiplicate nel corso degli ultimi anni. È soltanto nel febbraio del 2013 che Madiant, una ditta US nel campo della sicurezza, ha pubblicato un rapporto che attribuisce all'unità 61398 dell'esercito cinese le diverse attività di spionaggio degli ultimi anni, in particolare ai danni di imprese US[30]. Le autorità cinesi contestano tuttavia l'esistenza di questo genere di attività di spionaggio informatico da parte dello Stato.

4.5 Inaugurazione del CERT dell'Unione europea e del Centro europeo per la lotta alla criminalità informatica (EC3)

Il *CERT* (Computer Emergency Response Team) dell'Unione europea ha iniziato la propria attività l'11 settembre 2012 dopo un anno di attività pilota seguita da una valutazione. Il suo mandato principale consiste nella protezione delle istituzioni dell'UE dagli attacchi informatici. Il CERT è composto dagli specialisti TIC e della sicurezza delle principali istituzioni dell'UE. Il suo mandato comprende altresì la cooperazione con i CERT degli altri Stati membri dell'UE e con diverse imprese del settore della sicurezza. Nel corso degli ultimi anni la Commissione

[29] MELANI rapporto semestrale 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=it (stato: 28.2.2013). MELANI rapporto semestrale 2011/2: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=it (stato: 28.2.2013).

[30] Questo tema sarà trattato dettagliatamente nel prossimo Rapporto semestrale 2013/1.

dell'UE è stata a più riprese vittima di attacchi informatici[31] [32], circostanza che spiega la necessità di una simile istituzione.

Il Centro europeo per la lotta alla criminalità informatica (EC3) è stato inaugurato l'11 gennaio 2013 all'Aia, nei locali di Europol. Il Centro va inteso come servizio di contatto a livello di UE nella lotta alla criminalità informatica. Secondo quanto dichiarato da Cecilia Malmström, commissario europeo per le questioni interne, l'EC3 dell'UE offre molte più possibilità di lotta alla criminalità informatica e consente di tutelare un Internet libero, aperto e sicuro. Il rapporto MELANI 2012/1[33] contiene una descrizione dettagliata del Centro e delle sue competenze.

4.6 Apriti sesamo: serrature elettroniche negli alberghi

Nel luglio del 2012 un hacker ha dimostrato ai partecipanti alla Conferenza «Black Hat» di Las Vegas come si potessero sbloccare senza fatica determinate serrature elettroniche delle camere d'albergo. Il metodo consiste nella ricerca, attraverso la presa di programmazione ben visibile e senza protezione sulla serratura, della chiave di sicurezza memorizzata senza codice nel chip di controllo della serratura. Secondo quanto riferito dalla stampa sono soprattutto le serrature a codice della ditta Onity che presentano questa lacuna di sicurezza.

Un altro hacker – prendendo lo spunto dall'esempio appena citato – ha proposto al pubblico un'implementazione particolarmente efficace di questo metodo. Esso ha spiegato sul proprio blog tutti i dettagli della produzione di un apparecchio grazie al quale si può penetrare nelle camere d'albergo «protette» da un sistema elettronico. L'apparecchio ha le dimensioni e la forma di una penna a sfera e può quindi essere trasportato senza problemi perché non dà nell'occhio.

Un aggiornamento della serratura è possibile soltanto mediante la sostituzione della *platina*. I costi non sono tuttavia assunti dal produttore, ma devono essere pagati dall'albergo stesso. A titolo alternativo il produttore offre una variante gratuita nella quale un coperchio impedisce l'accesso alla presa di programmazione. Ne sarebbero toccate a livello mondiale oltre quattro milioni di serrature[34].

Questa lacuna di sicurezza era apparentemente nota da parecchio tempo. Dato che temeva che anche le autorità e i servizi segreti ne avessero conoscenza, lo scopritore ha ora reso pubblica la cosa.

Già da alcuni anni non sono più oggetto di attacchi informatici i soli computer e server. Ogni sistema informatico può finire nel mirino degli hacker. Sbloccare la porta elettronicamente protetta di una camera d'albergo è solo uno dei tanti esempi che illustrano questo dato di fatto. Nella progettazione di prodotti provvisti di una procedura elettronica di identificazione questo rischio dovrebbe essere preso sistematicamente in considerazione.

---

[31] Cfr. MELANI rapporto semestrale 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 28.2.2013).

[32] Cfr. MELANI rapporto semestrale 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de (stato: 28.2.2013).

[33] Cfr. MELANI rapporto semestrale 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 28.2.2013).

[34] http://www.t-online.de/computer/sicherheit/id_58856082/hacker-knacken-hotel-tueren-binnen-sekunden.html (stato: 28.2.2013).

L'accesso a una camera d'albergo può consentire alla persona non autorizzata di prendere visione di dati confidenziali. Poco importa in merito se tali dati si trovino su un laptop, una scheda USB o su carta. Il presente caso dischiude un aspetto parziale totalmente diverso e illustra come le imprese debbano procedere con i collaboratori in viaggio di servizio con dati sensibili. Rientra in questo ambito le sensibilizzazione del collaboratore e l'adozione di misure corrispondenti (p. es. l'archiviazione cifrata di informazioni sui supporti di dati) prima di un viaggio di servizio.

4.7 Apparecchiature collegate alle rete di telefonia mobile – grande varietà e poca consapevolezza della sicurezza

Anche la rete di telefonia mobile attira sempre più l'attenzione degli specialisti della sicurezza. Nel mese di luglio 2012 ricercatori tedeschi hanno fornito la prova di lacune potenziali di sicurezza della rete e delle apparecchiature che vi sono collegate.[35] Con l'ausilio di un'inchiesta basata su *RIPE* i ricercatori si sono in un primo tempo posti alla ricerca degli *indirizzi IP* che i gestori assegnano alle apparecchiature collegate alla rete di telefonia mobile. Successivamente essi poterono raccogliere diverse informazioni con un semplice scanner di porte. Un primo insegnamento tratto da questo esperimento è che sulla rete caracolla una varietà gigantesca di apparecchiature: *router GSM/GPRS*, fotocamere, *smart meter* (contatori del consumo di energia), *scanner di codice a barre*, sistemi di controllo del traffico ecc. I ricercatori tedeschi sono addirittura riusciti qualche volta a ottenere informazioni sulla localizzazione delle apparecchiature senza identificarsi in precedenza. Non è però stato effettuato alcun tentativo di login e di comando a distanza di queste apparecchiature.

