Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

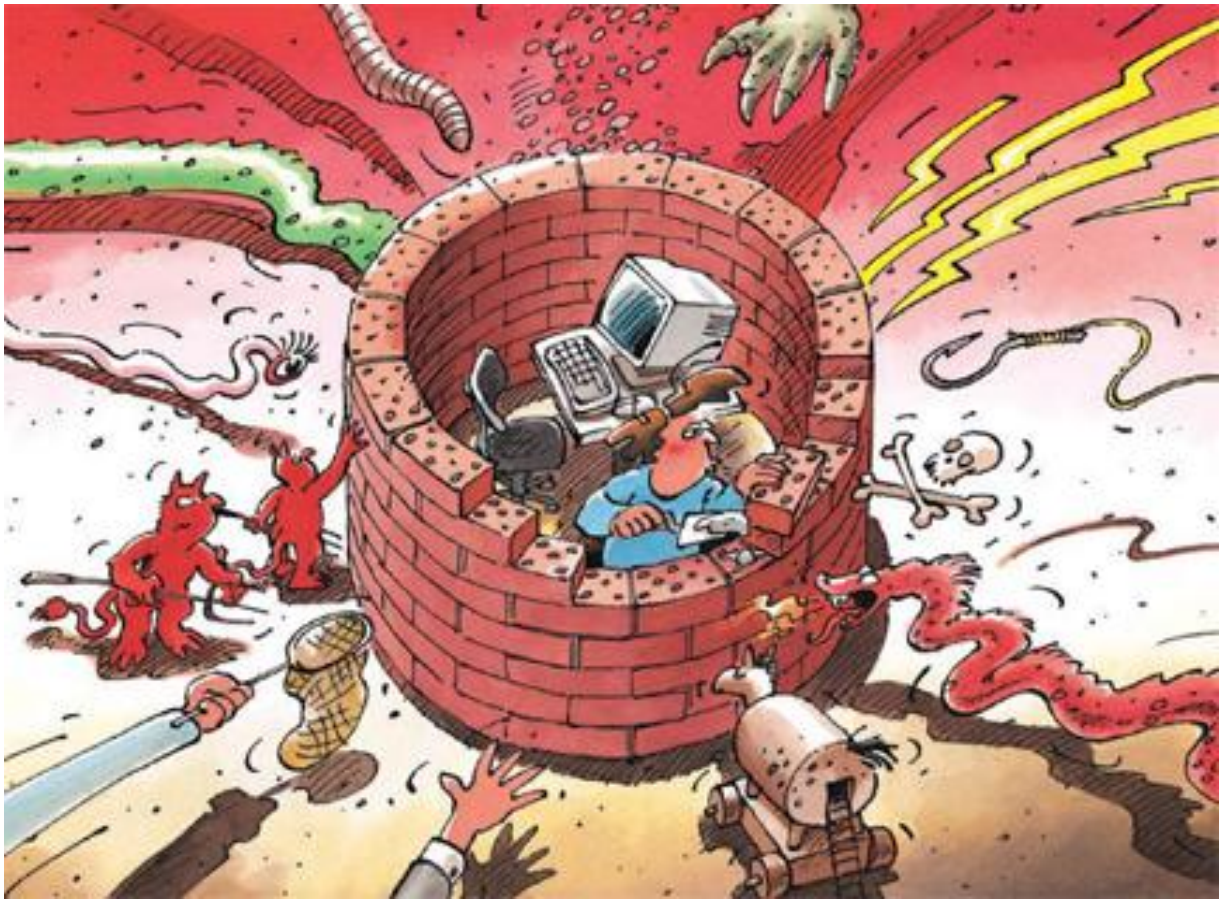
Organo strategia informatica della Confederazione OSIC
Ufficio federale di polizia fedpol

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2007/I (gennaio-giugno)



In collaborazione con:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Indice

Fulcri dell'edizione 2007/I

- **Attacchi contro servizi finanziari svizzeri**
  In Svizzera sono fortemente diminuiti gli attacchi «classici» di *phishing* tramite e-mail che sollecitano la comunicazione delle password. Inoltre tutti questi attacchi non hanno avuto successo. In compenso sono aumentati gli attacchi efficaci tramite *malware*. I sistemi di *autentificazione a due fattori* (p.es. elenchi di stralcio, SecurID ecc.) non offrono alcuna protezione contro simili attacchi e vanno pertanto considerati insicuri non appena il PC del cliente è stato infettato dal *malware*.
  ► Situazione attuale: capitolo 2.1 (cfr. anche 2.4)
  ► Tendenze per il prossimo semestre: capitolo 3.1
  ► Esempi / incidenti: Svizzera: capitolo 4.2; a livello internazionale: capitolo 5.2

- **Spionaggio industriale e furti di dati**
  La minaccia di spionaggio industriale mirato da parte di Stati o di privati permane. Sono minacciati non soltanto gli esercenti di *infrastrutture critiche*, ma anche l'industria d'armamento o i servizi dello Stato. Sono nel mirino dello spionaggio anche le imprese industriali del ceto medio, come i produttori di articoli di lusso o di articoli di moda. Gli attacchi sono perpetrati per il tramite di e-mail indirizzati in modo mirato a singoli collaboratori e contenenti in allegato malware o link a pagine Web appositamente predisposte.
  ► Situazione attuale: capitolo 2.3
  ► Esempi / incidenti: Svizzera: capitolo 4.1; a livello internazionale: capitolo 5.2

- **Attacchi contro i server Web: diffusione di malware, phishing, furto di dati**
  Sono aumentate le compromissioni di server Web. L'obiettivo è lo sfruttamento dei server Web per la diffusione di malware, come ad esempio tramite *infezioni drive-by* in vista del furto di dati (soprattutto sui server utilizzati a scopi commerciali), in vista della memorizzazione (temporanea) di dati (p.es. nel contesto del phishing) o per la diffusione di messaggi perlopiù politici.
  ► Situazione attuale: capitolo 2.2 (cfr. anche 2.4)
  ► Esempi / incidenti: Svizzera: capitolo 4.1; a livello internazionale: capitolo 5.1 e 5.2
  ► Prevenzione: capitolo 6 (sul tema delle infezioni drive-by)

- **Malware / Vettori di attacco**
  Nella maggior parte dei casi il *malware* viene tuttora diffuso tramite gli allegati agli e-mail o tramite e-mail contenenti link a pagine Web appositamente predisposte. Con l'ausilio di abili tecniche di *social engineering* la vittima è indotta ad aprire l'allegato o a cliccare sul link.
  Sono in forte aumento come veicolo di infezione pagine Web la cui visita comporta l'installazione di malware sul PC dell'utente senza alcun intervento da parte sua (infezioni drive-by). Si sfruttano a tale scopo le lacune di sicurezza del sistema operativo, del browser o di altre applicazioni. Da tempo ormai l'infezione non si propaga più soltanto tramite pagine dubbie, ma anche tramite pagine (compromesse) serie e conosciute.
  Il tasso di individuazione del malware da parte dei software antivirus permane basso.
  ► Situazione attuale: capitolo 2.4 (cfr. anche 2.2)
  ► Esempi / incidenti: Svizzera: capitolo 4.2; a livello internazionale: capitolo 5.1 e 5.2.
  ► Prevenzione: capitolo 6 (infezioni drive-by)

1 Introduzione

Il quinto rapporto semestrale (gennaio – giugno 2007) 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 un punto centrale in ambito di prevenzione e presenta in sintesi le principali attività degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario** alla fine del rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

Il **capitolo 2** descrive la situazione attuale, nonché i pericoli e rischi del semestre precedente. Il **capitolo 3** presenta in prospettiva le evoluzioni ipotizzate.

I **capitoli 4 e 5** 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 dei primi sei mesi del 2007. Il lettore dispone qui di esempi illustrativi e di informazioni complementari sui capitoli generali due e tre.

Il **capitolo 6** è d'ora in poi consacrato di volta in volta a una tematica attuale in ambito di prevenzione, in stretta relazione con i pericoli menzionati nel capitolo 2.

Il **capitolo 7** è focalizzato sulle attività dello Stato e dell'economia privata in ambito di sicurezza dell'informazione in Svizzera e all'estero.

Il **capitolo 8** riassume le modifiche delle basi legali.

Il **capitolo 9** compendia i principali studi e statistiche sulle tematiche TIC.

2 Situazione attuale, pericoli e rischi

2.1 Attacchi contro i servizi finanziari svizzeri

Nel corso del primo semestre sono fortemente diminuiti in Svizzera gli attacchi «classici» di *phishing* – e-mail con falso mittente e link a una pagina di phishing su Internet per carpire i numeri dell'elenco di stralcio di accesso ai portali di e-banking. I pochi attacchi osservati non hanno d'altra parte avuto successo. Le bande criminali seguono nuove vie per attaccare i sistemi di e-banking, come era del resto già stato preannunciato nell'ultimo rapporto semestrale (capitolo 3.1). I computer della clientela sono infettati con *malware* che consente di effettuare attacchi *man-in-the-middle*. Simili attacchi sono stati perpetrati con successo anche contro i portali svizzeri di e-banking.

Diffuso tramite e-mail contenenti allegati infettati o link a pagine Web appositamente predisposte, il malware si introduce inosservatamente nel computer del cliente sfruttando le *lacune di sicurezza* del sistema operativo e di un'applicazione. In Svizzera la diffusione è avvenuta tramite e-mail con un falso mittente (Ricardo.ch e uno studio legale bernese; cfr. capitolo 4.2), senza che venisse cliccato in precedenza il link contenuto nell'e-mail. Il malware è attivato non appena viene chiamata una pagina di e-banking. Il malware dirotta il cliente su una pagina bancaria falsificata oppure manomette i dati affissi nel browser.

Nel primo caso la pagina falsificata «riproduce» la pagina bancaria autentica, che richiede il nome di utente e la password. Dopo l'introduzione di questi ultimi da parte del cliente, le pagine delle banche richiedono un secondo fattore di autentificazione (p.es. il numero di un elenco di stralcio o un codice generato da un *token*). Anche queste indicazioni sono carpite tramite la pagina falsificata. Successivamente la pagina falsificata interrompe il collegamento con il cliente e visualizza un messaggio di errore. L'aggressore sfrutta simultaneamente i dati di accesso così ottenuti per annunciarsi (in tempo reale) alla banca e disbrigare transazioni finanziarie illegali.

Nel secondo caso il malware si annida nel browser. Prima che i dati relativi alla transazione del cliente siano trasmessi in maniera codificata alla banca tramite Internet, l'aggressore modifica il numero di conto, il nome del destinatario e l'importo. Anche la conferma da parte della banca è captata dal malware e visualizzata in maniera falsificata nel browser. La vittima crede di avere effettuato la transazione desiderata mentre in realtà il pagamento è stato eseguito a favore di un altro destinatario e il suo importo è stato eventualmente modificato.

Il malware di questo tipo può inoltre essere scaricato in ogni momento su computer già infettati – ad esempio quelli di una *rete bot*. Pertanto i sistemi infettati che gli aggressori avevano inizialmente destinato ad altre attività possono essere improvvisamente sfruttati anche per gli attacchi contro l'e-banking.

Senza che i clienti dell'e-banking abbiano reagito a un e-mail di phishing e quindi immesso numeri di elenchi di stralcio o password in una pagina di phishing, il malware è attualmente in grado di sferrare attacchi efficaci contro la clientela. Non appena il PC del cliente è compromesso dal malware, i *sistemi di autentificazione a due fattori*, come quelli utilizzati attualmente dalle banche svizzere ed estere (come p.es. elenchi di stralcio, elenchi

indicizzati di stralcio, token con codici variabili o calcolati in maniera crittografica ecc.) devono essere considerati insicuri.[1]

Gli utenti di computer devono pertanto osservare norme di comportamento nella manipolazione degli e-mail e nella navigazione in Internet, come pure mantenere aggiornati il sistema operativo e le applicazioni e utilizzare software antivirus e firewall aggiornati (cfr. in merito le raccomandazioni sulla homepage di MELANI)[2]. Le irregolarità osservate durante le sessioni di e-banking., come ad esempio l'interruzione inaspettata della sessione di e-banking, devono essere comunicate senza indugio al pertinente istituto finanziario.

Il capitolo 3.1 presenta una valutazione dell'evoluzione; la situazione in Svizzera è illustrata nel capitolo 4.2 e quella a livello internazionale nel capitolo 5.2. Le somme di denaro carpite sono sovente trasferite all'estero da cosiddetti «money mules» – si veda in merito il capitolo 4.3.

