Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

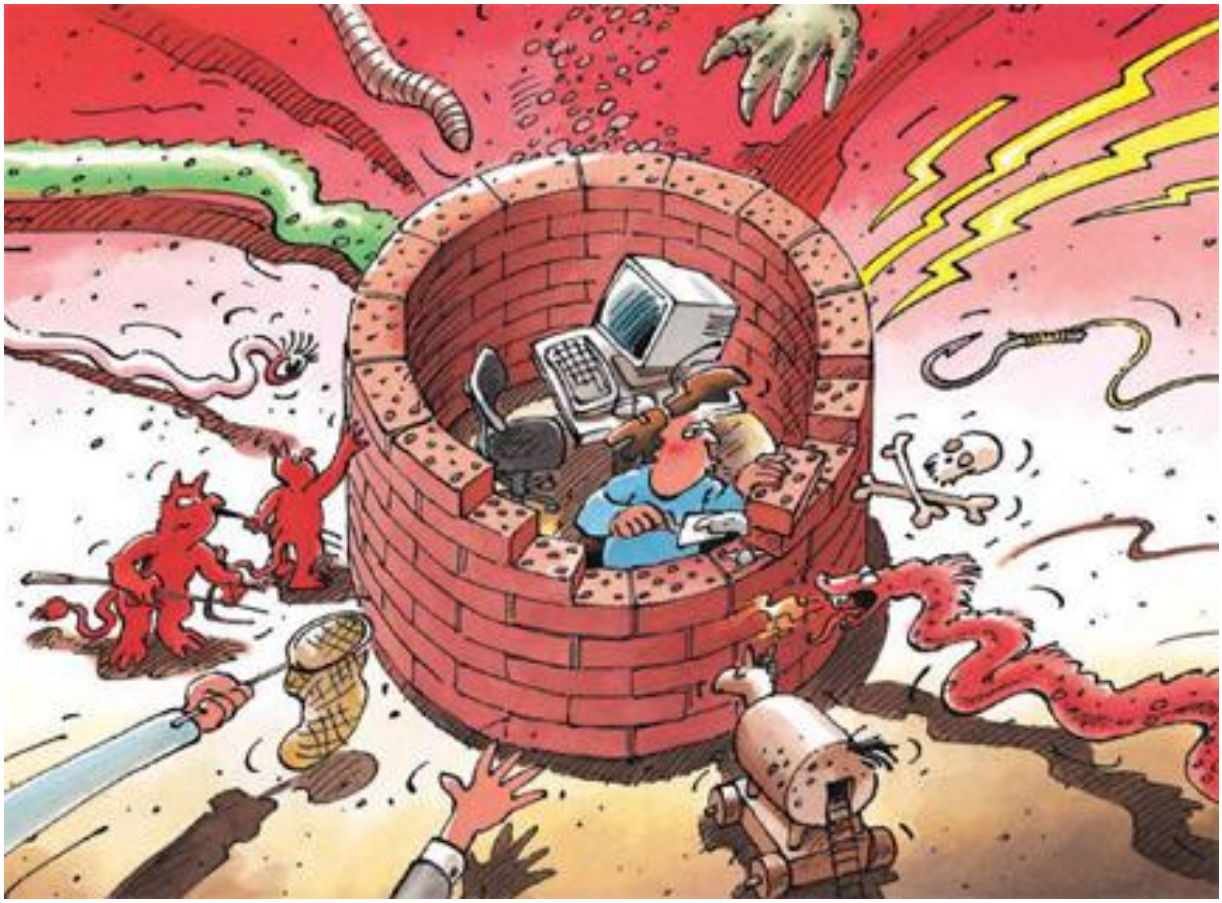
Organo strategia informatica della Confederazione OSIC
Ufficio federale di polizia fedpol

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

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2006/II (luglio – dicembre)



In collaborazione con:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Indice