Lo scopo di questa dimostrazione era di attirare l'attenzione sulle conseguenze potenziali di questa varietà di apparecchiature sulla rete e di evidenziare quanto facilmente esse possano essere identificate. Ciò potrebbe indurre persone malintenzionate a ricercare lacune di sicurezza per poter assumere il controllo di queste apparecchiature. Esse potrebbero quindi accedere ad apparecchiature utilizzate nel settore privato, pubblico e addirittura industriale.

Anche le apparecchiature maggiormente critiche sono sempre più collegate via GSM/GPRS, perlopiù per motivi di costi; fra queste anche i sistemi *SCADA*, i terminali di carte di credito e i distributori di denaro in contanti.

4.8 App Stores

I principali provider a livello mondiale di contenuti per smartphone hanno creato per i loro clienti shop virtuali dove questi ultimi possono acquistare applicazioni (app). Ci si chiede ovviamente quali siano i vantaggi e gli inconvenienti di queste piattaforme dal profilo della sicurezza.

App Store iOS
Nel caso dell'«App Store iOS» si tratta della piattaforma lanciata da Apple nel 2008. Per accedere al mercato Apple, ovvero per poter offrire apps, il produttore deve imperativamente sottoporsi ai controlli interni di verifica di Apple[36]. È soltanto dopo un'analisi corrispondente

[35] http://www.heise.de/security/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html (stato: 28.2.2013).
[36] https://developer.apple.com/appstore/guidelines.html (stato: 28.2.2013).

che l'applicazione è ammessa alla vendita sull'Apple Shop. Un simile processo è in particolare destinato a verificare le modalità di funzionamento di un'applicazione. L'applicazione non viene pubblicata se i criteri prescritti da Apple non sono rispettati. Parecchi di questi criteri riguardano la sicurezza del dispositivo dell'utente finale. Un'applicazione non viene ad esempio pubblicata se installa ed esegue un codice di programma supplementare, se dà accesso a dati protetti o li trasmette a terzi senza autorizzazione preliminare.

Nel caso dell'«App Store iOS» l'utente finale affida integralmente la sicurezza ad Apple. In quale misura è efficace questa soluzione? Nel sistema di Apple compaiono solo raramente applicazioni nocive. In alcuni rari casi i processi di verifica sono stati elusi. Il caso più famoso è probabilmente quello di Charlie Miller, un ricercatore la cui applicazione era stata verificata e accettata da Apple. Essa contravveniva alla regola di base del divieto di scaricare ed eseguire codice supplementare[37]. Dopo che ebbe pubblicato il suo atto di eroismo Apple revocò a Miller la sua licenza di sviluppatore. Mike Lee, un ex impiegato di Apple, si è espresso di recente sulla struttura di verifica di Apple[38]. Lee ritiene che il team di Apple incaricato di analizzare le applicazioni sia sottodotato. La verifica di numerose applicazioni sarebbe inoltre monotona e poco interessante per i verificatori. Ciò si applica sia al contenuto (sovente pornografico), sia al fatto che nel caso di numerose app si tratta di copie, rispettivamente di aggiornamenti di app esistenti. La monotonia dell'attività può pertanto determinare errori di superficialità, come ad esempio nel caso di «Find and Call» (cavallo di Troia: iOS/Fidall). Questa app poteva derubare l'elenco dei contatti e trasmetterlo a un server.

Play Store (Android)
Come già menzionato in un precedente rapporto semestrale[39], Google persegue una politica diversa per quanto riguarda le applicazioni. La sicurezza è in questo caso trasferita all'utente finale. Questa politica consente all'utente di scaricare le applicazioni per Android da qualsiasi sito Web. Essi non devono imperativamente passare da Play Store, lo shop ufficiale di Google. Ciononostante Google persegue l'obiettivo di offrire applicazioni sicure al cliente che visita la sua propria piattaforma. All'inizio del 2012 Google ha pertanto introdotto il sistema «Bouncer». Questo sistema analizza automaticamente tutte le applicazioni del Play Store alla ricerca di codice nocivo. Nel corso del mese di luglio due ricercatori – il già menzionato Charlie Miller e Jon Oberheide – hanno nondimeno dimostrato che è possibile ingannare «Bouncer» e infettare uno smartphone Android[40] con un'app appositamente predisposta.

Google tenta di colmare il fossato tra sicurezza e flessibilità: da un canto si vorrebbero offrire agli utenti di Android servizi possibilmente aperti e sicuri, ciò che attira ovviamente i criminali. D'altro canto Google vorrebbe offrire la massima sicurezza possibile all'utente.

Amazon Appstore (Android):
Amazon ha lanciato nel corso del primo semestre del 2011 il proprio Appstore Android. Alla fine del 2011 Amazon ha inoltre iniziato a distribuire un proprio tablet corrispondente. Su questo tablet di ultimissima generazione gira una versione modificata del sistema Android «Ice Cream Sandwich», che ha un accesso esclusivo allo shop virtuale di Amazon. Dopo il lancio dell'Appstore gli esperti hanno espresso alcuni dubbi riguardo la sicurezza. Si critica in particolare il fatto che l'utente Android che intende accedere allo store senza essere provvi-

---

37 http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (stato: 28.2.2013).

38 http://www.businessinsider.com/heres-why-it-really-sucks-to-be-an-app-reviewer-for-apple-2012-7#ixzz1zaB9ki4H (stato: 28.2.2013).