2.2 Attacchi contro i server Web in vista della diffusione di malware, di phishing o di furto di dati

Nel corso del primo semestre del 2007 sono aumentate le compromissioni di server Web[3]. Su un totale di circa 4.5 milioni di URL Google ha ad esempio individuato circa 450'000 URL che tentano di diffondere *malware*; per il solo mese di giugno Sophos rileva quasi 30'000 nuove pagine Web infettate al giorno, fermo restando che nella maggior parte dei casi non si tratta di pagine dubbie, bensì di pagine con contenuti assolutamente seri[4]. In questo senso è stato diffuso malware per il tramite delle seguenti homepage compromesse: quelle dei Miami Dolphins (i vincitori del Superbowl degli USA), dell'US-Disease-Control oppure dell'opera e del museo di arte contemporanea di Sidney[5].

Le compromissioni sono sovente operate sfruttando *lacune di sicurezza* non colmate delle applicazioni Web; sono parimenti frequenti gli attacchi contro banche dati che possono essere pilotate mediante server Web. Nel caso di un attacco sferrato in Italia sono state compromesse migliaia di pagine Web situate su un server. Ciò è stato possibile sfruttando la

[1] Cfr. in merito: http://www.schneier.com/blog/archives/2005/03/the_failure_of.html; http://www.schneier.com/essay-083.html; http://www.zdnetasia.com/news/security/0,39044215,62010658,00.htm; http://www.darkreading.com/document.asp?doc_id=116456; http://www.itseccity.de/?url=/content/virenwarnung/aktuellemeldungen/070329_vir_akt_trendmicro.html (stato: 18.07.2007).

[2] Cfr.: http://www.melani.admin.ch/themen/00166/index.html?lang=it (stato: 26.07.2007).

[3] Cfr. p.es.: http://blogs.iss.net/archive/WebBrowserexploitati.html; http://blog.washingtonpost.com/securityfix/2007/05/cyber_crooks_hijack_activities_1.html; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017261; http://googleonlinesecurity.blogspot.com/ (stato: 26.07.2007).

[4] Cfr. in merito: http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf, http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threats-update-2007_wsrus.pdf; http://www.heise.de/newsticker/meldung/93334; http://www.darkreading.com/document.asp?doc_id=120373, http://www.siteadvisor.com/studies/map_malweb_mar2007.html nonché il più recente rapporto dell'Anti-Phishing Working Group: http://www.antiphishing.org/reports/apwg_report_may_2007.pdf (stato: 17.07.2007).

[5] Cfr.: http://www.smh.com.au/news/security/virus-blight-spreads-to-museum-site/2007/06/13/1181414340831.html; http://www.heise.de/newsticker/meldung/84761; http://www.theregister.co.uk/2007/02/08/cdc_malware/; http://www.heise.de/newsticker/meldung/87965 (stato: 26.07.2007).

lacuna di sicurezza di un'unica pagina, in combinazione con un errore di configurazione da parte del provider di hosting (cfr. capitolo 5.1 in merito a MPack)[6].

Gli attacchi ai server Web sono destinati a più scopi: anzitutto il server Web può essere sfruttato per diffondere malware, nel senso che tenta di infettare i computer dei visitatori. Secondariamente il controllo di un server Web utilizzato per l'e-commerce consente sovente di derubare dati preziosi (p.es. dati relativi alle carte di credito). In terzo luogo un server Web compromesso può essere utilizzato per l'hosting di dati illegali, sia come pagina di phishing, sia come luogo di memorizzazione di software piratato o di dati procacciati illegalmente. Sulle pagine Web compromesse vengono sovente effettuate anche modifiche per diffondere messaggi politici (*defacement*).

Si raccomanda agli esercenti di pagine Web di mantenere aggiornate le loro applicazioni Web e di garantire che anche i provider di hosting effettuino gli aggiornamenti e le misure di sicurezza necessari[7].

Le infezioni tramite pagine Web sono nuovamente esaminate nel capitolo 2.4. Gli esempi figurano nei capitoli 4.1 e 5.1, mentre il capitolo 6 è dedicato a corrispondenti misure di prevenzione su questo tema.

2.3 Spionaggio tramite malware mirato

La minaccia costituita dallo spionaggio industriale mirato, che è in parte praticato anche dagli Stati, è già stata esaminata come punto centrale nel rapporto semestrale 2005/II e da allora è stata tematizzata in tutti i rapporti successivi (cfr. anche il rapporto semestrale 2006/II, capitoli 2.3 e 5.2). Essa permane tuttora di attualità.

Negli USA è aumentato il numero di attacchi di spionaggio contro i sistemi del Governo, in particolare contro le reti dei ministeri degli affari esteri e della difesa[8]. Il problema permane di attualità anche per l'economia privata. In passato MELANI ha a più riprese messo in guardia da attacchi mirati contro l'economia privata svizzera. Questa tematica è sempre più oggetto di dibattiti pubblici anche in altri Paesi. Secondo le stime effettuate dalla rivista Der Spiegel, nella sola Germania ne risultano danni dell'ordine di miliardi[9] di euro.

Nel caso dello spionaggio industriale si procede perlopiù come segue: anzitutto si effettua una ricerca relativa ai collaboratori e all'ambiente dell'impresa (p.es. per il tramite di pagine di social networking come Xing, Linked-In ecc., pagine ufficiali delle imprese, homepage private dei collaboratori, rapporti annuali o notizie di stampa, ecc.). Si esegue successivamente l'invio mirato di e-mail ad alcuni pochi collaboratori. Nella maggior parte dei

[6] Ne sono sovente colpiti i medesimi provider di hosting, cfr.: http://blogs.stopbadware.org/articles/2007/05/04/stopbadware-identifies-hosting-providers-of-larged-numbers-of-sites-in-badware-website-clearinghouse (stato: 26.07.2007).

[7] Raccomandazioni concernenti la configurazione sicura dei server Web sono ad esempio reperibili in: http://www.cpni.gov.uk/docs/re-20030801-00726.pdf; http://www.cpni.gov.uk/ProtectingYourAssets/applications.aspx nonché http://www.stopbadware.org/home/security (stato: 19.07.2007).

[8] Cfr. p.es.: http://www.fcw.com/article97658-02-13-07-Web&printLayout; http://seclists.org/isn/2007/Jan/0023.html; http://www.heise.de/newsticker/meldung/91571/ (stato: 30.07.2007).

[9] Cfr.: http://www.manager-magazin.de/unternehmen/mittelstand/0,2828,464284,00.html; http://www.ftd.de/unternehmen/industrie/159669.html; http://www.spiegel.de/wirtschaft/0,1518,465041,00.html; http://www.vnunet.com/vnunet/news/2184744/intellectual-property-theft (stato: 30.07.2007).

casi di tratta di persone con funzioni di quadro che possono accedere a dati confidenziali[10]. Il mittente degli e-mail è falsificato; dal profilo linguistico e contenutistico gli e-mail sono adeguati ai compiti della vittima e contengono *malware* in allegato o link a pagine Web di diffusione di malware (cfr. capitoli 2.2, 2.4 e 5.1). A tale scopo si ricorre sovente a documenti della famiglia Microsoft Office (Word, Excel, Powerpoint), nonché a file PDF[11]. Gli attacchi sono in parte perpetrati facendo capo a cosiddetti *0-day-exploit,* che sfruttano lacune di sicurezza finora ignote[12].

Per quanto riguarda il settore statale e gli esercenti di infrastrutture critiche lo spionaggio concerne soprattutto dati confidenziali rilevanti per l'industria d'armamento oppure dati che potrebbero essere di utilità per attività terroristiche o militari (cfr. il capitolo 4.1 per l'esempio proveniente dalla Svizzera).

Un numero sempre maggiore di imprese, in particolare del ceto medio e del settore industriale (soprattutto imprese di costruzione di macchine e di impianti), è confrontato con lo spionaggio industriale, prevalentemente di origine cinese. Si trovano parimenti nel mirino dello spionaggio i produttori di articoli di lusso e di articoli di moda[13]. Le imprese dell'industria privata sono soprattutto minacciate quando dispongono di un vantaggio in termini di know-how rispetto alla concorrenza oppure hanno contatti d'affari in regioni economicamente arretrate e/o sprovviste di una chiara legislazione sulla proprietà intellettuale.

Nel caso degli aggressori si può trattare di criminali informatici organizzati o di criminali informatici minori (alla ricerca di informazioni barattabili in denaro), della concorrenza (che vuole procacciarsi oppure sabotare know-how e vantaggi scientifici), di attori sponsorizzati dagli Stati (prevalentemente alla ricerca di dati importanti dal profilo militare ed economico) come pure di terroristi (che raccolgono informazioni concernenti le infrastrutture in vista della commissione di attentati).

Dato che gli attacchi sono effettuati in modo mirato e che a tale scopo si fa capo a malware specialmente programmato all'uopo, simili attacchi non sono in generale individuati dai programmi antivirus e anti-spyware. Ci si deve inoltre attendere un incremento della diffusione di malware per il tramite di pagine Internet serie, ma compromesse. Gli aggressori scelgono le pagine Web rilevanti in vista degli obiettivi da attaccare (cfr. in merito anche i capitoli 2.2, 2.4 e 5.1).

---

[10] Cfr. in merito i rapporti di MessageLabs relativi agli attacchi mirati: http://www.messagelabs.com/mlireport/messagelabs_intelligence_special_report__targeted_attacks_april_2007_5.pdf und http://www.messagelabs.com/mlireport/MessageLabs%20Intelligence%20-%20Jun%20Q2%20Report%20-%20FINAL.pdf (stato: 30.07.2007).

[11] Cfr. la precedente nota a piè di pagina nonché: http://www.usatoday.com/tech/news/computersecurity/2007-04-22-cyberspies-microsoft-office_N.htm; http://www.heise.de/security/news/meldung/84311; http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=software&articleId=9018519&taxonomyId=18&intsrc=kc_top (stato: 30.07.2007).

[12] Cfr. p.es.: http://www.theregister.co.uk/2007/04/19/us_state_dept_rooted/. Una descrizione tecnica di un attacco medio è reperibile in: https://isc.sans.org/diary.html?storyid=2894; consigli di difesa sono parimenti disponibili presso ISC SANS: http://isc.sans.org/diary.html?storyid=2967 (stato: 30.07.2007).

[13] Cfr. p.es. i seguenti articoli del Washington Times (link all'archivio): http://nl.newsbank.com/nl-search/we/Archives?p_product=WT&p_theme=wt&p_action=search&p_maxdocs=200&p_text_search-0=chinese%20AND%20hackers%20AND%20get%20AND%20the%20AND%20drop%20AND%20on%20AND%20fashion%20AND%20houses&s_dispstring=chinese%20hackers%20get%20the%20drop%20on%20fashion%20houses%20AND%20date(last%20180%20days)&p_field_date-0=YMD_date&p_params_date-0=date:B,E&p_text_date-0=-180qzD&p_perpage=10&p_sort=YMD_date:D&xcal_useweights=no (stato: 30.07.2007).

2.4 Malware / Vettori di attacco

A prescindere da un aumento delle infezioni tramite le pagine Web, poco è cambiato rispetto all'ultimo semestre. Nella maggior parte dei casi il *malware* continua ad arrivare sui computer tramite gli allegati agli e-mail o tramite e-mail contenenti link a pagine Web contaminanti. Gli indirizzi dei mittenti sono falsificati e comportano con maggiore frequenza rispetto al passato un riferimento regionale per confortare la credibilità degli e-mail. In Svizzera i principali esempi in merito sono gli e-mail di Ricardo.ch e di un avvocato bernese (cfr. capitolo 4.2).

È aumentato come veicolo di infezione il numero di pagine Web la cui visita provoca lo scaricamento di malware sul computer dell'utente senza alcun intervento da parte sua. Questo tipo di infezione viene denominato «*infezione drive-by*». Sono manifestamente state individuate anche pagine Web che diffondono una sola volta per vittima il loro malware – all'atto della seconda visita tali pagine non presentano più alcun carattere stravagante[14]. Se per diffondere software nocivo venivano finora utilizzate soprattutto pagine Web dubbie, si può ora essere attaccati dal malware su un numero crescente di pagine con contenuti seri. Queste pagine non diffondono intenzionalmente il malware – al contrario vengono sfruttate le vulnerabilità e gli errori di configurazione delle applicazioni Web per collocare direttamente il codice nocivo sulla pagina Web oppure per dirottare l'utente su pagine Web nelle quali è annidato il malware (cfr. capitolo 2.2). L'infezione del cliente è effettuata per il tramite delle *lacune di sicurezza* del browser Web o di altre applicazioni, come ad esempio i software antivirus o i *plugin* (tra l'altro Adobe Reader, Flash, QuickTime). In tempi recenti ha fatto soprattutto cronaca il tool MPack (cfr. capitolo 5.1). MPack è uno dei diversi kit di malware venduti sulla scena malware; esso consente anche ai profani di compromettere i sistemi (cfr. capitolo 5.2).