Fulcri dell'edizione 2006/II

- **Social Engineering**
  Gli attacchi di *social engineering* sfruttano la disponibilità all'aiuto, la buona fede o l'incertezza delle persone. Essi rappresentano il tipo di attacco più diffuso contro le imprese e gli utenti privati. Ci si deve aspettare che con l'aumento della sicurezza (tecnica) dei sistemi operativi e delle applicazioni gli attacchi di social engineering acquistino ulteriore importanza e che divengano ancor più professionali.
  ► Situazione attuale: capitolo 2.1
  ► Tendenze per il prossimo semestre: capitolo 3.1 e 3.2
  ► Esempi / incidenti: Svizzera capitolo 4.1; a livello internazionale capitolo 5.2 e 5.3
  ► Prevenzione: capitolo 6

- **Spam**
  Nel corso della seconda metà del 2006 lo spam ha registrato un notevole incremento. Nuove tecniche, in particolare l'invio di messaggi spam sotto forma di immagini e non di testo, consentono di eludere i filtri spam, nonostante il loro miglioramento. Sono particolarmente diffusi anche i cosiddetti «Stock Pump and Dump Spams» che consigliano l'acquisto di determinate azioni.
  ► Situazione attuale: capitolo 2.2
  ► Esempi / incidenti: capitolo 5.2 e 5.3

- **Furto di dati e di identità**
  Nel corso della seconda metà del 2006 il *phishing* e il *furto di dati o di identità* con l'ausilio di *malware* hanno registrato un forte aumento. Sono stati derubati dati con i quali è possibile procacciarsi denaro, come ad esempio quelli sfruttati abusivamente per effettuare transazioni illegali di e-banking. Ci si deve aspettare che nel 2007 anche gli istituti finanziari che utilizzano l'*autentificazione a due fattori* si troveranno sempre più nel mirino degli aggressori.
  ► Situazione attuale: capitolo 2.3
  ► Tendenze per il prossimo semestre: capitolo 3.1 e 3.2
  ► Esempi / incidenti: Svizzera capitolo 4.1; a livello internazionale capitolo 5.2 e 5.3

- **Malware / vettori di attacco**
  L'aumento di *malware* appositamente predisposto e la diminuzione contemporanea dell'apparizione su vasta scala di malware (ad es. sotto forma di *vermi informatici*) è proseguito anche nel secondo semestre del 2006. Il miglioramento della sicurezza dei sistemi operativi ha provocato un accresciuto sfruttamento delle lacune di sicurezza delle applicazioni sul fronte del cliente, come ad esempio a livello di software di sicurezza, di plug-in, di driver per hardware o di prodotti MS Office. Le quote di rilevamento sono in continuo peggioramento. Hanno parimenti acquistato importanza le infezioni successive a visite di pagine Web appositamente predisposte.
  ► Situazione attuale: capitolo 2.4
  ► Tendenze per il prossimo semestre: capitolo 3.1 e 3.2
  ► Esempi / incidenti: Svizzera capitolo 4.1; a livello internazionale capitolo 5.2 e 5.3
  ► Prevenzione: capitolo 6 (il social engineering è la principale via di infezione da malware)

1 Introduzione

Il quarto rapporto semestrale (luglio – dicembre 2006) 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), presenta un compendio degli avvenimenti in Svizzera e all'estero, illustra i principali sviluppi 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 ora più facilmente reperibili perché figurano in sezioni graficamente 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. Con esempi scelti sono illustrati i principali avvenimenti degli ultimi sei mesi del 2006. 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 un punto centrale della prevenzione.

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.

2 Situazione attuale, pericoli e rischi

2.1 Social engineering

Gli attacchi di *social engineering* sfruttano la disponibilità all'aiuto, la buona fede o l'incertezza delle persone per accedere a dati confidenziali o per indurre le vittime a eseguire determinate azioni.