39 MELANI rapporto semestrale 2011/2, capitolo 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 28.2.2013).

40 http://jon.oberheide.org/files/summercon12-bouncer.pdf (stato: 28.2.2013).

sto di un tablet Amazon debba attivare l'opzione «Installazione di app provenienti da fonti sconosciute» per poter effettivamente utilizzare l'Amazon Appstore. Le restrizioni al download sono così allentate e viene offerta la possibilità di installare un numero imprecisato di app, magari anche nocive, scaricandole da siti non affidabili. Dal rapporto di F-Secure relativo al secondo trimestre del 2012[41] risulta che la maggior parte delle applicazioni nocive per Android proviene da «mercati paralleli» al Google Play Store. Nel corso del medesimo trimestre F-Secure ha individuato il primo download drive-by per Android. Sorprende infine il rapporto dell'impresa di sicurezza TrustGo che, dopo aver analizzato 2,2 milioni di app su un totale di 187 mercati, giunge alla conclusione[42] che Play Store e Amazon Appstore occupano soltanto il quarto e il quinto rango della graduatoria in ambito di sicurezza. Secondo questo rapporto i cinque shop virtuali Android «più pericolosi» si trovano tutti in Cina.

Nei sistemi chiusi come quello di Apple la sicurezza dell'utente finale è nelle mani dell'impresa produttrice. Questa circostanza presenta il vantaggio che i compiti complicati in materia di sicurezza vengono affidati a un'impresa che dovrebbe disporre delle possibilità e delle conoscenze necessarie. Come già menzionato è raro che si introducano applicazioni nocive nei sistemi di Apple. L'inconveniente consiste nel fatto che i clienti dell'App Store devono fidarsi assolutamente dell'impresa e non possono verificare ciò che succede effettivamente nel loro sistema.

D'altro canto il sistema di sicurezza del Play Store è già stato attaccato con successo, mentre Amazon incita i propri utenti a modificare i propri parametri di sicurezza in maniera tale da poter scaricare applicazioni all'infuori del mercato originale. Sui diversi mercati circolano migliaia di programmi nocivi. Anche se l'utente ottiene da Android le informazioni indispensabili per valutare i diritti necessari alle applicazioni si fa raramente capo a questa possibilità. Per l'utente ordinario che intende installare un'applicazione in maniera semplice e rapida l'aspetto della sicurezza viene al secondo posto. Anche l'operatore di mercato deve prendere in considerazione questo aspetto se vuole raggiungere un livello elevato di sicurezza.

4.9 Obbligo di comunicazione dei casi di hackeraggio e di controllo della rete – Pro e contro

Alcuni Paesi, come ad esempio la Francia, gli USA e la Germania hanno annunciato di avere in preparazione interventi legali volti all'introduzione dell'obbligo di annuncio in caso di gravi attacchi informatici. Anche la Commissione europea vorrebbe rendere più sicuro Internet introducendo, conformemente alla strategia informatica dell'Unione europea (UE), un obbligo uniforme di annuncio per le imprese che offrono prestazioni pubbliche di servizi di importanza nazionale. Gli offerenti di telecomunicazioni sottostanno già attualmente a un obbligo di annuncio da quando è stato adottato il pacchetto telecomunicazioni dell'UE.

Si oppongono in particolare a questo modo di procedere l'economia, gli offerenti di servizi Internet e l'industria, tanto più che essi temono che un annuncio possa ripercuotersi negativamente sulla loro impresa ed essere vincolato a un danno alla reputazione. Anche l'onere amministrativo viene ritenuto elevato. Si dovrebbe inoltre spiegare più dettagliatamente cosa si intende per attacco o lacuna di sicurezza. In linea di massima le imprese e i gestori di infrastrutture critiche preferiscono una collaborazione volontaria e adeguata alle necessità con le autorità.

[41] http://www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf (stato: 28.2.2013).

[42] http://www.trustgo.com/images/en-GB/trustgo_q4_mobile_mayhem.pdf (stato: 28.2.2013).

I vantaggi e gli inconvenienti dell'obbligo di annuncio, rispettivamente dello scambio volontario di informazioni, sono oggetto di dibattiti controversi nei diversi Paesi. Da un canto l'istituzione di un simile scambio volontario di dati costituisce un processo basato sulla fiducia che può esigere un tempo corrispondentemente lungo. Risultati immediati sono una merce rara. Se però un simile partenariato si è affermato lo scambio di informazioni è in genere qualitativamente più elevato che non nel caso di un obbligo di annuncio. D'altro canto, nel caso dell'obbligo di annuncio le informazioni affluiscono per definizione fin da principio. Esse sono però costrette in un corsetto legale che lascia poco spazio sia alle autorità che alle imprese. Il pericolo che queste informazioni affluiscano ma non procurino alcun utile non può essere negato. L'esperienza insegna che anche la discussione precedente una legge sull'obbligo di annuncio e vertente su quali informazioni, in quale grado di dettaglio e in quale forma esse debbano essere fornite esige molto tempo.

Non è possibile affermare quale variante sia la migliore. Ciò dipende fortemente dalla struttura e dalle dimensioni del singolo Paese. Dato che in un grande Paese esistono anche più attori e imprese, l'istituzione di un rapporto di fiducia costituisce indubbiamente una sfida maggiore. In Svizzera si è affermato nel corso degli ultimi anni lo scambio volontario di informazioni nel quadro di una Public Private Partnerships (PPP).

5 Tendenze / Prospettive

5.1 Lacune dei browser – Strategia a due browser e altre possibilità

È divenuto nel frattempo uno standard effettuare regolarmente e ancor meglio automaticamente gli aggiornamenti di sicurezza disponibili del sistema operativo e delle applicazioni. Ciononostante continuano a esistere cosiddette lacune di sicurezza *0-Day*, ossia lacune per le quali non esiste ancora alcun aggiornamento di sicurezza. Simili lacune di sicurezza compaiono quasi quotidianamente nelle più diverse applicazioni. Neppure i *browser* di Internet ne sono eccettuati. A seconda della gravità della lacuna di sicurezza resa nota può rivelarsi opportuno utilizzare, perlomeno temporaneamente, un altro browser finché la lacuna di sicurezza è stata rimossa dal produttore.

Ciò che può sembrare triviale nel settore privato può senz'altro provocare problemi nel mondo aziendale. Diversamente dal caso dei computer privati, nel caso dei computer aziendali non è sovente così semplice passare a un browser alternativo. Questo ad esempio perché non esiste una cosiddetta strategia a due browser. Ne è spesso il caso affinché i servizi TIC competenti debbano provvedere alla manutenzione di un solo browser.