Sfortunatamente i tassi di individuazione dei software antivirus non sono notevolmente migliorati. Nel caso di alcune varianti del malware ci sono volute parecchie settimane prima che esse potessero essere rintracciate dalla maggior parte delle soluzioni antivirus.

Gli aggressori sviluppano in continuazione nuove versioni del medesimo malware. Essi diffondono per il tramite di pagine Web compromesse una nuova versione per ogni visitatore oppure modificano le versioni a brevi intervalli di tempo. Inoltre il malware è sempre meglio camuffato sui computer infettati. Questo modo di procedere ha lo scopo di impedire che il malware sia rintracciato dai software di sicurezza e di renderne difficile l'individuazione e l'analisi da parte degli specialisti. Il tasso di individuazione del malware attuale da parte dei software antivirus si situa pertanto a un livello basso.

Gli esempi in merito si trovano nei capitoli 4.2, 5.1 e 5.2.

[14] Cfr. in merito: http://www.finjan.com/GetObject.aspx?ObjId=443 (stato: 26.07.2007).

3 Tendenze / Evoluzioni generali

3.1 Criminalità informatica e attacchi contro i servizi finanziari svizzeri

Come già menzionato nell'ultimo rapporto semestrale (capitolo 3.2), il mercato sotterraneo delle prestazioni di servizi della criminalità informatica si è nel frattempo affermato e si trova attualmente in una fase di consolidamento. Ciò vale in particolare nel settore del *phishing* e in quello del furto finanziario tramite *malware*. Nonostante la difficoltà di determinare cifre precise, esistono stime secondo le quali la criminalità informatica consente di realizzare profitti maggiori di quelli del traffico internazionale di stupefacenti[15].

Sulla scena operano diversi attori, organizzati in misura crescente con professionalità e secondo i principi della divisione del lavoro e dotati di gradi diversi di energia criminale (cfr. in merito il capitolo 5.2). Dovrebbe in particolare aumentare il numero di attori con poche qualifiche tecniche, quelli che consacrano pertanto maggiori energie criminali e perpetrano i furti veri e propri avvalendosi di malware (acquistato). Il commercio di malware sviluppato professionalmente è in continua crescita mentre cala simultaneamente il relativo grado di individuazione da parte dei software antivirus (cfr. in merito i capitoli 2.4 e 5.2).

Si può constatare una svolta: l'epoca delle «ondate» puntuali di phishing, con un inizio e una fine precisi, dovrebbe essere superata. Per quanto concerne il futuro ci si deve aspettare che gli attacchi tramite malware contro le soluzioni di e-banking provochino un deflusso di denaro durevole – paragonabile a quello delle truffe con le carte di credito.

Ci si deve aspettare che la diffusione di malware contro i portali svizzeri di e-banking venga effettuata quanto prima per il tramite di *infezioni drive-by*, invece che mediante semplici e-mail come finora (cfr. in merito i capitoli 2.1, 2.2, 2.4, 5.1 e 6). Potrebbero ben presto divenire vittime di furti di denaro dal proprio conto le persone che navigano in Internet senza tutelarsi con sufficienti misure di sicurezza (come un sistema operativo e applicazioni interamente aggiornati) e visitano homepage appositamente predisposte. Non basterà più reagire a un messaggio e-mail sospetto.

La diffusione di attacchi di malware contro i servizi finanziari non subirà grandi cambiamenti finché non sarà stato raggiunto a livello internazionale un migliore coordinamento delle procedure di perseguimento penale e non sarà stata implementata un'armonizzazione delle legislazioni e finché non saranno stati attuati miglioramenti tecnici nel settore della sicurezza delle soluzioni di e-banking. In Svizzera si lamenta inoltre l'assenza di una sovranità di perseguimento penale a livello federale per questi casi tipicamente intercantonali e internazionali. Il coordinamento delle indagini tra i corpi cantonali di polizia interessati ne sminuisce l'efficienza e dovrebbe pertanto essere operato imperativamente a livello federale. Occorrerebbe inoltre che in caso di eventi si sporga una denuncia conseguente alla polizia.

La situazione attuale è tematizzata nel capitolo 2.1; il capitolo 4.2 esamina gli eventi in Svizzera, mentre il capitolo 5.2 analizza la situazione a livello internazionale.

[15] Cfr. p.es.: http://www.vnunet.com/articles/print/2189322; http://www.silicon.com/publicsector/0,3800010403,39166127,00.htm (stato: 30.07.2007).

4 Situazione attuale dell'infrastruttura TIC a livello nazionale

4.1 Attacchi

Attacco contro il sito Web di una ditta svizzera nel campo della tecnologia spaziale

Nel corso del mese di giugno 2007 è stato constatato un accesso non autorizzato al settore protetto da password di una pagina Web contenente dati nel campo della ricerca sui propulsori per razzi. Grazie ai sensori installati l'accesso illegale ha potuto essere rapidamente individuato e impedito, di modo che nessun dato ha potuto essere scaricato. L'accesso alla pagina in questione è stato operato da un *indirizzo IP* del Vicino Oriente, segnatamente dalla Palestina e dalla Siria. Non è chiaro se l'attacco sia stato effettivamente sferrato da questi Paesi oppure a partire da computer che vi sono situati, per camuffarne la provenienza effettiva. In questo contesto occorre però menzionare che una settimana circa prima dell'attacco era stato inviato un e-mail, anch'esso da un indirizzo IP in Palestina, che sollecitava una collaborazione con la ditta in questione.

Questo esempio illustra che anche imprese di minori dimensioni possono essere vittima di attacchi di spionaggio industriale. In questo caso solo l'applicazione esemplare di misure di sicurezza ha potuto impedire il trasferimento involontario di conoscenze.

Nel capitolo 2.2 MELANI effettua una valutazione degli attacchi contro i server Web; il capitolo 2.3 tematizza lo spionaggio industriale mirato contro le imprese svizzere.

4.2 Criminalità

Attacchi di malware contro i servizi finanziari svizzeri

Come menzionato nel capitolo 2.1, gli attacchi tramite malware contro gli istituti finanziari svizzeri sono fortemente aumentati nel corso del primo semestre del 2007. È soprattutto nei mesi di maggio e di giugno che si sono verificati due incidenti maggiori per il tramite di e-mail i cui mittenti erano stati falsificati.

Una prima ondata di *spam* a scapito di indirizzi svizzeri di posta elettronica si è spacciata come comunicazione ufficiale di Ricardo.ch, una nota ditta di aste online. L'e-mail del presunto team di Ricardo.ch invitava il destinatario a pagare una fattura ancora scoperta. Per visionare i dettagli della fattura occorreva aprire un allegato, all'apparenza un documento in formato PDF. In realtà l'allegato era un programma eseguibile: aprendo il documento il proprio PC veniva infettato dal *malware* Nurech / Wsnpoem.

Un attacco analogo si è verificato alcune settimane dopo. Questa volta l'e-mail era inviato in nome di uno studio legale bernese che non aveva niente a che fare con l'attacco. Anche questa volta il malware era camuffato in una finta fattura in formato PDF. Il numero di indirizzi elettronici validi ai quali i criminali hanno inviato l'e-mail è impressionante: il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) ha ricevuto nel giro di pochi giorni oltre 600 comunicazioni relative a questo evento, il che costituisce un primato.

In entrambi i casi le vittime non potevano accorgersi di essere state infettate dopo aver aperto l'allegato: al momento dell'attacco la maggior parte dei programmi antivirus non erano ancora in grado di individuare questo malware. Il malware rimaneva inattivo finché la vittima decideva di accedere al proprio conto bancario tramite e-banking. Solo a quel momento alcuni processi inabituali facevano presagire la presenza del malware. A titolo di esempio veniva visualizzata una pagina vuota con una sbarra che indicava il caricamento lento della pagina oppure si apriva una finestra pop-up. Queste indicazioni erano destinate a far credere alla vittima che i servizi di e-banking erano temporaneamente sovraccarichi. In realtà veniva interrotto il collegamento con il server in modo che i criminali potessero effettuare simultaneamente transazioni finanziarie illegali in nome della vittima.

Diversamente dai casi di «*infezioni drive-by*» (cfr. in merito i capitoli 2.2, 2.4, 5.1 e 6) l'utente stesso infetta il proprio computer cliccando sulla presunta fattura. Per confortare la credibilità degli e-mail, gli aggressori vi inseriscono informazioni adeguate al contesto regionale – il medesimo malware è stato utilizzato contro le banche anche all'estero, ma inviando e-mail diversi o operando tramite infezioni drive-by (cfr. in merito il capitolo 5.2). MELANI raccomanda di non cliccare mai sugli allegati o sui link senza avere la certezza che gli e-mail provengono da persone degne di fiducia e che si tratta effettivamente di un documento atteso.

Gli attacchi perseguono l'obiettivo di assumere il controllo delle sessioni di e-banking. Se avete già cliccato sull'allegato dubbio o su un link, sincerateVi prima della prossima sessione di e-banking che il vostro computer è esente dal malware. Se del caso ricorrete ai consigli di uno specialista. Se durante la sessione di e-banking osservate comportamenti inabituali (come quelli descritti qui sopra) rivolgetevi senza indugio alla vostra banca.

Gli attacchi perpetrati dopo l'ondata di spam sono stati in parte efficaci. MELANI non dispone di cifre precise riguardo al volume dei fondi sottratti e al numero di incidenti. Essi si situano comunque a un livello nettamente inferiore rispetto a quello delle truffe in ambito di carte di credito e di carte EC.

Nel capitolo 2.1 MELANI effettua una valutazione degli attacchi di malware contro i servizi finanziari; le tendenze sono tematizzate nel capitolo 3.1 e la situazione a livello internazionale nel capitolo 5.2. Il prossimo contributo tematizza gli attacchi classici di phishing contro gli istituti finanziari svizzeri. Il trasporto del denaro viene in genere effettuato da «money mules» – cfr. in merito il capitolo 4.3.

Attacchi classici di phishing contro i servizi finanziari svizzeri

Ondate di phishing contro la clientela VISA svizzera

Nel corso del primo semestre del 2007 sono state osservate tre ondate di *phishing* contro la clientela svizzera delle carte di credito VISA. Esse si sono sempre verificate seguendo il medesimo modello. Un e-mail di *spam*, inviato presuntamente dal servizio di sicurezza di VISA, esige la verifica dei dati della carta di credito, perché la carta corrispondente potrebbe essere stata oggetto di abusi. A tale scopo si richiede di passare allo scanner il recto e il verso della carta di credito e di inviarli come documento PDF, tramite e-mail, all'indirizzo di posta elettronica fornito dai truffatori.

Un dettaglio interessante di questi e-mail di spam è costituito dal fatto che ogni destinatario è interpellato con il suo proprio nome. Tale nome non può essere desunto in ogni caso dall'indirizzo di posta elettronica. Ciò significa che gli elenchi di indirizzi e-mail dei truffatori migliorano qualitativamente e potrebbero senz'altro contenere ulteriori indicazioni oltre a quella dell'indirizzo di posta elettronica. Per questo tramite gli autori possono dare un tocco di maggiore professionalità alle loro truffe e quindi rivolgersi personalmente alle vittime,

come descritto qui sopra. È pure degno di nota il fatto che gli e-mail delle due prime ondate siano stati redatti in inglese. Nel caso della terza ondata i truffatori hanno tradotto il testo in tedesco. Questo significa che i primi due tentativi non hanno avuto molto successo e che i truffatori hanno reagito a questa circostanza. Va pure notato che ogni volta MELANI ha potuto rapidamente disattivare i domini utilizzati per la truffa (con gli indirizzi e-mail) di modo che il periodo durante il quale essa poteva essere perpetrata è stato molto breve.

Niente più tentativi efficaci di phishing «classico» contro gli istituti finanziari svizzeri

Anche nel corso del primo semestre si sono verificati tentativi di phishing «classico» contro i fornitori svizzeri di prestazioni finanziarie. Essi sono stati di scarsa quantità e qualità e non hanno avuto successo. Gli attacchi concernevano ad esempio i nomi di login e le password, ma non però i numeri degli elenchi di stralcio. La cattiva preparazione e le procedure in parte dilettantistiche fanno presumere che si trattasse di altri autori, meno professionisti di quelli degli attacchi di malware osservati (cfr. in merito l'ultimo contributo). Un accertamento interessante è comunque il fatto che questi attacchi sono stati diretti anche contro fornitori di prestazioni finanziarie piccoli e meno conosciuti. È pure stata osservata un'ondata di e-mail di phishing in lingua francese, una novità in Svizzera.