Un esempio di attacco di social engineering nei confronti delle persone private è il cosiddetto *phishing*, nel cui ambito le vittime sono solitamente sollecitate tramite e-mail a rivelare i loro dati di accesso all'e-banking. Con l'ausilio dei metodi di social engineering viene inoltre diffusa una grande parte del *malware*. Il più sovente tale diffusione è operata tramite e-mail contenenti allegati infettati oppure cliccando sui link inseriti nell'e-mail.

Nel settore delle imprese il social engineering viene per lo più sfruttato a scopi di spionaggio economico. Anche nel corso del secondo semestre le vulnerabilità fino ad allora ignote dei prodotti MS Office sono state sfruttate per introdurre clandestinamente malware nei calcolatori delle imprese. Nel mirino degli aggressori si trovano solitamente detentori potenziali di conoscenze del cui ruolo nell'impresa e dei cui interessi personali si è venuti a conoscenza in precedenza. Grazie a queste conoscenze è possibile sferrare attacchi particolarmente efficaci di social engineering, inducendo ad esempio le vittime ad aprire i dati infettati (*Spear-Phishing*). Gli attacchi di social engineering tramite Internet non costituiscono il solo problema delle imprese. A titolo di esempio è anche possibile accedere agli edifici e agli uffici per visionare dati sensibili, penetrandovi con una stampante sotto il braccio e simulando una falsa identità.

MELANI ritiene che il social engineering acquisterà ulteriore importanza perché i sistemi operativi cliente più recenti applicano meccanismi di protezione sempre migliori. Grazie a queste misure anche le lacune ancora ignote non possono più essere facilmente sfruttate. Per corrispondenza vengono a sparire numerosi *vettori di attacco* sperimentati e nel migliore dei casi il malware penetra nel sistema soltanto se si effettua un doppio clic su file eseguibili. Questa tendenza dovrebbe rafforzarsi nel corso dei prossimi due o tre anni.

Il capitolo 5.2 elenca esempi di attacchi social engineering, mentre il capitolo 6 presenta raccomandazioni sulle modalità di prevenzione contro gli attacchi di social engineering.

2.2 Spam

Gli e-mail di *spam* hanno registrato un forte aumento nel corso del secondo semestre. Secondo diversi studi a fine 2006 lo spam rappresentava tra l'80% e il 90% dell'intero traffico e-mail[1].

[1] Cfr. in merito:
http://www.postini.com/news_events/pr/pr110606.php; http://www.postini.com/news_events/pr/pr120606.php; http://www.barracudanetworks.com/ns/news_and_events/news.php?nid=238; http://www.f-secure.de/f-secure/pressroom/news/fs_news_20070111_1_deu.html (stato: 5.02.2007).

È aumentata in particolare la quota dei cosiddetti «Image-Spams». I messaggi «Image-Spam» contengono parole casuali, la cui combinazione è priva di senso, nonché un'immagine come file allegato (attachment). L'informazione vera e propria del messaggio di spam si trova nell'immagine. Prima dell'invio le immagini sono modificate a livello di margini da calcolatori situati su *reti bot* (ad esempio la loro altezza o larghezza) in modo tale che anche i filtri spam che ricercano immagini conosciute non sono più in grado di riconoscerle. La maggior parte dei messaggi spam è ulteriormente inviata avvalendosi delle reti bot. Questa circostanza ne rende più difficile il filtraggio perché i mittenti modificano continuamente gli *indirizzi IP*. Gli spammer riescono così a eludere sempre più i meccanismi di protezione contro lo spam, peraltro migliorati nel corso degli ultimi anni.

Un trucco particolarmente diffuso è quello degli «Stock Pump and Dump Spams»: i messaggi spam reclamizzano l'acquisto di azioni. Prima dell'invio dello spam, gli spammer acquistano azioni delle pertinenti imprese; durante l'ondata di spam queste azioni realizzano in parte notevoli incrementi di valore, per poi ricadere successivamente sui loro valori iniziali. Nel frattempo lo spammer ha venduto la sua quota e incassato la differenza di prezzo, mentre gli altri acquirenti di azioni devono sopportare la perdita di valore[2].