Nel caso di gravi lacune di sicurezza ne potrebbe addirittura risultare un pregiudizio anche per i dati confidenziali e segreti. È quindi opportuno essere preparati all'emergenza sia nella vita privata che nel mondo aziendale, per poter passare in maniera possibile rapida a un browser alternativo.

Nel mondo aziendale sono ipotizzabili le seguenti possibilità. L'enumerazione non è esauriente:

Equipaggiamento capillare di tutti i posti di lavoro con almeno due browser
Tutti i posti di lavoro di un'impresa sono equipaggiati con almeno due browser. In caso di emergenza il personale può essere invitato a non più utilizzare il browser in questione fino a nuovo avviso contrario. Questo passaggio può se del caso essere pilotato tramite il *proxy*,

nel senso che viene impedito l'accesso a Internet attraverso il browser in questione. Questa soluzione è nondimeno vincolata a forti costi, perché è necessaria la manutenzione di più browser e l'utente non è sovente in chiaro quando può utilizzare quale browser.

Equipaggiamento puntuale con almeno due browser
I posti di lavoro che devono assolutamente avere accesso a Internet sono equipaggiati con più browser. Se un browser è colpito da una lacuna di sicurezza si può impedire l'accesso a Internet. L'accesso a Internet diviene allora possibile soltanto tramite un browser alternativo. Questa soluzione presenta tuttavia l'inconveniente che in caso di emergenza una parte del personale non ha temporaneamente accesso a Internet. Anche se ciò non influisce grandemente sul lavoro gli utenti che ne sono toccati possono sentirsi sotto tutela o svantaggiati.

White List
Tutte le divisioni di un'impresa annunciano ai loro servizi TIC gli URL la cui chiamata deve essere possibile anche in caso di emergenza. Tali URL sono registrati su una cosiddetta «White List». Nell'ipotesi che si verifichi una lacuna di sicurezza vengono bloccati tutti gli URL che non figurano sulla «White List». Grazie a questa misura si può rinunciare a un browser alternativo. Il rischio di danno viene minimizzato, nel senso che sono raggiungibili solo determinati URL. L'installazione di aggiornamenti di sicurezza deve essere rapidamente possibile in modo da sopprimere al più presto possibile il bloccaggio degli URL che non figurano nella «White List».

Comunque si decida a livello di TIC private o aziendali: è un'illusione credere che i browser alternativi siano più sicuri: prima o poi una lacuna di sicurezza fa la sua apparizione in ogni browser. Il fatto che al momento non siano note lacune di sicurezza dei browser non sta a significare che il browser sia sicuro al 100 per cento. In Internet ci si dovrebbe sempre muovere con la dovuta prudenza e con un sano intendimento.

5.2 Panoramica delle strategie informatiche

Finora 20 Paesi avevano pubblicato una strategia completa di sicurezza informatica. La maggior parte dei Paesi considera la minaccia in provenienza dal cyberspazio come una delle maggiori sfide del XXI secolo e integrano la sicurezza informatica nelle strategie nazionali di politica di sicurezza (p.es. Francia, Paesi Bassi e Gran Bretagna) come conseguenza di un aumento degli incidenti informatici (p. es. Stuxnet, Duqu, Flame e Ghostnet).

Tutte le strategie informatiche definiscono l'utilizzazione delle tecnologie dell'informazione e della comunicazione (TIC) come motore del progresso economico e del benessere sociale. Simultaneamente esse descrivono come priorità nazionale l'incremento delle capacità di resistenza delle infrastrutture critiche e la riduzione a un minimo dei rischi informatici.

L'informatica come compito trasversale
Il coordinamento delle attività delle autorità a livello politico-strategico e tecnico-operativo è considerato centrale. Questo perché i rischi informatici sono intesi come compito trasversale e perché nel quadro del loro mandato centrale i vari uffici e attori devono d'ora in poi provvedere anche all'impronta informatica. Per garantire tutto questo alcuni Paesi hanno istituito cosiddetti centri di difesa informatica (p.es. Germania e Paesi Bassi).

Public Private Partnership
Dato che la maggior parte dei servizi pubblici di infrastruttura è in mani private è essenziale la collaborazione tra Stato ed economia. La maggior parte delle strategie evidenzia la necessità di intensificare e di istituzionalizzare questa collaborazione. Numerose strategie informatiche poggiano sull'idea che il cyberspazio non va reso più sicuro mediante prescrizioni e in-

terventi dello Stato, bensì su base volontaria, attraverso una più forte collaborazione (p.es. Svizzera, Gran Bretagna e Paesi Bassi).

Cooperazione internazionale
La riduzione efficace dei rischi informatici a un minimo necessita una più forte cooperazione a livello internazionale. Questa ammissione si ritrova in tutte le strategie informatiche. Sono pochi tuttavia i Paesi che descrivono in maniera dettagliata come possa e debba essere migliorata e istituzionalizzata la cooperazione a livello internazionale. Un'eccezione è costituita dagli USA, la cui strategia informatica è esplicitamente orientata sul piano internazionale. Anche la Gran Bretagna promuove un dialogo internazionale volto alla definizione di norme di comportamento nel cyberspazio, iniziato nel 2011 alla Conference on Cyberspace di Londra. Le organizzazioni internazionali (p.es. Unione europea, G8, Nazioni Unite e Organizzazione per la sicurezza e la cooperazione in Europa) svolgono parimenti un ruolo importante nell'elaborazione delle norme di comportamento. Sia la Germania che l'Australia si adoperano a favore di un sistema comune di preallarme e per l'istituzione di interlocutori attraverso i quali fare passare la comunicazione in caso di crisi.