Si può affermare in genere che in Svizzera gli attacchi «classici» di phishing non presentano praticamente più alcun pericolo – esso è invece presente negli attacchi perpetrati con malware.

Nel capitolo 2.1 MELANI effettua una valutazione degli attacchi di malware contro i servizi finanziari; le tendenze sono tematizzate nel capitolo 3.1 e la situazione a livello internazionale nel capitolo 5.2. Gli attacchi di malware contro le banche svizzere sono tematizzati nell'ultimo contributo (cfr. pagina precedente).

4.3 Diversi

Pump and dump, banche fittizie e money mules. Questi mail di spam intasano le caselle postali elettroniche in Svizzera

Pump and dump

Nel secondo rapporto semestrale 2006 di MELANI è già menzionata l'esistenza dei cosiddetti «*spam* stock pump and dump» (capitolo 2.2). Queste informazioni spam consigliano l'acquisto di azioni e sono destinate ad aumentarne per breve tempo la loro quotazione in borsa. Durante questo periodo di tempo gli spammer vendono le azioni acquistate in precedenza, approfittando dell'aumento a breve termine del corso. Le informazioni, inizialmente redatte in maniera semplice, si sono nel frattempo sviluppate in vere e proprie analisi finanziarie che seducono per il loro linguaggio curato, che ne può accrescere la credibilità. Talvolta vi si aggiungono nuove tecniche, come ad esempio il contatto telefonico.

Banche fittizie

La rinomanza della Svizzera come piazza finanziaria funge ulteriormente da calamita per la creazione di banche online fittizie, nella cui denominazione viene inserito il nome del nostro Paese. Nel primo semestre del 2007 sono stati registrati diversi URL con nomi come www.swissbank-offshoreuk.page.tl oppure www.swissbank.page.tl; su queste pagine Web

sono addirittura state collocate immagini della Direzione generale della Banca nazionale per conferire loro un carattere ufficiale.

Money mules

Nella prospettiva di realizzare un guadagno accessorio – soprattutto quando l'onere è minimo e non si esigono speciali qualifiche – numerose persone sono indotte a farsi arruolare dai criminali come cosiddetti «agenti finanziari». Gli agenti finanziari devono consacrare ogni giorno un po' del loro tempo per farsi versare sul loro conto denaro che dovranno successivamente trasferire a terzi. Una determinata percentuale del denaro versato può essere conservata come provvigione. Questi cosiddetti *money mules*, ossia corrieri finanziari, che si lasciano arruolare per il riciclaggio di denaro proveniente da truffe online (soprattutto phishing), sono sempre più apprezzati dai criminali. I numerosi casi annunciati a MELANI costituiscono una testimonianza delle dimensioni raggiunte nel frattempo da questo fenomeno di criminalità su Internet. Parallelamente all'aumento degli attacchi di *malware* (cfr. in merito i capitoli 2, 4.1 e 5.2) cresce anche il numero di offerte di lavoro per corrieri finanziari, che sono in genere proposte alla vigilia di attacchi di malware contro i portali di e-banking. Nei pertinenti e-mail si prospettano attività semplici e remunerative; sovente queste offerte contengono link a pagine Internet allestite appositamente a questo scopo.

Nel corso del primo semestre del 2007 sono state registrate numerose pagine Web di questo genere. Tutte presentano nomi analoghi e hanno sovente il medesimo stile. Le imprese che vi appaiono affermano di essere attive nei più diversi settori, dal settore finanziario a quello del commercio su Internet, passando dal settore delle donazioni. Esse si presentano per il tramite di homepage di aspetto professionale, con nomi come Mimotrans, GammaFinance, Next Level oppure Donation Europe e tentano in tal modo di dissipare i dubbi eventuali dei corrieri potenziali sulla legittimità del loro operato[16].

Numerosi criminali (informatici) si avvalgono dei sistemi di trasferimento di denaro in contanti come Western Union, MoneyGram ecc. per trasferire all'estero il denaro derubato. Si vuole così interrompere il cosiddetto paper-trail, ossia la tracciabilità di un trasferimento di denaro. Si impone di massima la prudenza ogni volta che una persona o un'organizzazione sconosciute insistono sull'utilizzazione dei servizi di simili istituti di trasferimento di denaro in contanti per effettuare una transazione finanziaria. Ciò non si applica unicamente al caso qui descritto degli agenti finanziari, ma anche alle aste online di merci, alla prenotazione di camere d'albergo o a una vincita inattesa al lotto. MELANI consiglia di raccogliere un massimo di informazioni sulle persone (o organizzazioni) che esigono il trasferimento in contanti di denaro. In caso di dubbio vale il principio: giù le mani! Va inoltre rammentato che le persone che forniscono il loro aiuto al trasferimento di denaro proveniente da attività illegali si rendono colpevoli di riciclaggio di denaro.

Internet: ondata di e-mail di spam con minacce di morte

All'inizio del mese di maggio è stato inviato un e-mail che esigeva dal destinatario, minacciandolo di morte, il versamento di una somma di denaro. In Svizzera numerose persone e piccole e medie imprese hanno ricevuto simili e-mail. L'e-mail di spam, redatto in

[16] Un esempio di simile falsa offerta di lavoro à reperibile in: http://www.melani.admin.ch/dienstleistungen/archiv/01023/index.html?lang=it nonché http://www.melani.admin.ch/dienstleistungen/archiv/00441/index.html?lang=it (stato: 21.08.2007).

un tedesco approssimativo, è stato inviato per il tramite di server all'estero. L'invio è stato effettuato in modo aleatorio, senza un modello riconoscibile di selezione dei destinatari. Il contenuto, compresa la minaccia, non è stato che uno scherzo di cattivo gusto.

In considerazione dell'elevato fabbisogno di informazione della popolazione, l'Ufficio federale di polizia ha pubblicato un comunicato stampa d'intesa con i Cantoni. Il comunicato in questione raccomanda ai cittadini di non rispondere in nessun caso a simili e-mail e di non comunicare qualsiasi dato personale.

5 Situazione attuale dell'infrastruttura TIC a livello internazionale

5.1 Attacchi

Sollevano questioni gli attacchi DDos contro l'Estonia dettati da motivazioni politiche

Alla fine del mese di aprile l'Estonia è stata per più settimane oggetto di *attacchi DDos* tramite Internet. La maggior parte degli obiettivi attaccati è rimasta indisponibile per parecchio tempo. Per arginare gli attacchi l'Estonia si è in parte vista costretta a impedire i collegamenti Internet con l'estero. L'origine degli attacchi potrebbe essere stata il trasferimento del monumento russo al «milite ignoto (russo)» dal centro della capitale estone Tallin a un cimitero militare alla periferia della città. Il trasferimento in questione aveva provocato violente dimostrazioni da parte della minoranza russa di Tallin nonché attacchi della gioventù russa contro l'ambasciata estone a Mosca. I Russi considerano primariamente il monumento come simbolo della loro vittoria nella Seconda guerra mondiale, mentre per la maggior parte degli Estoni esso dovrebbe essere posto in relazione con l'occupazione russa durante la guerra fredda. L'Estonia è considerata uno dei Paesi più progrediti d'Europa per quanto concerne l'impiego delle nuove tecnologie dell'informazione e della comunicazione[17].

Poco tempo dopo l'inizio degli attacchi le pagine Web del presidente estone, del primo ministro, del Parlamento e di quasi tutti i ministeri non sono più state raggiungibili. A partire dal 30 aprile gli attacchi si sono intensificati e si sono estesi ai provider di servizi Internet estoni, ai giornali, ai server di posta elettronica, alle banche online, alle università e a diversi altri servizi Internet. Gli attacchi hanno raggiunto il loro culmine il 9 maggio, data alla quale la Russia commemora la sua vittoria sulla Germania nazista: gli attacchi, verosimilmente sferrati da una *rete bot* distribuita in tutto il mondo e comprendente oltre un milione di «zombie» infettati, hanno in parte raggiunto una notevole larghezza di banda. Il 10 maggio i

[17] Cfr. le informazioni che fanno luce sul contesto di questo incidente: http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598; http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868 (stato: 16.07.2007).

violenti attacchi DDos sono nuovamente cessati, perché era presumibilmente scaduto il termine di locazione di 24 ore della rete bot utilizzata[18].

Poco dopo l'inizio degli attacchi le autorità estoni dichiararono che esistevano prove dell'origine di questi attacchi al Cremlino[19]. Da analisi successive – anche da parte di esperti internazionali inviati sul posto dalla NATO, dagli USA, da Israele e dall'UE – è emerso che l'attacco non era riconducibile a Mosca. Si doveva piuttosto partire dall'idea che si trattava di un caso tipico di «hacktivismo», ossia di hacking con motivazioni politiche. Questa supposizione è corroborata dal fatto che gli attacchi sono stati sferrati da fonti diverse e si sono succeduti con intensità e durata diversa. Inoltre gli attacchi sarebbero stati troppo poco elaborati per presumere la presenza di un Governo dietro di essi[20]. Di massima la situazione è la medesima di quella nel caso della criminalità informatica in generale: è estremamente difficile identificare indubbiamente l'autore di un attacco.

Gli attacchi DDoS contro l'Estonia non sono stati gli unici importanti attacchi nel primo semestre del 2007: dopo un attacco (senza successo) contro parecchi *server root DNS* nel mese di febbraio, nel corso del mese di giugno anche diversi fornitori di servizi antispam si sono trovati nel mirino degli aggressori[21]. Questi attacchi evidenziano di quali risorse disponga nel frattempo la criminalità organizzata: le sue reti bot non sono affittate unicamente per l'invio di e-mail di spam. Anche le persone interessate ad attacchi DDos sono disposte a pagare per l'utilizzo di reti bot, come con grande probabilità nel caso degli attacchi contro l'Estonia.

Gli attacchi DDoS a sfondo politico – proprio come la deturpazione di homepage (i cosiddetti «de*facement*») con pamphlet politici – non sono una novità. Al bombardamento per errore dell'ambasciata cinese nel corso della guerra del Kosovo alla fine degli anni Novanta, all'inizio dell'ultima guerra dell'Iraq nel 2003 e all'apparizione delle caricature di Maometto sui giornali danesi nel 2006 hanno fatto seguito simili attacchi. Anche questa volta si è potuto osservare come nei pertinenti forum circolassero istruzioni sulle modalità di attacco delle pagine Web estoni in maniera semplice, anche da parte di persone senza qualifiche tecniche. La novità in questo caso è costituita dall'entità dell'attacco che è stato in grado di impedire a tutto un piccolo Stato l'utilizzazione delle sue tecnologie dell'informazione.

Nello stato attuale delle conoscenze gli attacchi contro l'Estonia non possono essere attribuiti alla Russia ufficiale o posti in relazione con un altro attore concreto. Alcuni indizi consentono nondimeno di concludere che la loro origine debba piuttosto essere ricercata presso le cerchie nazionaliste russe. In questo contesto non si tratta di accertare in quale misura siano esistite intese, istigazioni o sostegni reciproci tra i presunti attori. Vengono nondimeno sollevate importanti questioni: come deve essere considerato in diritto internazionale (della guerra) un attacco con mezzi informatici contro uno Stato? Cosa significa un simile attacco per la NATO? In caso di attacco militare contro un membro della NATO l'articolo 5 del

[18] Cfr.: http://www.nytimes.com/2007/05/29/technology/29estonia.html?hp nonché http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html (stato: 16.07.2007).

[19] Cfr. in merito: http://www.heise.de/tp/r4/artikel/25/25218/1.html; http://www.tagesspiegel.de/politik/International;art123,1785339 (stato: 16.07.2007).

[20] L'analisi più particolareggiata è fornita da Arbor Networks: http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/; anche l'US-CERT giunge alla medesima conclusione: http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/print_view/ (stato: 16.07.2007).

[21] In merito ad attacchi DDos paragonabili cfr. anche il rapporto semestrale MELANI 2006/I, capitolo 5.3; in merito agli attacchi contro i server root DNS: http://asert.arbornetworks.com/2007/06/february-2007-root-server-attacks-a-qualitative-report/ (stato: 16.07.2007).

trattato NATO che lo considera automaticamente come un attacco diretto contro tutti i membri della NATO (cosiddetto caso di difesa collettiva)[22]?

La NATO ha già iscritto la questione delle cosiddette «information operations» nella sua agenda e intende da un canto raggiungere una migliore capacità di difesa contro gli attacchi ai sistemi di informazione ed estendere d'altro canto anche a simili eventi l'applicazione dell'articolo 5 del suo trattato[23]. In genere il diritto internazionale non si esprime sulla questione degli attacchi informatici sebbene l'esempio dell'Estonia dimostri in quale misura le economie odierne siano dipendenti dalle tecnologie dell'informazione.