Nel 2006 lo spam non è solo aumentato in cifre ma, consecutivamente all'invio di immagini, ha sollecitato maggiori risorse dell'infrastruttura Internet. Se recentemente se ne poteva ancora prospettare un calo grazie al miglioramento dei filtri, si teme ora che lo spam permarrà anche in futuro un problema per l'infrastruttura Internet e per la produttività degli utenti dell'e-mail.

2.3 Furto di dati e di identità

Il *phishing* e il *furto di dati o di identità* tramite *malware* hanno raggiunto un nuovo punto culminante nel secondo semestre del 2006. Tra i mesi di settembre e di ottobre l'«Anti-Phishing Working Group» ha registrato un aumento del numero di pagine Web di phishing di quasi oltre il 52%. Si presume che questa circostanza sia riconducibile alla maggiore disponibilità di kit di phishing che consente anche ai phisher meno versati tecnicamente di allestire pagine di phishing. Nel contempo si è assistito a un aumento del malware che registra le digitazioni sulla tastiera o esegue in maniere diverse furti di dati a scopi finanziari (cfr. anche i capitoli 2.4 e 3.1)[3].

Alcuni tipi di malware di questo genere scandagliano l'intero computer o reti condivise alla ricerca di informazioni sfruttabili a scopi finanziari, mentre altri registrano tutte le digitazioni sulla tastiera non appena si naviga su una pagina Web che interessa l'aggressore (ad es. sito Web di una banca). Nel caso dei siti Web delle banche i dati derubati possono ad esempio essere sfruttati per effettuare transazioni illegali – una tecnica che viene a completare il phishing (ossia l'invio di e-mail per indurre a rivelare i dati di login).

---

[2] Secondo uno studio negli USA l'utile per gli spammer ammonta di volta in volta a quasi il 6%: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920553. Cfr. anche: http://www.securityfocus.com/print/news/11435 (stato: 5.2.2007).

[3] Cfr. http://www.antiphishing.org; http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html (stato: 6.2.2007).

Un'altra forma di furto di identità è operata con malware che manipola il browser in modo tale da falsificare direttamente durante la sessione di e-banking ciò che il browser rappresenta – in questo senso la vittima non si accorge neppure che viene effettuato un pagamento diverso dal proprio pagamento.

Nel mese di luglio si è inoltre assistito negli USA a un efficace attacco *Man-in-the-Middle* contro un istituto finanziario, attacco grazie al quale è stato possible eludere la cosiddetta *autentificazione a due fattori* (cfr. in merito anche i capitoli 3.1 e 5.3).

Le vittime del furto di dati e di identità sono soprattutto utenti privati, ma anche imprese. Anche chi ritiene di non aver memorizzato alcun documento importante nel proprio computer dispone comunque di documenti che possono interessare gli aggressori. Essi prendono di mira tutti i tipi di dati che possono essere trasformati in denaro. Si può trattare di password, di dati per sfruttare l'identità di persone private, di segreti aziendali, di dati relativi alle carte di credito, di informazioni relative ai conti, di dati di login a giochi online, di chiavi di licenza di software ecc.

Gli attacchi sono effettuati tramite malware che i software antivirus sono sempre meno in grado di individuare in maniera affidabile (cfr. capitolo 2.4). Ne sono colpiti i calcolatori aziendali, i computer di utenti privati, ma anche i server Web sui quali girano le applicazioni di e-commerce e tramite i quali l'aggressore potrebbe mettere le mani su preziosi dati relativi alle carte di credito[4].

Come in precedenza attacchi estremamente mirati di spionaggio economico contro imprese ed esercenti di *infrastrutture nazionali critiche* – anche in Svizzera – sono sferrati a partire dall'area asiatica (cfr. anche il capitolo 5.2, nonché l'ultimo Rapporto semestrale, capitolo 2.2).