Con l'adozione della sua «Strategia nazionale per la protezione della Svizzera contro i rischi informatici» la Svizzera punta ancor più fortemente sulla collaborazione tra attori pubblici e privati in ambito di rischi informatici. L'approccio della Public Private Partnership (PPP) non costituisce una novità per la Svizzera, tanto più che dall'epoca della privatizzazione di diverse prestazioni pubbliche di servizi, come ad esempio il settore delle telecomunicazioni, le autorità dello Stato sostengono il processo di tutela dell'informazione delle infrastrutture critiche. La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, istituita nel 2004, informa i gestori di infrastrutture critiche in merito agli incidenti e alle minacce nel cyberspazio, fornendo in tal modo un contributo alla gestione dei rischi delle imprese. Con riferimento alla sua struttura MELANI è peraltro paragonabile ai centri di difesa informatica istituiti negli altri Paesi. Se confrontati con gli sforzi di altri Paesi in questa direzione, la collaborazione e il mandato di MELANI vanno addirittura ben oltre.

Questa collaborazione tra autorità ed economia si è affermata e funziona bene. Grazie alla «Strategia nazionale per la protezione della Svizzera contro i rischi informatici» sono ulteriormente rafforzate le attuali strutture decentralizzate. Diversamente dagli altri Paesi la Svizzera rinuncia a istituire un organismo centrale di controllo e di coordinamento.

5.3 Regolamentazione vs. libertà – Come rendere sicuro Internet?

Internet, all'origine un progetto militare di ricerca statunitense denominato «Advanced Research Projects Agency» (*ARPA*), si è affermato come piattaforma di informazione e di offerta e si è sviluppato da mera rete scientifica in un'infrastruttura di grado superlativo utilizzata a scopo commerciale. Questa rapida evoluzione può essere rilevata dal numero di utenti di Internet: nel 1991 si trattava ancora di circa 500 000 persone, mentre oggi gli utenti sono circa 2.5 miliardi di persone. Si stima che nel 2020 5 miliardi di persone (il 60 % della popolazione mondiale) saranno collegate a Internet.

Attualmente Internet non è regolamentato dallo Stato e viene ulteriormente disciplinato come spazio libero da standard tecnici e direttive amministrative (cosiddette policies). La «Internet Corporation for Assigned Names und Numbers» (ICANN) e la «Internet Society» (ISOC) in quanto organizzazioni non governative sviluppano in merito queste direttive tecniche e amministrative e consentono la collaborazione di politica, economia, scienza e società civile nella gestione di Internet. I Governi occidentali sostengono questo modello di governance a

multicommittenza e lo considerano conforme all'obiettivo, ossia la garanzia della libertà dell'informazione

Esiste d'altra parte una forte coalizione di Paesi che si adoperano a favore di una regolamentazione di Internet per estendere il proprio potere di controllo sul cyberspazio e rafforzare o assicurare la loro sovranità.

La conferenza mondiale dell'Unione internazione delle telecomunicazioni (ITU) – un'organizzazione speciale delle Nazioni Unite – che si è svolta a Dubai a fine 2012 ha previsto di estendere anche a Internet l'accordo in materia di cooperazione in ambito di reti telefoniche (International Telecommunication Regulations, ITRs). Il fatto che 55 Stati su 144 non lo abbiano sottoscritto sebbene la gestione di Internet non ne venga toccata concretamente o al massimo soltanto a livello di interpretazione, illustra il disaccordo della comunità internazionale in materia di ripartizione delle competenze nella gestione di Internet.

Svolgono inoltre un influsso da non sottovalutare le imprese globali come gli offerenti di software, di motori di ricerca e siti sociali Web, come pure l'industria musicale e cinematografica. Queste imprese sono particolarmente interessate a sviluppare Internet in maniera tale da fare funzionare i loro settori di attività. Esse tentano altresì di praticare il lobby contro l'introduzione di prescrizioni oppure contro la loro assenza, ovvero contro prescrizioni che costano loro denaro o che riducono le loro chance di mercato.

5.4 Tracce in Internet – Quali dati rivelano gli utenti quando visitano un sito Web

Le informazioni costituiscono la nuova moneta in Internet. Questa frase la sentiamo decisamente quando si tratta di raccogliere informazioni in Internet. Programmi sempre migliori e una sempre maggiore capacità di calcolo consentono una valutazione qualitativa sempre migliore di grandi quantità di dati, che possono indubbiamente essere meglio commercializzati. In simili casi la singola persona è invero travolta dal flusso di dati, ma numerosi utenti che utilizzano quotidianamente apparecchiature elettroniche si chiedono quali dati relativi alla loro persona e a quale scopo sono raccolti, elaborati e memorizzati.

Diversi offerenti online sono particolarmente interessati al comportamento degli utenti per poter affissare il maggior numero possibile di messaggi pubblicitari specifici e misurarne i risultati. L'esempio più conosciuto è quello di Google che avvalendosi delle richieste degli utenti «personalizza» i messaggi pubblicitari affissati. Le ditte che affissano pubblicità vivono del fatto che gli utenti cliccano i link corrispondenti. Per le imprese costituisce poi denaro in contanti il fatto che la pubblicità sia possibilmente mirata e confezionata su misura per l'utente. Nella maggior parte dei casi l'insegna pubblicitaria non proviene dal sito stesso, ma viene affissata dall'impresa come sito nel sito (il cosiddetto *IFrame*). Nell'IFrame della ditta pubblicitaria sono poi incorporati piccoli script che raccolgono dati come l'indirizzo IP, il *dominio*, il *browser*, l'ora locale e il sistema operativo[43]. I profili degli utenti possono essere elaborati in maniera tanto più affinata quanto maggiore è il numero di siti sui quali sono collocate le insegne pubblicitarie e i collettori di informazioni. È ovvio che l'utente deve poter essere riconosciuto sui diversi siti. Per raggiungere questo risultato si ricorre ai cosiddetti *cookie*. I cookie non sono in linea di massima niente di nocivo, ma vengono utilizzati per assegnare i parametri personali all'utente corrispondente, in modo che i dati non debbano essere nuovamente

[43] http://de.wikipedia.org/wiki/DoubleClick (stato: 28.2.2013).

immessi a ogni visita o su ogni sito. Le imprese pubblicitarie hanno rapidamente scoperto questa tecnica per i loro scopi, integrandola nelle loro insegne pubblicitarie.