Non soltanto la NATO ma anche gli Stati nazionali si apprestano a istituire e ad ampliare le loro capacità nel settore della guerra informatica (cfr. in merito anche il capitolo 7.1).

Attacchi tramite il World Wide Web (infezioni drive-by): esempio «MPack»

Nel corso del primo semestre del 2007 è aumentato il numero di cosiddette «*infezioni drive-by*» (installazione di *malware* all'atto della visita di pagine Web infettate), che costituiscono una delle minacce di maggiore attualità (cfr. capitoli 2.2, 2.4 nonché l'ultimo rapporto semestrale). L'esempio più rilevante per illustrare questa tendenza è «MPack» – un'applicazione per server Web per il cui tramite decine di migliaia di computer sono stati infettati da malware nel mese di giugno per il solo fatto di avere visitato pagine Web appositamente predisposte. MPack può essere ottenuto come toolkit provvisto di supporto e di aggiornamenti sulla scena sotterranea del malware (cfr. in merito alla scena malware, ai prezzi ecc. il capitolo 5.2)[24].

Gli aggressori hanno in particolare manipolato pagine Web dell'Italia – probabilmente oltre 10'000[25] – introducendovi una riga di codice che all'atto del caricamento della pagina scarica malware in provenienza da un altro server. Essa contiene MPack, un tool di infezione automatica. Esso esamina anzitutto quale sistema operativo e quale browser utilizza la vittima per poi provare in successione *exploit* a seconda delle applicazioni utilizzate – ossia per sfruttare simultaneamente più *lacune di sicurezza* (p.es. in diversi prodotti Microsoft come Internet Explorer, i servizi dei sistemi operativi Windows, Media Player ecc., ma anche WinZip o Apple QuickTime). Di fatto MPack ha finora sfruttato unicamente lacune di sicurezza già note. I sistemi interamente aggiornati non hanno potuto essere infettati. È comunque ipotizzabile che un simile tool venga ampliato in ogni momento mediante *0-day-exploit.*

Non appena un exploit funziona è possibile caricare a piacimento malware sul sistema infettato. Si può trattare ad esempio anche di «Torpig» (cfr. in merito i capitoli 4.2 e 5.2), finora diretto soltanto contro l'e-banking estero oppure di malware per collezionare dati personali. È altresì ipotizzabile l'integrazione dei computer infettati in una *rete bot* che può essere successivamente utilizzata per l'invio di *spam*. L'attacco contro le pagine Web italiane ha manifestamente infettato oltre 80'000 computer. Per quanto concerne le pagine Web

---

[22] Cfr. in merito: http://www.economist.com/world/international/displaystory.cfm?story_id=9228757 (stato: 16.07.2007).

[23] Cfr.: http://www.nato.int/docu/pr/2007/p07-067e.html (stato: 16.07.2007).

[24] Informazioni generali concernenti MPack: http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=8656&ver=21&pagina=3&numprod=&entorno= http://reviews.cnet.com/4520-3513_7-6745285-1.html; http://www.heise.de/newsticker/meldung/91542 nonché http://blog.washingtonpost.com/securityfix/2007/06/the_mother_of_all_exploits_1.html (stato: 17.07.2007).

[25] Cfr. in merito: http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782 (stato: 17.07.2007).

manipolate si tratta perlopiù di offerte turistiche, alberghiere, di locazione di veicoli o di altre offerte per niente dubbie[26].

Come comunicato da ISC SANS le pagine Web compromesse sono state ospitate a migliaia su pochi server fisici. La compromissione di tutte le pagine Web è stata manifestamente effettuata per il tramite della lacuna di sicurezza di un'unica pagina Web che gli aggressori hanno potuto sfruttare in combinazione con una configurazione carente del server a livello di provider. In altre parole è bastata una pagina Web mal curata su questo server per pregiudicare tutte le altre pagine che vi erano memorizzate[27].

Nel caso di questo tipo di attacco è degno di nota il fatto che un numero sempre maggiore di pagine Web serie è vittima degli attacchi degli hacker e che poi venga diffuso malware all'insaputa dei webmaster responsabili (cfr. capitolo 2.2). La navigazione con pieni diritti di amministratore diviene pertanto un rischio notevole, in particolare anche per le imprese.

In teoria, anche se il sistema operativo e le applicazioni sono interamente aggiornati, è possibile essere infettati dal malware per il solo fatto di aver visitato una homepage seria e senza avere cliccato su alcunché, senza avere aperto un allegato o senza avere ricevuto un e-mail e avervi reagito. Nella prassi però vengono attualmente sfruttate quasi esclusivamente lacune di sicurezza conosciute che non si riscontrano sui computer aggiornati.

Il capitolo 2.2 tematizza l'aumento degli attacchi ai server Web, mentre il capitolo 6 esamina le misure preventive contro le infezioni drive-by.

5.2 Criminalità

Attacchi di phishing e tramite malware contro i servizi finanziari: situazione internazionale

Gli attacchi di *phishing* e di *malware* non sono di attualità soltanto in Svizzera (cfr. capitoli 2.1 e 4.2). Anche a livello internazionale di afferma la tendenza agli attacchi con malware contro i fornitori di prestazioni finanziarie. Nelle sue statistiche per il primo semestre del 2007 l'Anti-Phishing Working Group rileva ad esempio un notevole aumento del numero di pagine Web che diffondono malware in questo intento[28].

L'incidente più spettacolare è venuto alla luce all'inizio dell'anno in Svezia quando la Nordea, la maggiore banca scandinava, è stata vittima di un attacco efficace di malware. Furono derubati circa 900'000 euro da almeno 250 clienti della banca. A tale scopo è stato utilizzato un malware appositamente predisposto per questo attacco, che può essere acquistato per poche migliaia di dollari US sul mercato nero russo da un programmatore denominato «The Corpse» (cfr. in merito il prossimo contributo). Il malware è fornito unitamente alla garanzia che non può essere individuato dai software antivirus. L'*autentificazione a due fattori* praticata dalla banca Nordea – analoga al sistema di autentificazione utilizzato dalle banche

[26] Informazioni dettagliate su MPack sono reperibili in: http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf?sitepanda=particulares nonché http://isc.sans.org/diary.html?storyid=3015 (stato: 17.07.2007).

[27] Cfr.: http://isc.sans.org/diary.html?storyid=3078 (stato: 17.07.2007).

[28] Cfr.:http://www.antiphishing.org; http://www.darkreading.com/document.asp?doc_id=123771 (stato: 18.07.2007).

svizzere – ha potuto essere elusa efficacemente[29]. Anche in altri Paesi si sono verificati numerosi attacchi *man-in-the-middle* (attacchi MITM) efficaci, come ad esempio in aprile nei Paesi Bassi contro la banca ABN Amro[30].

Nel primo semestre del 2007, specialmente nel corso del mese di aprile, si è osservato un forte aumento delle pagine di phishing, anche se il numero di incidenti notificati permane costante da circa un anno[31]. Ne è origine il fatto che i kit di phishing si diffondono sempre più[32]. Nel caso di questi kit si tratta di tool, sovente provvisti di una semplice interfaccia grafica di utente, venduti da programmatori esperti e tramite i quali anche i principianti possono effettuare in maniera relativamente facile attacchi di phishing (cfr. in merito anche il contributo su «RockPhish» nell'ultimo rapporto semestrale nonché il secondo prossimo contributo). Grazie a questi tool è possibile predisporre centinaia di pagine phishing (oppure pagine proxy per attacchi MITM) che per il solo fatto del loro grande numero possono essere difficilmente combattute e sono pertanto piuttosto efficaci[33]. Il numero di gruppi che praticano il phishing ad alto livello dovrebbe invece essere rimasto costante.

Contro i sistemi di autentificazione più semplici sono tuttora in atto gli attacchi classici di phishing tramite e-mail e richiesta del nome di utente e della password, come tra l'altro contro gli utenti di homepage di social networking, come ad esempio MySpace[34].

Uno dei principali motivi dell'aumento degli attacchi potrebbe essere l'introduzione progressiva dell'autentificazione a due fattori nello spazio anglosassone: PayPal, Ebay e Barclays, una della maggiori banche britanniche, ne sono soltanto gli esempi più eminenti[35]. Ne è causa la raccomandazione reiterata nell'agosto 2006 dall'autorità statunitense di vigilanza sulle banche di introdurre l'autentificazione a due fattori nel settore bancario. La raccomandazione è stata seguita da un numero sempre maggiore di banche; entro la fine di quest'anno la maggior parte della banche dello spazio anglosassone dovrebbero avere raggiunto l'elevato standard di sicurezza applicato in Europa e soprattutto in Svizzera[36]. Se finora gli aggressori non si erano dati la pena di attaccare i sistemi a due fattori a causa della vasta diffusione di obiettivi semplici, le cose stanno ormai cambiando.

È pure degno di nota il fatto che per attaccare i servizi finanziari all'estero si faccia in parte capo alla medesima (famiglia) di malware utilizzata in Svizzera. Esso è però diffuso tramite e-mail di aspetto diverso e in parte tramite *infezioni drive-by* (cfr. in merito i capitoli 2.2, 2.4 e 5.1). Anche i metodi di s*ocial engineering* sono adeguati a livello regionale dagli aggressori.

---

[29] Informazioni sull'incidente Nordea: http://www.nytimes.com/2007/01/25/technology/25hack.html?ex=1327381200&en=58990497ce27b2b2&ei=5088&partner=rssnyt&emc=rss (stato: 18.07.2007).

[30] Cfr. in merito all'incidente ABN Amro: http://www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/ (stato: 18.07.2007).

[31] Cfr. i rapporti dell'Anti-Phishing Working Group: http://www.antiphishing.org (stato: 18.07.2007).

[32] Cfr.: http://blogs.iss.net/archive/PhishingIncreases.html; http://blogs.iss.net/archive/PhishingKits.html; http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0607.pdf; http://www.rsa.com/press_release.aspx?id=7667; http://asert.arbornetworks.com/2007/04/peeling-the-covers-off-of-rock/; http://blog.washingtonpost.com/securityfix/2007/05/phishing_attacks_soar_nets_wid_1.html (stato: 18.07.2007).

[33] Una sintesi chiara delle procedure è reperibile in: http://blogs.iss.net/archive/PhishingMicroscope.html (stato: 18.07.2007).

[34] Cfr. in merito: http://isc.sans.org/diary.html?storyid=2808; oppure un'intervista con un phisher di MySpace in: http://ha.ckers.org/blog/20070508/phishing-social-networking-sites/ (stato: 18.07.2007).

[35] Cfr. in merito: http://www.infoworld.com/article/07/06/15/paypal-using-verisign-tokens_1.html; http://www.infoworld.com/article/07/06/15/paypal-using-verisign-tokens_1.html (stato: 18.07.2007).

[36] Cfr. in merito: http://www.ffiec.gov/press/pr101205.htm; http://www.ffiec.gov/press/pr081506.htm; nonché http://www.darkreading.com/document.asp?doc_id=129868&f_src=darkreading_default (stato: 18.07.2007).

Il capitolo 2.1 contiene una valutazione sugli attacchi di phishing e di malware e sulla sicurezza dell'autentificazione a due fattori. I commenti relativi agli incidenti in Svizzera figurano nel capitolo 4.2.

Rimane di attualità la rivelazione involontaria di dati dovuta allo spionaggio industriale o alla perdita di supporti di dati: l'esempio della TJX

La maggior parte delle perdite di dati sono il fatto di smarrimenti o di furti di laptop, di nastri di backup, di CD-ROM, di schede USB o di altri media di memorizzazione. Negli ultimi quattro anni persino l'FBI ha smarrito 160 laptop sui quali erano per l'appunto memorizzati dati confidenziali[37]. Come spiegato nei capitoli 2.2 und 2.3 sono però sempre più in aumento le perdite di dati consecutive ad attacchi mirati (s*ocial engineering*) contro i collaboratori, sui server Web e su altri sistemi.