Il capitolo 3.1 presenta una valutazione dell'ulteriore evoluzione di questo pericolo, mentre i capitoli 4.1, 4.2, 5.2 e 5.3 contengono degli esempi.

2.4 Malware / Vettori di attacco

Anche nel corso del secondo semestre sono proseguiti l'aumento del *malware* utilizzato in maniera mirata, ad esempio sotto forma di *cavalli di Troia*, e la diminuzione contemporanea dell'apparizione ampia e facilmente sfruttabile di malware sotto forma di *vermi informatici*. Il miglioramento delle misure di protezione dei sistemi operativi ha provocato un accresciuto sfruttamento delle *lacune di sicurezza* delle applicazioni sul fronte del cliente per installare malware. L'aspetto piccante è che rientrano in questo ambito software di sicurezza (software antivirus, *firewall* ecc.), driver per hardware (ad es. per le carte *WLAN*), prodotti MS Office, ma anche plug-in, come ad esempio il Flash Player o il Reader di Adobe. Si sfruttano in mi-

[4] Cfr. anche:
http://www.net-security.org/dl/articles/Report-DOJ_Computer_Crime_Prosecutions.pdf;
http://www.computerworld.cz/cw.nsf/id/CDC9ECF819BAAACCC125726A0069222E/$File/McAfee_wp_id_theft_de.pdf; http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html; http://www.fightidentitytheft.com;
http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html (stato: 06.02.2007).

sura crescente le lacune di sicurezza delle applicazioni Web, che gli aggressori riprendono e spiano successivamente oppure sfruttano abusivamente per la diffusione di malware[5].

Hanno acquistato ulteriore importanza anche le infezioni consecutive alla semplice navigazione in Internet. La visita casuale a una pagina Web appositamente predisposta oppure la visita consecutiva all'apertura di un link contenuto in un messaggio di e-mail o di Instant Messaging infetta il computer (cosiddette «infezioni drive-by»). Rientrano viepiù in questo ambito anche le pagine Web di offerenti seri, in particolare le pagine di «Social Networking» che mettono a disposizione contenuti generati dagli utenti[6]. Nella maggior parte dei casi i computer infettati sono successivamente aggregati a una *rete bot*.

L'obiettivo degli sviluppatori di malware è di impedire possibilmente a lungo l'individuazione del malware. La quota di rilevamento dei programmi di sicurezza basati sulle firme diminuisce in maniera corrispondente, con la conseguenza che con il passare del tempo questi programmi offrono sempre meno protezione contro i pericoli attuali.

Nel contempo i vettori di attacco si spostano su Internet: sono in aumento le infezioni «drive-by» dovute a pagine Web (come ad es. pagine Internet di «Social Networking» o pagine Internet oggetto di hacking). La navigazione avventata in Internet costituisce pertanto uno dei maggiori pericoli che le imprese, in particolare, devono prendere seriamente in considerazione.

Gli esempi sono reperibili nei capitoli 5.2 e 5.3.

3 Tendenze / evoluzioni generali

3.1 Minacce per il settore finanziario

Un numero sempre maggiore di istituti finanziari degli USA e di altri Paesi rafforzano la loro sicurezza in ambito di e-banking e introducono l'*autentificazione a due fattori*. Quanto più la sicurezza aumenta tramite misure tecniche, tanto maggiore è la probabilità di nuovi tipi di attacchi contro i sistemi di autentificazione nell'e-banking. Nel mercato underground ha già fatto la sua apparizione un toolkit grazie al quale anche gli aggressori meno esperti possono implementare gli attacchi *Man-in-the-Middle* a scopi di *phishing*.

Nel 2007 ci si aspetta un aumento dei rari attacchi Man-in-the-Middle osservati finora contro i sistemi di autentificazione nell'e-banking e una loro utilizzazione anche contro le banche svizzere (cfr. l'esempio in provenienza dagli USA al capitolo 5.3).