In uno studio del Wall Street Journal pubblicato nell'agosto del 2010 si effettua la navigazione in Internet sui 50 siti maggiormente visitati. Il computer utilizzato per il test aveva successivamente memorizzato 3180 Tracking-Cookies, provenienti per la maggior parte da imprese pubblicitarie. Le informazioni contenute nei cookie sono affinate per il tramite di altre informazioni, come ad esempio il domicilio, per poter allestire un profilo possibilmente preciso dell'utente.[44]

A prescindere dall'indirizzo IP queste indicazioni rimangono sempre più o meno anonime. La cosa cambia però quando le imprese possono confrontare questi profili di utente con dati personali. Il pulsante «mi piace (like)» di Facebook è regolarmente tematizzato in questo contesto. Anche in questo caso è possibile allestire, in maniera analoga alle insegne pubblicitarie, un profilo d'utente sui diversi siti sui quali appare il pulsante di Facebook. I dati sono trasmessi a Facebook ancor prima che l'utente abbia cliccato il pulsante[45]. Se poi l'utente si trova simultaneamente su Facebook, a Facebook sarebbe possibile assegnare direttamente il sito a questa persona. Si utilizzano altresì cookie con una maggiore durata di validità fino a 2 anni, affinché l'assegnazione sia possibile anche ex post.

Ai dati forniti in retroscena si aggiungono peraltro i dati forniti volontariamente, come ad esempio su Facebook, Xing o altre piattaforme di media sociali. Ognuno deve essere ovviamente consapevole dei dati che intende o no fornire. Sussiste nondimeno il pericolo che i dati raccolti in retroscena vengano collegati a quelli forniti volontariamente.

Le nuove tecnologie suscitano sempre nuove avidità. Dato che la navigazione su Internet si sposta sempre più dai «normali» computer sugli *smartphone* la pubblicità è decisamente sempre più dipendente dal luogo. Per via di corrispondenza i dati *GPS* svolgeranno un ruolo sempre maggiore in futuro. Un primo passo in questa direzione è l'annuncio fatto dall'offerente di telefonia mobile «Telefonica» di sfruttare commercialmente i geodati. All'inizio del mese di ottobre 2012 è stata fondata la divisione «Telefonica Dynamic Insight». L'impresa ha la competenza di approntare e di analizzare informazioni – tra l'altro anche geodati di provider di telecomunicazioni – che possono poi anche essere sfruttate a scopo commerciale. Sulla scorta di questi dati sarà ad esempio possibile prevede flussi di persone a dipendenza della meteorologia, del giorno della settimana o dell'ora del giorno. Questo genere di informazioni serve ad esempio al commercio per disporre del personale corrispondente e acquistare merci oppure ai Comuni per controllare i flussi di persone.

In questo senso acquistano sempre maggiore importanza le *app* per smartphone. Proprio in questo ambito esiste attualmente poca trasparenza sui dati trasmessi al produttore. Anche le nuove tecniche di riconoscimento del volto suscitano avidità da parte del settore della pubblicità. La sfida per ogni persona di decidere quali dati che lo riguardano possono essere elaborati e se del caso trasmessi a terzi oppure no (autodeterminazione in materia di informazione) non sarà certamente più semplice in avvenire.

La maggior parte delle persone sa nel frattempo che occorre avere un atteggiamento consapevole nei confronti dei propri dati personali in Internet. Sul retroscena vengono però raccolti numerosi altri dati relativi al comportamento durante la navigazione; questo perlopiù nell'intento di affissare una pubblicità adeguata, ovvero di fare soldi.

---

[44] http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html (stato: 28.2.2013).

[45] http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html (stato: 28.2.2013).

Per evitare che le imprese possano ottenere informazioni sul proprio comportamento di navigazione i produttori di browser hanno previsto appositi parametri. Una prima limitazione è ottenuta disinserendo la funzione «Accetta i cookie di offerenti terzi». Questa funzione può essere utilizzata su qualunque browser, unitamente ad altri parametri concernenti la sfera privata. Firefox e Internet Explorer (si veda qui il numero esatto della versione[46]) offrono inoltre la funzione «Do not Track» che può essere attivata a titolo complementare e che comunica tramite *«opt-out»* a un sito Web che non può essere effettuato un profilo di navigazione. Va poi ancora menzionato l'add-on «Ghostery»[47] di Firefox che vieta nella massima misura possibile i tentativi di tracking ricorrendo a una Blacklist. Nel caso di questa e di altre procedure non vi è tuttavia la certezza al 100 per cento che nessun dato venga raccolto e semmai posto in relazione con altri dati.

5.5 Dati di imprese terze sui siti delle imprese – Un problema di sicurezza?

Su numerosi siti Web viene affissa pubblicità. Questa pubblicità proviene nel minor numero dei casi dall'impresa stessa, ma è prodotta e gestita da un'impresa terza (cfr. in merito anche il capitolo 5.4). Oltre alla pubblicità esistono ovviamente diversi altri contenuti che non vengono generati dall'impresa stessa, bensì da fornitori esterni. Si può ad esempio trattare di un servizio di statistica oppure di un servizio che affissa news o corsi di borsa. Al riguardo non viene affissa soltanto un'immagine, ma generalmente un sito pienamente funzionale nel sito (*IFrame*), provvisto di tutti i medesimi diritti del sito principale. Questa funzione è in particolare utilizzata dei siti di news che devono collegare informazioni provenienti da diversi siti.

Figura 7: URL di imprese terze che pubblicano contenuti su due giornali svizzeri utilizzando Javascript. A tale scopo è stato utilizzato il programma NoScript che blocca i siti di terzi che usano Javascript e li indica.

La figura 7 mostra diversi contenuti affissi sui siti Web di due quotidiani svizzeri. Entrambi i siti ricevono contenuti Web da imprese terze. La fornitura dei contenuti compete in parte alle

[46] http://ie.microsoft.com/testdrive/browser/donottrack/default.html (stato: 28.2.2013).