Un esempio eminente è costituito dall'incidente occorso alla catena anglo-americana di grandi magazzini TJX. Come reso noto all'inizio dell'anno, dal luglio del 2005 sono stati manifestamente derubate sistematicamente 45 milioni di stringhe di dati di carte di credito dai sistemi di disbrigo dei pagamenti e di memorizzazione dell'impresa. L'effrazione nei sistemi informatici è stata constata soltanto nel dicembre 2006. Nel corso delle indagini successive è emerso che gli aggressori continuavano ad avere accesso ai sistemi. L'accesso ha potuto essere impedito definitivamente soltanto nel gennaio del 2007. Questo incidente rappresenta il maggiore furto in assoluto di dati di carte di credito: secondo le dichiarazioni delle associazioni dei banchieri si presume che ne sia stato colpito fino al 30% della popolazione della Nuova Inghilterra. In Florida è stata arrestato un circolo di commercianti che utilizzava abusivamente dati di carte di credito forniti dalla TJX. I dati delle carte di credito erano in vendita su apposite pagine in Internet. Per quanto concerne i costi insorti alla TJX si sa unicamente che la sola inchiesta sull'incidente e le successive misure di rafforzamento della sicurezza informatica ammontano a 5 milioni di dollari US. TJX dovrebbe comunque essere confrontata con costi maggiori in considerazione delle querele già sporte, tanto più che le banche hanno manifestamente dovuto indennizzare i clienti versando dozzine di milioni di dollari US. Il Wall Street Journal stima fino a 1 miliardo di dollari US i costi a lungo termine della TJX. Si presume che gli aggressori abbiano avuto accesso alla rete a causa della protezione insufficiente del WLAN e della successiva lettura concomitante delle password, come pure tramite l'utilizzazione di software di spionaggio[38].

Come menzionato nel capitolo 2.3, nel caso degli attacchi contro le imprese si tratta attualmente soprattutto di attacchi mirati. A prescindere dagli e-mail allestiti in maniera abile, indirizzati a persone selezionate e provvisti di un link a una pagina Web infestata da *malware* o accompagnati da malware in allegato, si verificano sovente attacchi ai server Web (cfr. i capitoli 2.2 e 5.1) o tramite il WLAN, come nel caso della TJX.

---

[37] Cfr. il rapporto del Department of Justice statunitense: http://www.usdoj.gov/oig/reports/FBI/a0718/exec.htm (stato: 19.07.2007).

[38] Cfr.: http://www.boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9009300; http://www.infoworld.com/article/07/03/29/HNtjxfiling_2.html nonché http://online.wsj.com/article_email/article_print/SB117824446226991797-lMyQjAxMDE3NzA4NDIwNDQ0Wj.html. Una sintesi dei furti di dati negli USA è reperibile in: http://www.privacyrights.org/ar/ChronDataBreaches.htm (stato: 19.07.2007).

Pertanto i dati sensibili dovrebbero essere memorizzati in maniera cifrata (in particolare sui laptop, i PDA, le schede USB, i CD ROM o i nastri di backup). Per quanto concerne il caso della TJX va osservato che i WLAN dovrebbero essere cifrati.

Mercato sotterraneo e criminalità informatica: tendenze più recenti e prezzi

La divisione del lavoro all'interno della scena criminale informatica è già stata tematizzata nell'ultimo rapporto semestrale come pure nel capitolo 3.1. Illustriamo ora sulla scorta di alcuni esempi di attualità a quali prezzi sono ottenibili alcune prestazioni di servizi.

Nel corso del primo semestre del 2007 ha potuto essere constatata una tendenza all'utilizzazione di «kit di *malware*», come evidenziato dall'esempio di MPack (cfr. il capitolo 5.1). Il toolkit, ottenibile con supporto e aggiornamenti regolari degli *exploit* utilizzabili, è stato originariamente offerto per 1000 dollari US sul mercato sotterraneo russo da un certo «$aSH»[39]. Con la crescita della sua notorietà taluni avvoltoi lo hanno successivamente offerto a prezzi di dumping[40]. Il team di sviluppo consta manifestamente di tre persone, mentre «$aSH» è stato designato come «Marketing Director» da uno sviluppatore. Secondo le indicazioni fornite dallo sviluppatore gli exploit utilizzati per il kit sono oggetto di scambio, sono derivati da *lacune di sicurezza* conosciute oppure acquistati sul mercato sotterraneo. Nel caso di questo gruppo si tratta manifestamente di sviluppatori con un posto regolare di lavoro, che non si considerano personalmente come criminali, ma che durante il loro tempo libero sviluppano e vendono malware[41].

Anche Haxdoor, il malware utilizzato per l'attacco alla banca svedese Nordea (cfr. in merito un primo contributo del capitolo 5.2), è ottenibile sul mercato sotterraneo. Un giornalista svedese si è veduto offrire per 3000 dollari US una versione adeguata e non individuabile da parte dei software antivirus. Questo malware proviene manifestamente da uno sviluppatore che opera da solo, denominato «Corpse», che lo offre anche in proprio – compreso il supporto e, se ne è fatta richiesta, un sito sicuro di memorizzazione online dei dati derubati[42].

Per i bisogni della criminalità informatica (praticamente) tutto è disponibile presso gli «esperti» del mercato: malware, exploit, informazioni sulle lacune di sicurezza, *reti bot* per l'invio di *spam* o per estorsioni tramite attacchi *DDos*, siti sicuri di hosting del malware o di dati ottenuti illegalmente[43]. I prezzi sono calcolati per unità di tempo (tra 10 e 20 dollari US all'ora per gli attacchi DDos), per server di spam e spam inviati (600 dollari US per 10'00'000 di e-mail al giorno), per account (50 dollari US per le pagine russe di e-business, 7 dollari US per gli account EBay o PayPal) o per carta (500 dollari US per numero di carta di credito, compreso il codice PIN; 25 dollari US senza codice PIN, ma con tutti i dati necessari all'e-business). I *keylogger* sono disponibili a partire da 40 dollari US, i *cavalli di Troia* per un

---

[39] Uno studio della scena russa è reperibile in: http://www.verisign.com/static/042139.pdf (stato: 26.07.2007).

[40] Cfr: http://isc.sans.org/diary.html?storyid=3015; nonché http://www.theregister.co.uk/2007/07/06/pirate_mpack_toolkit/ (stato: 24.07.2007).

[41] Cfr. il colloquio dello sviluppatore denominato DCT su SecurityFocus: http://www.securityfocus.com/news/11476 (stato: 24.07.2007).

[42] Cfr. un'«intervista» con l'offerente «Corpse»: http://computersweden.idg.se/2.2683/1.93344 (stato: 24.07.2007).

[43] Cfr. in merito p.es.: http://asert.arbornetworks.com/2007/04/botconomics-the-monetization-of-your-digital-assets/; http://www.networkworld.com/news/2007/050907-fbi-organized-crime-cybercrime.html; http://www.theregister.co.uk/2007/06/13/black_hat_list/ nonché http://www.washingtonpost.com/wp-dyn/content/article/2007/03/13/AR2007031301522.html (stato: 24.07.2007).

prezzo che va da alcune centinaia a diverse migliaia di dollari US a seconda del tipo[44]. Tra gli offerenti esiste manifestamente una forte concorrenza[45].

Un numero sempre maggiore di fornitori di prestazioni di sicurezza tenta nel frattempo di istituire un mercato legale per le lacune di sicurezza e gli exploit, pagando di tasca propria oppure operando piattaforme di asta online[46]. È fortemente controverso come ne possano essere esclusi gli acquirenti dubbi e se questa misura sia in grado di arginare un mercato sotterraneo fiorente[47].

La scena della criminalità informatica è organizzata in maniera efficiente e secondo i principi della divisione del lavoro. Esistono compiti per tutti gli interessati, a seconda dello stato delle conoscenze e dell'energia criminale. In genere gli «esperti» sviluppano e vendono in proprio malware, exploit, toolkit ecc., mentre altre persone li utilizzano, ad esempio per gestire reti bot, effettuare furti di dati oppure attacchi di phishing o di spionaggio industriale. Anche per i dati derubati sono disponibili mercati sotterranei[48].

In altre parole gli «esperti» devono fornire un'energia criminale minore di quella degli acquirenti dei loro prodotti che, dal canto loro, non devono fruire di conoscenze esperte. Gli acquirenti commettono successivamente i furti di dati veri e propri e i furti di denaro e di identità che ne derivano oppure reclutano ulteriore personale a tale scopo.

Le cifre d'affari effettive della scena possono soltanto essere stimate – si tratta indubbiamente di un'attività lucrativa con rischi tuttora molto bassi[49].

5.3 Terrorismo

Londra: sventato un attacco dinamitardo contro i nodi Internet

Come reso noto da Scotland Yard nel mese di marzo, nel corso di perquisizioni a domicilio effettuate fin dal 2006 presso persone sospette di terrorismo sono stati trovati sui dischi rigidi

---

[44] Cifre di: http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/04/23/Cybercrime_2E002E002E00_-for-sale-_2800_I_2900_.aspx; http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/03/Cybercrime_2E002E002E00_-for-sale-_2800_II_2900_.aspx; http://www.heise.de/security/news/meldung/82679; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025464&intsrc=industry_list (stato: 24.07.2007).

[45] Cfr. p.es.: http://www.theregister.co.uk/2007/07/01/malware_gang_war/; http://www.viruslist.com/en/analysis?pubid=204791938#inet; http://www.darkreading.com/document.asp?doc_id=122116&WT.svl=news1_1 (stato: 24.07.2007).

[46] Cfr. p.es.: http://www.wslabi.com/wabisabilabi/initPublishedBid.do? (stato: 24.07.2007).

[47] Cfr. in merito: http://www.economist.com/science/displaystory.cfm?story_id=9507422; http://www.theregister.co.uk/2007/01/25/bug_brokers_offering_higher_bouties/; http://www.securityfocus.com/news/11468 nonché il rapporto di uno scienziato legittimo sulle sue esperienze nella vendita dei suoi risultati: http://weis2007.econinfosec.org/papers/29.pdf (stato: 24.07.2007).

[48] Cfr. p.es.: http://blog.washingtonpost.com/securityfix/2007/03/stolen_identities_two_dollars.html; http://www.itseccity.de/content/virenwarnung/statistiken/070327_vir_sta_symantec.html (stato: 25.07.2007).

[49] Cfr. in merito p.es.: http://www.vnunet.com/2189322, http://www.theregister.co.uk/2007/03/19/fbi_crime_report_2006/ nonché il rapporto dell'FBI Internet Crime Complaint Center con cifre relative agli USA: http://www.fbi.gov/page2/march07/ic3031607.htm (stato: 24.07.2007).

dei computer piani che inducevano a supporre un attacco terroristico contro l'importante nodo Internet «London Internet Exchange» (LINX)[50].

Secondo i piani le persone sospette si proponevano di introdursi nei quartieri generali della Telehouse Europe sui Telehouse Docklands, dove si situa fisicamente una parte cospicua di LINX, per pregiudicare l'Internet britannico con un attentato dinamitardo. Sebbene negli articoli riguardanti questo tema si affermasse che ciò avrebbe praticamente scollegato le isole britanniche da Internet, questa affermazione non corrisponde al vero: LINX gestisce due reti interamente separate le une dalle altre, ripartite geograficamente su sette diverse località, ragione per la quale l'avaria di un unico nodo non avrebbe avuto le drammatiche ripercussioni descritte. Ciò vale anche per le ripercussioni presso i Telehouse Docklands, benché si tratti del nodo più importante. In questa sede va inoltre constatato che i nodi Internet di queste dimensioni sono eccellentemente protetti dal profilo fisico, circostanza che dovrebbe rendere difficile un attentato dinamitardo[51]. Oltre ai piani di attentato al nodo Internet sono stati ritrovati piani di attentato alle condotte del gas, ai depositi di carburante e alle infrastrutture di comunicazione. I piani si trovavano comunque in uno stadio preliminare.

Il piano scoperto evidenzia che le cerchie terroristiche si preparano manifestamente sempre più ad attaccare le i*nfrastrutture critiche (nazionali)*. Come menzionato negli ultimi rapporti semestrali (soprattutto 2005/II), i terroristi non dispongono (per il momento) ancora del know-how necessario per poter perpetrare attacchi alle reti con le sole risorse delle tecnologie dell'informazione. Per questo motivo il proscenio è occupato da attacchi con risorse convenzionali (anche contro simili obiettivi).

Oltre a perseguire il numero massimo di vittime o un elevato carattere simbolico, sembra ora che la scelta degli obiettivi venga sempre più operata anche secondo i criteri del danno economico raggiungibile.

6 Prevenzione

6.1 Fulcro: infezioni drive-by

In materia di sicurezza dei computer il comportamento di ogni utente è decisivo. In questo contesto è pertanto ovvia una manipolazione prudente degli e-mail e del software scaricato. Tutti dovrebbero mostrarsi diffidenti, ad esempio in caso di ricezione tramite e-mail di fatture di imprese, soprattutto se non si è mai avuto a che fare con esse. L'obiettivo di questi e-mail è di incitare il destinatario ad aprire l'allegato, prima ancora di chiedersi se l'e-mail ha un senso. Di massima è meglio diffidare una volta di troppo che una volta di meno. Attualmente

[50] Cfr. in merito: http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece; http://www.technologyreview.com/blog/garfinkel/17561/ nonché http://www.daniweb.com/blogs/entry1345.html (stato: 25.07.2007).