[47] http://www.ghostery.com/ (stato: 28.2.2013).

medesime imprese e ai medesimi server. La compromissione di un simile server può avere ripercussioni corrispondentemente ampie e nella peggiore delle ipotesi infettare una parte considerevole dei computer della popolazione svizzera. Nel corso degli ultimi anni si sono verificati diversi incidenti di minori dimensioni di questo genere. In questo senso a metà maggio 2012 à stato diffuso un *software nocivo* su wetter.com per il tramite di un'insegna pubblicitaria[48]. Anche imprese svizzere sono già state colpite da simili incidenti e hanno diffuso inconsciamente sui loro siti Web software nocivo per il tramite delle insegne pubblicitarie di imprese terze che vi erano integrate.

Oltre che di tutti i vantaggi e del risparmio di costi offerto dalla centralizzazione dei contenuti Web, ogni impresa dovrebbe anche essere consapevole dei rischi vincolati a una simile centralizzazione. A prescindere dal pericolo di infezioni da software nocivo sul computer del visitatore del sito Web, in caso di incidente sussiste il pericolo di una perdita di reputazione da parte dell'impresa.

È imperativo definire in precedenza come procedere in caso di contenuti compromessi di offerenti terzi. L'impresa ha accesso ai contenuti di terzi, rispettivamente può influenzarli o impedirli in caso di emergenza? Si dovrebbero soprattutto chiarire in precedenza i contatti con le divisioni di sicurezza TIC delle imprese terze in modo da poter informare rapidamente le persone giuste in caso di incidente e da poter avviare contromisure adeguate.

5.6 Fiducia nella Supply Chain

A fine aprile 2012 è stato reso noto che Sunrise avrebbe scorporato per i prossimi cinque anni a Huawei l'esercizio e la manutenzione della rete mobile e della rete fissa. Dal 1° settembre 2012 Huawei ha parimenti ripreso da Sunrise la responsabilità operativa globale. All'inizio del mese di febbraio 2013 anche Swisscom ha concluso un partenariato con l'offerente cinese. Il mandato, limitato a una durata di otto anni, comprende l'ampliamento della rete a fibra ottica fino alle abitazioni (Fibre to the Street, FTTS). In questo contesto si pone tuttavia la questione se la penetrazione di imprese estere nei mercati nazionali delle telecomunicazioni possa mettere in pericolo la sicurezza nazionale. Questo in particolare in considerazione dell'accesso a informazioni sensibili o della possibilità di un sabotaggio dell'infrastruttura di informazione.

Sebbene non si sia attualmente a conoscenza di simili incidenti, non si può ovviamente escludere del tutto cha la partecipazione di un'impresa estera di telecomunicazioni all'ampliamento o all'esercizio di una rete svizzera di telecomunicazioni possa essere utilizzata in maniera abusiva. Le imprese di telecomunicazioni con contratti a livello mondiale non hanno tuttavia alcun interesse a esporsi volutamente a simili macchinazioni. Se un caso simile dovesse essere reso noto l'impresa – oltre alla perdita della fiducia e al danno alla reputazione – dovrebbe anche aspettarsi sanzioni, come ad esempio il bloccaggio dell'accesso a determinati mercati.

Una possibile presa di influenza da parte di un qualsiasi Stato non può essere interamente esclusa, tanto più che il contesto politico esterno può mutare in ogni momento. Dato che simili apparecchiature sono provviste di un *firmware* il collocamento di software nocivo è possibile anche in un momento successivo. Alla fiducia in un produttore fa tuttavia riscontro una possibilità di controllo che comporta per ogni prodotto e per ogni aggiornamento del firmware

[48] MELANI rapporto semestrale 2012/1, capitolo 4.9: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 28.2.2013).

un'analisi del *codice fonte (Sourcecode)* e un test di sicurezza onerosi in termini di tempi e di costi. Anche in questo caso la verità si situa da qualche parte nel mezzo. Le analisi di rischio e di vulnerabilità fanno parte degli elementi di base di ogni strategia aziendale. In questo senso le imprese devono meno focalizzarsi sul Paese d'origine del produttore, ma piuttosto sulle possibilità di integrare a valle misure di sicurezza indipendenti dalle apparecchiature utilizzate.

6 Glossario

Advanced Research Projects Agency Network (ARPANet)	Arpanet è stato originariamente sviluppato dal 1962 da un piccolo gruppo di ricercatori sotto la direzione del Massachusetts Institute of Technology e del Ministero US della difesa su mandato delle Forze aeree US. È il predecessore dell'attuale Internet.
0-day-exploit	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
App	Il concetto di app (dall'abbreviazione inglese di Application) designa in generale ogni forma di programmi di applicazione. Nell'uso linguistico si fa nel frattempo perlopiù riferimento alle applicazioni per i moderni smartphone e tablet computer.
Attacco DoS	Attacco Denial-of-Service. Ha lo scopo di rendere irraggiungibile un determinato servizio all'utente o perlomeno di ostacolare notevolmente la raggiungibilità di detto servizio.
Barcode Scanner (lettore di codici a barre)	Apparecchio di registrazione dei dati che può leggere e riprodurre diversi codici a barre. Il riconoscimento di questa striscia di codice è effettuato in maniera puramente ottica con luce rossa oppure infrarossa.
BitTorrent	Protocollo collaborativo di filesharing, particolarmente adeguato alla distribuzione rapida di grandi quantità di dati.
Browser/Navigatore	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Netscape, Opera, Firefox e Safari.
Certificato digitale	Certifica l'appartenenza di una chiave pubblica (PKI) a un soggetto (persona, elaboratore).
Cifratura RSA	Abbreviazione di cifratura Rivest-Shamir-Adleman. Procedura di cifratura con chiavi pubbliche, introdotta nel 1978. La cifratura RSA è una procedura asimmetrica.
Circuito stampato (platina)	Supporto di componenti elettroniche. Essa è destinata alla fissazione meccanica e al collegamento elettrico. Pressoché ogni apparecchio elettronico possiede una o più platine.
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.
Computer Emergency Re-	Computer Emergency Response Team Si designa come CERT (ma anche come CSIRT per Computer Security

sponse Team (CERT)	Incident Response Team) un gruppo che si occupa del coordinamento e dell'adozione di misure nel contesto di incidenti rilevanti ai fini della sicurezza delle IT.
Cookie	Piccolo file di testo depositato sul computer dell'utente alla visita di una pagina Web. Con l'ausilio dei cookies è per esempio possibile salvaguardare le impostazioni personali di una pagina Internet. Essi possono però anche essere sfruttati in modo abusivo per registrare le abitudini di navigazione dell'utente e allestire in tale modo un profilo di utente.
Defacement	Deturpamento di pagine Web.
Domain Name System (DNS)	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).
DNS Amplification Attack	Attacco di Denial of Service (DoS), che sfrutta abusivamente server DNS accessibili al pubblico e li utilizza come amplifier (amplificatore).
DNS Resolver	Modulo software di costruzione semplice installato sul calcolatore di un partecipante DNS che può richiamare informazioni dal server dei nomi. Esso costituisce l'interfaccia tra l'applicazione e il server dei nomi.
Domini	Il nome di dominio (ad es. www.example.com) può essere risolto dal DNS (Domain Name System) in un indirizzo IP che può poi essere utilizzato per istituire collegamenti con questo computer.
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere – ossia sul vostro computer.
Firma della transazione	Elemento supplementare di sicurezza in ambito di e-banking. Quando impartisce un mandato di pagamento il cliente riceve un codice tramite un SMS sul suo telefono cellulare. Il pagamento è effettuato dalla banca dopo aver immesso il codice nel sistema e-banking.
Firmware	Dati di comando per il controllo di un apparecchio (ad es. scanner, carte grafiche ecc.), memorizzati in un chip. Questi dati possono di norma essere modificati per il tramite di Upgrades (aggiornamenti).
General Packet Radio Service (GPRS)	In italiano «servizio generale radio a pacchetti»; servizio utilizzato nelle reti GSM (telefonia mobile) basato su pacchetti per la trasmissione dei dati.
Global Positioning System	Global Positioning System (GPS), dont le nom officiel est

(GPS)	NAVSTAR GPS, est un système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
Global System for Mobile Communications (GSM)	(già Groupe Spécial Mobile, GSM) Standard delle reti di telefonia mobile integralmente digitali, utilizzato prevalentemente nella telefonia, ma anche per la trasmissione di dati per multiplex o per pacchetti, come pure per la messaggeria breve (short messages).
HyperText Transfer Protocol Secure (https) (protocollo sicuro di trasmissione di ipertesto)	Protocollo di comunicazione del World Wide Web per trasmettere dati al sicuro da intercettazioni.
IFrame	Un IFrame (anche Inlineframe) è un elemento HTML che serve alla strutturazione delle pagine Web. Esso viene utilizzato per integrare contenuti Web esterni nella propria homepage.
Infezione da «drive-by-download»	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo scopo di diffondere il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
IP-Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
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.
Master Boot Record (MBR)	Il Master Boot Record è il primo blocco di dati (512 byte) di un media di memorizzazione. Il MBR contiene informazioni che descrivono le partizioni del supporto di dati e, in opzione, un programma che avvia un sistema operativo su una delle partizioni.
Opt-out	Procedura di marketing che prevede l'inserimento automatico in un elenco di distribuzione e la possibilità per il cliente di espungersi dall'elenco di distribuzione al primo invio.
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.
Phreaking	Manipolazione di collegamenti telefonici.

Numero di identificazione personale (PIN)	Un numero di identificazione personale o numero segreto è un numero con il quale ci si autentifica nei confronti di una macchina.
Point of Sales (POS)	Un terminale POS (in Svizzera terminale EFT/POS) è un terminale online per il pagamento senza contanti presso un punto di vendita («point of sale»).
Proxy	Interfaccia di comunicazione in una rete che funge da intermediario che riceve le richieste da un lato per poi effettuare il collegamento dall'altro lato con il proprio indirizzo.
Public IP Address	Indirizzo IP che può essere raggiunto direttamente e da ogni punto in Internet.
Réseaux IP Européens (RIPE)	Registro regionale di Internet competente per l'attribuzione di settori di indirizzi IP e di numeri AS in Europa, nel Vicino Oriente e nell'Asia centrale.
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.
Server DNS autoritario	Un server di nomi autoritario è responsabile di una zona. Le sue informazioni su questa zona vanno pertanto considerate tutelate.
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Skimming	Lo skimming (dall'inglese scremare) è un concetto inglese per gli attacchi Man-in-the-middle, destinati a spiare i dati delle carte di credito e delle carte bancarie. Nel caso dello skimming si accede ai dati della carta leggendo i dati della striscia magnetica e ricopiandoli su carte falsificate.
Smart Meter	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.
Short Message Service (SMS)	Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
Sourcecode (codice fonte)	Con il concetto di codice fonte (inglese: source code) si designa in informatica il testo di un programma per com-

	puter scritto in linguaggio di programmazione e leggibile da parte dell'uomo.
Spoofing	Nel tecnica informatica si designano come spoofing diversi tentativi di inganni sulle reti di computer per camuffare la propria identità.
Stack di rete	In ambito di trasmissione dei dati lo stack di rete è un'architettura concettuale di protocolli di comunicazione.
Top-Level-Domains	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separate da un punto. La designazione Level-Domain si riferisce all'ultimo nome di questa successione e costituisce il livello più elevato della risoluzione del nome. Se ad esempio il nome completo di dominio di un computer, rispettivamente di un sito Web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome.
Traboccamento della memoria tampone (Buffer overflow)	Le più frequenti lacune di sicurezza del software attuale che possono tra l'altro essere sfruttate via Internet.
Transmission Control Protocol / Internet Protocol (TCP/IP)	Famiglia di protocolli di rete anche designata come famiglia di protocolli Internet a causa della sua grande importanza per Internet.
Uniform Resource Locator (URL)	L'indirizzo Web di un documento composto dal protocollo, dal nome del server e dal nome del documento con il percorso (esempio: http://www.melani.admin.ch/test.html).
Universal Serial Bus (USB)	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).
Voice-Phishing	Forma di truffa in Internet con uno stratagemma e prende il nome dal concetto inglese di pescare (fishing) e dal metodo di telefonia VoIP utilizzato.
Voice over IP (VoIP)	Telefonia tramite il protocollo Internet (IP). I protocolli utilizzati con maggiore frequenza sono: H.323 e SIP.