[51] Cfr in merito: https://www.linx.net/pubtools/topology.html; http://en.wikipedia.org/wiki/London_Internet_Exchange; http://en.wikipedia.org/wiki/Telehouse (stato: 25.07.2007).

però, pur attenendosi alle norme usuali di comportamento, non si è al cento per cento al riparo dai danni[52].

Un motivo sempre più importante in merito si chiama *infezione drive-by*. Con questo termine si intende un'infezione da *malware* per il solo fatto di una visita a una pagina Web. Da lungo tempo ormai non corrisponde più al vero l'opinione diffusa secondo la quale simili infezioni sono possibili unicamente sulla pagine di offerenti dubbi, come ad esempio i siti pornografici o di gioco. Si espongono parimenti a un rischio gli utenti dei motori di ricerca – e quindi praticamente ognuno di noi. Da un esame per campionatura di pagine Web indicizzate da un motore di ricerca è risultato un numero di pagine con infezione drive-by pari a quasi il 10% (cfr. in merito anche il capitolo 2.2)[53]. Questa percentuale elevata è spiegata dal fatto che i criminali iniziano a captare interi server Web e inseriscono malware su tutte le pagine che vi sono ospitate (cfr. in merito il capitolo 5.1). Nella primavera di quest'anno una pagina Web consacrata al disco su ghiaccio è stata ad esempio vittima degli hacker che la hanno successivamente sfruttata per la diffusione di malware. Questo è successo proprio durante il fine settimana, al momento della finale del campionato del mondo di disco su ghiaccio. Ci si può facilmente rappresentare l'efficienza di questo metodo. Un ulteriore metodo di diffusione del malware sulle pagine Web è l'utilizzazione di cosiddetti typodomain. A tale scopo sono registrati domini la cui grafia è analoga a quella di pagine universalmente conosciute. Se si commette un errore di battitura alla chiamata della pagina Web si rischia di installare malware sul computer.

Come viene infettato il computer?

Attualmente i browser sono configurarti in modo tale che i file non siano scaricati e avviati automaticamente. È necessaria di volta in volta un'interazione dell'utente, con l'avvertimento dei pericoli vincolati al download. L'infezione drive-by funziona invece senza interazione dell'utente. Ciò è reso possibile dal fatto che praticamente ogni programma installato sul computer può essere affetto da *lacune di sicurezza*. Finché queste lacune non sono colmate – sia perché il produttore non ha ancora messo a disposizione un *patch*, sia perché l'utente non lo ha ancora installato – pagine o documenti predisposti all'uopo possono determinare un'infezione da malware. Il pericolo è particolarmente grande se le lacune di sicurezza concernono il browser Web o altri programmi che accedono a Internet. Si tratta ad esempio dei programmi *plugin* integrati nel browser come i movie-player (Flash, QuickTime, RealPlayer, Windows Media Player) o Adobe Reader. Se il programma corrispondente non è aggiornato si è esposti alla minaccia di un'infezione da malware se si naviga su una pagina Web appositamente predisposta.

Nel primo semestre del 2007 ha ad esempio fatto parlare di sé un malware diffuso da una cartolina di saluti. Gli e-mail contenevano un link su un *indirizzo IP*. Cliccando questo link si tentava di introdurre clandestinamente malware sul computer sfruttando le lacune di sicurezza del browser e senza intervento alcuno dell'utente. A tale scopo venivano provati sul browser diversi *exploit*. Se veniva individuato l'exploit idoneo si tentava nuovamente di indurre l'utente ad installare manualmente il malware.

La situazione è pure pericolosa quando gli exploit possono essere diffusi per il tramite di immagini. Se si introduce clandestinamente un file di immagine appositamente predisposto sul server di un'impresa specializzata nel collocamento di striscioni pubblicitari, anche pagine Web conosciute divengono diffusori di malware. Sono inoltre luoghi di predilezione per il

[52] Le norme di comportamento sono reperibili in: http://www.melani.admin.ch/themen/00166/00172/index.html?lang=it (stato: 20.08.2007).

[53] Cfr.: http://scmagazine.com/us/news/article/657903/google-450000-websites-launching-drive-by-attacks/ (stato: 20.08.2007).

collocamento di malware piattaforme Web 2.0 come YouTube o MySpace. Per visualizzare i filmati i visitatori di queste pagine utilizzano infatti i media player menzionati qui sopra e sovente affetti da lacune di sicurezza.

Misure

Una delle principali misure consiste nell'aggiornamento continuo del sistema operativo e di tutti i programmi che vi sono installati. Il lasso di tempo tra la pubblicazione del patch e la sua installazione è determinante. In considerazione della professionalità e della divisione del lavoro sulla scena della criminalità informatica trascorrono nel frattempo poche ore fino all'apparizione del primo exploit che sfrutta le lacune sicurezza rese note con il rilascio del patch. Sembra comunque che i criminali prediligano anche lacune di sicurezza più vecchie. Recentemente è stato diffuso per la prima volta un tool che esamina automaticamente se il sistema operativo e i programmi sono aggiornati[54]. In considerazione del numero degli *0-day-exploit* in circolazione anche un sistema interamente aggiornato non offre però una sicurezza al cento per cento.

Una possibilità di riduzione di una parte dei pericoli è costituita dalla disattivazione o perlomeno dalla limitazione di ActiveX in Internet Explorer o di Javascript negli altri browser. Molte pagine necessitano nondimeno di queste componenti. Sulle pagine di MELANI è pubblicata una guida sulle modalità di attivazione esclusiva di ActiveX per le pagine degne di fiducia[55].

Una maggiore attenzione e una certa consapevolezza dei pericoli da parte di ogni singolo utente di computer consente di evitare danni. Occorre diffidare se si constatano irregolarità. Rientrano ad esempio in questo ambito il crash del browser o l'apertura indesiderata di finestre all'atto della visita di una pagina. Se osserva un simile evento il collaboratore dovrebbe informare l'amministratore del computer in merito alla pagina in questione. Una comunicazione a MELANI può essere di ausilio perché allora la pagina viene analizzata e se del caso il provider ne viene informato, in modo da poter rimuovere il malware.

Un'ulteriore possibilità di riduzione dei pericoli di infezioni drive-by è la creazione di uno speciale conto di navigazione sul computer. Il conto di navigazione deve essere configurato in maniera tale da limitare nella misura del possibile i diritti (di amministratore) per impedire l'esecuzione automatica di malware. Se si lavora senza Internet si passa a un conto con diritti meno limitati.

Il pericolo di infezione drive-by è valutato nei capitoli 2.2 e 2.4; gli esempi in merito figurano nel capitolo 5.1.

[54] Cfr.: http://secunia.com/software_inspector (stato: 20.08.2007); attualmente è disponibile unicamente una versione beta.
[55] Cfr.: http://www.melani.admin.ch/themen/00166/00172/00176/index.html?lang=it (stato: 20.08.2007).

7 Attività / Informazioni

7.1 Stati

Svizzera: sarà proseguita l'attività di MELANI

Lo scorso 24 gennaio il Consiglio federale ha deciso di proseguire l'attività della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI. MELANI è operativa dal 1° ottobre 2004 e ha il compito di proteggere le *infrastrutture critiche* della Svizzera, in particolare laddove queste ultime dipendono dal funzionamento delle infrastrutture di informazione e di comunicazione.

Il Consiglio federale ha deciso in merito sulla scorta di una valutazione effettuata dal PF di Zurigo. I risultati della valutazione poggiano su inchieste condotte presso gli esercenti di infrastrutture critiche dell'economia svizzera, presso servizi paragonabili all'estero nonché presso i servizi della Confederazione. L'efficacia e l'opportunità delle attività di MELANI sono valutate in maniera estremamente positiva[56].

UE: collaborazione rafforzata nel settore della sicurezza interna

Nel corso del primo semestre del 2007 l'Unione europea ha ulteriormente promosso un rafforzamento della collaborazione nel settore della sicurezza interna. Sotto la presidenza germanica del Consiglio sono state potenziati le competenze operative di Europol e lo scambio di informazioni a livello di UE. Da un profilo concreto vanno menzionati i seguenti punti:

Il rafforzamento operativo di Europol è divenuto realtà con l'entrata in vigore del protocollo di modifica della convenzione Europol. In futuro gli agenti di Europol potranno partecipare a gruppi comuni di indagine degli Stati membri. Per migliorare lo scambio di informazioni tra Europol e gli Stati membri, ulteriori autorità degli Stati membri – oltre alle attuali agenzie centrali nazionali – avranno un accesso diretto al sistema di informazione di Europol. Inoltre esperti di Paesi terzi potranno collaborare direttamente a Europol nel quadro di un gruppo di analisi degli Stati membri. L'ultimo punto è soprattutto rilevante in vista della collaborazione tra UE e USA nel settore della lotta al terrorismo. L'ulteriore progetto di trasposizione della convenzione Europol nel corpo legislativo dell'UE è destinato a estendere il settore di compiti di Europol a tutte le forme di grave criminalità transfrontaliera[57].

Europol deve svolgere un ruolo centrale nella sorveglianza di Internet. Le osservazioni e le analisi effettuate dagli Stati membri in ambito di attività terroristiche su Internet dovranno confluire attraverso un portale di informazione ospitato presso Europol. Questo progetto di

[56] Cfr.: http://www.isb.admin.ch/aktuell/medieninfo/00126/index.html?lang=it&msg-id=10361 (stato: 10.8.07).
[57] Cfr.: http://www.bmi.bund.de/cln_012/nn_175818/Internet/Content/Nachrichten/Pressemitteilungen/2007/04/JI__Rat__Europol__DE.html; http://www.heise.de/newsticker/meldung/88599 (stato: 10.8.07).

sorveglianza, denominato «Check the Web», è stato posto in esercizio all'inizio del mese di maggio. Nell'ambito di «Check the Web» saranno inoltre indetti incontri regolari tra esperti[58].

In vista di un migliore coordinamento delle misure di lotta contro la criminalità su Internet la Commissione europea auspicherebbe sviluppare un quadro politico coerente dell'UE. Nel mese di maggio la Commissione ha adottato in merito la comunicazione «Una politica generale di lotta alla criminalità su Internet». La comunicazione ribadisce tra l'altro la necessità di un rafforzamento del dialogo tra il settore pubblico e l'economia privata[59].

USA: lacuna significativa della sicurezza IT presso il Department of Homeland Security (DHS), mentre l'esercito cerca di controllare il cyberspazio

Il Department of Homeland Security (DHS) degli USA è tra l'altro responsabile della sicurezza informatica. È soltanto nel mese di settembre del 2006 che il DHS ha designato un responsabile con il compito di meglio proteggere gli USA dagli attacchi informatici[60]. Il DHS è tuttora oggetto di critiche per le carenze delle sue proprie misure di sicurezza e per le lacune nei controlli di sicurezza. Lo scorso mese di giugno il Government Accountability Office (GAO), l'autorità statunitense di vigilanza, ha nuovamente criticato in un suo rapporto alla Camera dei rappresentanti la sicurezza dell'informazione del DHS. Il GAO constata che si sono verificati progressi ma che sussistono «punti deboli significativi» che minacciano la confidenzialità, l'integrità e la disponibilità delle informazioni e dei sistemi di informazione del DHS[61].

Simultaneamente viene presa sul serio l'importanza militare dello spazio informatico negli USA. Ciò è tra l'altro evidenziato dalla creazione di una nuova unità spazio informatico da parte dell'US Air Force. Il cosiddetto «Cyber Command» si prefigge di controllare lo spazio informatico e di migliorare le capacità di condotta della guerra nello spazio informatico. Il tutto poggia sulla convinzione che lo spazio informatico e la superiorità dell'informazione costituiscono le premesse di operazioni efficaci in tutti gli ambiti di condotta della guerra[62].

Diversi altri Stati hanno parimenti creato capacità militari nel settore informatico. In particolare gli sforzi di armamento della Cina nello spazio informatico offrono agli USA una motivazione concreta a garantire la superiorità americana anche in questo settore [63].

Si veda il capitolo 5.1 per una valutazione delle questioni giuridiche che suscitano gli attacchi con risorse informatiche nonché per informazioni sull'attacco informatico all'Estonia dell'aprile 2006.

---

[58] http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2007/05/Check__the__web.html; http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=it (capitolo 7.1) (stato: 10.8.07).

[59] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF (stato: 10.8.07).

[60] Cfr. rapporto semestrale 2006/2, capitolo 7: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=de (stato: 10.08.2007).

[61] Cfr.:http://www.gao.gov/new.items/d071003t.pdf; http://homeland.house.gov/hearings/index.asp?ID=65 (stato: 10.8.07).

[62] Cfr.: www.af.mil; http://www.heise.de/newsticker/meldung/91131 (stato: 10.8.07).

[63] Cfr. in merito la valutazione della potenza militare cinese da parte del Ministero statunitense della difesa: http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf (stato: 10.08.2007).

7.2 Economia privata

Svizzera: i provider bloccano l'accesso a pagine di pornografia infantile

Nell'ambito di un progetto comune della Prevenzione svizzera della criminalità (PSC), di ECPAT Switzerland della Protezione svizzera dell'infanzia e del Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) i provider svizzeri di Internet sono stati invitati a bloccare volontariamente le pagine Web commerciali di pornografia infantile. Nel frattempo una parte cospicua dei provider svizzeri di Internet si è dichiarata disposta a partecipare al progetto e alcuni bloccaggi sono già attivi. L'obiettivo è di rendere difficile l'accesso alla pornografia infantile e di scoraggiare i consumatori di pornografia infantile tramite un intervento manifesto.

La campagna di bloccaggio è diretta contro gli offerenti commerciali di pornografia infantile all'estero. L'elenco delle pagine Web da bloccare è stabilito dall'Ufficio federale di polizia e costantemente completato. Gli indirizzi delle pertinenti pagine Web sono inseriti in un filtro. In caso di chiamata di una di queste pagine, l'utente di Internet è dirottato su una pagina di avvertimento. Una parte degli indirizzi di pornografia infantile è stata ripresa dalle autorità scandinave, dopo essere stata sottoposta un esame giuridico; tali autorità operano con filtri di bloccaggio analoghi. Gli altri indirizzi provengono dalle indagini dello SCOCI.

Anche nel 2007 la pornografia infantile costituisce il motivo più frequente di comunicazione al Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI). La campagna di bloccaggio è destinata a fornire un importante contributo all'arginamento della domanda nel settore della pornografia infantile e quindi alla protezione di nuove vittime potenziali.

8 Basi legali

Nuova legislazione anti-spam in Svizzera

Dal 1° aprile 2007 lo *spam* è di massima vietato in Svizzera. Gli invii di massa effettuati mediante telecomunicazione sono autorizzati unicamente a determinate condizioni. Secondo la legge federale contro la concorrenza sleale la pubblicità di massa che non ha relazione diretta con un contenuto richiesto dal destinatario deve di massima adempiere le tre seguenti condizioni:

1. la pubblicità di massa deve essere inviata dopo che il destinatario ha dato il proprio consenso (modello opt-in);

2. deve menzionare direttamente il mittente; e

3. deve indicare la possibilità di opporvisi in modo agevole e gratuito.

L'unica eccezione alla disposizione opt-in è l'indicazione dell'indirizzo fornito nel caso di acquisto, a condizione che sia menzionata la possibilità di opporvisi. Il venditore può

utilizzare questo indirizzo per la propria pubblicità. Se la pubblicità di massa inviata mediante telecomunicazione non adempie questi criteri si è allora in presenza di spam e quindi di concorrenza sleale.

Se dall'identificazione dell'indirizzo (*indirizzo IP*) risulta che si tratta di un offerente svizzero di servizi di telecomunicazione gli si può comunicare l'invio di spam. Gli offerenti di servizi di telecomunicazione hanno l'obbligo di istituire un servizio di comunicazione e – posto che ne abbiano conoscenza – di impedire che i loro clienti inviino o inoltrino spam.

Lo spam è punibile se è inviato intenzionalmente. La fattispecie dell'intenzionalità presuppone che lo spam sia deliberato. Se nel caso dello spam si tratta di pubblicità sleale di massa con riferimento alla Svizzera, inviata intenzionalmente, sussiste la possibilità di sporgere querela contro l'impresa che fa pubblicità o contro il mittente. Occorre comunque ponderare se un eventuale procedimento penale è proporzionato al danno subito. Lo spam è un reato punito su querela il cui perseguimento penale compete ai Cantoni.

Nell'intento di analizzare in maniera semplice l'origine di uno spam il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) ha allestito un formulario di analisi degli spam[64]. Per il suo tramite ognuno può scoprire se lo spam è stato inviato o inoltrato dalla Svizzera e, nell'ipotesi affermativa, tramite quale offerente di servizi di telecomunicazione (provider di Internet). Per analizzare lo spam è necessaria l'intestazione dell'e-mail di spam. Presso il medesimo servizio è altresì ottenibile una guida precisa sulle modalità di lettura delle intestazioni.

La nuova legislazione non si applica però agli spam inviati in Svizzera dall'estero. Poiché la maggior parte degli e-mail di spam proviene dall'estero non si dovrebbe assistere a grandi cambiamenti nelle caselle postali elettroniche degli Svizzeri[65].

Perquisizioni online in Germania

Internet viene sempre più utilizzato come mezzo di comunicazione. Quindi anche da criminali e da persone che possono minacciare la sicurezza dello Stato. Sia in Svizzera che nel resto dell'Europa sono in corso vivaci dibattiti su questo tema e sui limiti della sorveglianza di Internet e dei computer da parte dello Stato. In merito occorre distinguere se si tratta di un'inchiesta senza sospetto concreto oppure di una sorveglianza effettuata nel quadro di un perseguimento penale.

La Corte federale germanica (Bundesgerichtshof, BGH) di Karlsruhe ha deciso lo scorso 5 febbraio 2007 che le perquisizioni furtive online da parte della polizia sono illecite perché non esiste una chiara base legale. La Corte ha dichiarato che la procedura penale non legittima questo metodo di ricerca. Le perquisizioni online non possono essere fondate sulle disposizioni relative alle perquisizioni a domicilio né tantomeno essere paragonate ad altre misure di inchiesta come la sorveglianza telefonica o quella degli spazi abitativi. Il Ministero federale dell'interno ha annunciato di voler elaborare un adeguamento delle basi legali attuali. Il Ministero punta su metodi elettronici di ricerca nel contesto della lotta contro il terrorismo. Il controllo di Internet e dei sistemi di computer è considerato necessario perché il terrorismo utilizza sempre più questi moderni mezzi di comunicazione.

[64] Cfr.: http://www.cybercrime.ch/spamanalyse/spam_it.php#spam (stato: 20.08.2007).

[65] http://www.bakom.admin.ch/dienstleistungen/info/00542/00886/index.html?lang=it (stato: 20.08.2007).

Nel quadro delle procedure di inchiesta le autorità germaniche di polizia sfruttano già da lungo tempo, a livello nazionale, la possibilità di procacciarsi informazioni insinuandosi nei sistemi di computer.

In Svizzera le perquisizione online di sistemi di computer non sono per il momento autorizzate senza un sospetto concreto. Il nuovo disegno di legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI) prevede nondimeno l'insinuazione nei computer a severe condizioni. Alle Camere sono imminenti i dibattiti in merito a questo disegno di legge. L'impiego di software di spionaggio nel quadro del perseguimento penale può però essere autorizzato. La legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) de diversi codici di procedura penale possono servire da base legale.

Una valutazione dell'utilizzazione di Internet da parte dei terroristi figura in più rapporti semestrali precedenti di MELANI (edizioni 2006/2, 2006/1 e soprattutto 2005/2, ogni volta il capitolo 5.4).

9 Statistica

Saturazione degli accessi Internet in Svizzera

L'Ufficio federale di statistica ha pubblicato nel corso del primo semestre del 2007 uno studio sull'utilizzazione di Internet da parte delle economie domestiche svizzere. I risultati del rilevamento effettuato nel 2004 evidenziano che il 71% circa delle economie domestiche svizzere hanno un computer. Il 61% di esse ha accesso a Internet. La Svizzera si situa al quinto posto della graduatoria internazionale. Secondo lo studio in questione l'accesso a Internet da casa propria è in ulteriore aumento, seppure a un ritmo meno elevato di quello degli anni Novanta o dell'inizio del 21° secolo. Un quinto delle economie domestiche svizzere non desidera alcun accesso a Internet o non ne vede l'utilità. Per questo motivo nei prossimi tempi ci si deve aspettare una saturazione dei nuovi collegamenti. Ulteriori motivi di mancata utilizzazione di un accesso Internet da casa propria sono l'assenza di precise competenze, i costi e la possibilità di un accesso alternativo a Internet[66].

Il timore dei problemi che suscitano la sicurezza dei dati e la protezione della sfera privata svolgono soltanto un ruolo minore nella decisione di un accesso Internet a casa propria, perché ognuno di questi argomenti è adotto da meno dell'1% delle economie domestiche.

Le ditte svizzere sono praticamente collegate in rete sull'intero territorio nazionale

L'informatica e Internet svolgono un ruolo sempre più importante per le imprese svizzere. In particolare le piccole e medie imprese (PMI) fanno viepiù capo a prestazioni online

[66] http://www.bfs.admin.ch/bfs/portal/fr/index/themen/16/22/publ.Document.87095.pdf (stato: 20.08.2007).

qualificate, mentre le grandi imprese presentano un elevato livello di collegamento in rete. Le offerte elettroniche delle autorità maggiormente conosciute dalle imprese sono quelle dei Cantoni, come risulta da uno studio rappresentativo dell'istituto di ricerca gfs.bern. Tra il 5 il 25 febbraio 2007 sono state interrogate complessivamente 1050 imprese su mandato del Segretariato di Stato dell'economia SECO e della Cancelleria federale[67].

Il 91 percento delle imprese interrogate con più di 10 collaboratori dispongono di un accesso a Internet direttamente sul posto di lavoro. Nelle imprese con meno di 10 collaboratori il 63% di essi lavora quotidianamente con Internet, mentre nelle grandi imprese tale percentuale raggiunge il 71% dei collaboratori. Il 72% delle imprese considera molto o piuttosto importante un conto e-mail per tutti i collaboratori; il 76% considera molto o piuttosto importanti i servizi mobili come i telefoni mobili, i telefoni cellulari e le agende elettroniche (PDA).

La protezione delle infrastrutture di informazione non va più trascurata nemmeno da parte delle PMI e assume sempre maggiore importanza. MELANI ha commissionato uno studio che illustra la sicurezza dell'informazione nelle imprese svizzere. L'esistenza delle imprese può già essere minacciata da un crash di più giorni delle risorse informatiche[68].

[67] http://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=it&msg-id=12087 (stato: 20.08.2007).
[68] http://www.melani.admin.ch/dokumentation/00123/00125/index.html?lang=it (stato: 20.08.2007).

10 Glossario

Il presente glossario contiene tutti i termini indicati in *italico*. Un glossario più completo lo si può trovare all'indirizzo :
http://www.melani.admin.ch/glossar/index.html?lang=it.

0-day-exploit	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
Attacco DoS	Attacco Denial-of-Service Ha lo scopo di rendere irraggiungibile un determinato servizio all'utente o perlomeno di ostacolare notevolmente la raggiungibilità di detto servizio.
Attacco DDoS	Attacco Distributed-Denial-of-Service Un *attacco DoS* in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Autentificazione a due fattori	A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. passwort, PIN ecc.); 2. una cosa che si ha (ad es. certificato, *token*, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.).
Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
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.
Codice Exploit	(abbrev.: Exploit) Un programma, uno script o una riga di codice per il tramite dei quali è possibile sfruttare le lacune dei sistemi di computer.
Defacement	Deturpamento di pagine web
DNS	Domain Name System Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
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 e*xploit* che sfruttano le *lacune nel sistema di sicurezza* lasciate scoperte dal

	visitatore.
Infrastrutture critiche (nazionale)	Infrastruttura o parte dell'economia la cui avaria o il cui danneggiamento ha ripercussioni massicce sulla sicurezza nazionale o sul benessere sociale e/o economico di una nazione. In Svizzera sono definite critiche le seguenti infrastrutture: approvvigionamento energetico e idrico, servizi d'emergenza e di salvataggio, telecomunicazione, trasporti e traffico, banche e assicurazioni, governo e pubbliche amministrazioni. Nell'era dell'informazione il loro funzionamento dipende sempre più dai sistemi di informazione e di comunicazione. Tale sistemi sono detti infrastrutture critiche di informazione.
IP Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
Keylogger	Apparecchi o programmi intercalati tra il computer e la tastiera per registrare i dati immessi sulla tastiera.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Malware	Termine composto dalle parole inglesi «Malicious» e "Software". Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i *virus*, *vermi informatici*, *cavalli di Toia*.
Man-in-the-Middle (MITM)	Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in grado di seguire o di modificare lo scambio di dati.
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza. Vedi anche Hotfix.
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.
Plugin	Un software di complemento che amplia le funzioni di base di un'applicazione. Esempio: i Plug-In di Acrobat per i browser di Internet consentono la visualizzazione diretta di file PDF.
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.
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.
Token	Componente hardware che genera un fattore di autenticazione (vedi *Autenticazione a due fattori*) (ad es. SmartCard, token USB, SecureID ecc.).