Si assisterà ulteriormente al *phishing* in senso classico (ossia l'invio di e-mail che sollecitano l'indicazione dei dati di login). La tendenza in ambito di transazioni finanziarie illecite nell'e-banking – transazioni per il cui tramite sono depredati i conti bancari – va in direzione di un

[5] Cfr. http://www.theregister.co.uk/2006/09/18/web_vulnerabilities/; http://cve.mitre.org; http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html (stato: 7.2.07).

[6] Cfr. http://www.aladdin.com/news/2006/eSafe/mySpace.asp (stato: 7.2.07).

malware sul fronte del cliente (che deruba i dati di login all'insaputa delle vittime) e di attacchi in tempo reale (come ad esempio gli attacchi Man-in-the-Middle).

La situazione attuale è valutata al capitolo 2.3, mentre gli esempi figurano ai capitoli 4.1, 4.2, 5.2 e 5.3.

3.2 Il mercato della criminalità informatica si è affermato: fase di consolidamento

Il mercato della criminalità informatica si è affermato: è possibile guadagnare denaro mediante l'invio di *spam*, la locazione di *reti bot*, lo sviluppo di *malware*, la ricerca di *lacune di sicurezza*, l'allestimento di perizie in ambito di riciclaggio di denaro e altre attività. Esiste in particolare un mercato lucrativo dei dati derubati (cfr. per gli esempi il capitolo 5.3).

Anche la criminalità organizzata ha scoperto che in uno spazio virtuale può svolgere le sue attività con minori rischi – in particolare le truffe, i furti e le estorsioni.

La criminalità informatica è un'attività proficua con rischi relativamente piccoli. Invece di rubare una grossa somma a una sola vittima, i criminali informatici rubano relativamente poco a un grande numero di vittime. Avvalendosi di risorse tecniche essi camuffano la loro ubicazione reale e possono quindi essere difficilmente catturati.

Gli attacchi partono sovente da Paesi dell'Europa dell'Est, dell'Asia o dell'America del Sud, ma gli autori non vanno affatto ricercati in queste regioni. Rimarrà però difficile identificare e arrestare i criminali informatici finché lo scambio di informazioni tra autorità del perseguimento penale e la situazione giuridica non saranno stati migliorati e posti in sintonia a livello internazionale.

MELANI ritiene pertanto che il mercato si consoliderà ulteriormente e che sussisterà la tendenza a un ulteriore ampliamento e a un'ulteriore professionalizzazione della scena della criminalità informatica. Il capitolo 5.3 presenta esempi in merito.

4 Situazione attuale dell'infrastruttura TIC a livello nazionale

4.1 Attacchi

Ulteriore diffusione del phishing

Nel secondo semestre del 2006 è stato registrato in Svizzera un forte numero di reati economici tramite Internet. In questo contesto il *phishing* costituisce una delle manovre criminali preferite. Nel corso del mese di agosto i clienti della banca Migros hanno ricevuto un e-mail che li sollecitava a indicare i codici di accesso dei loro conti per poterne verificare l'esattezza. L'istituto finanziario decise allora di sospendere temporaneamente il disbrigo delle transazio-

ni via e-banking per poter bloccare le transazioni eventualmente effettuate con codici derubati.

Le tracce di attacchi phishing all'estero conducono anche in Svizzera. Nel corso del mese di settembre l'istituto finanziario Australia and New Zealand Banking Group Limited (ANZ) ha avvertito le autorità svizzere che dietro un dominio svizzero si celava una pagina Web di phishing. Pochi giorni dopo si verificò un caso analogo: questa volta ne furono colpite la Smile Internet Bank e la Suntrust Bank. Ad avvenuto accertamento dei fatti i nomi di dominio sono stati bloccati.

Sebbene gli attacchi di phishing più recenti abbiano seguito modelli diversi (cfr. capitoli 2.3, 3.1 nonché gli esempi del capitolo 5.3), si verificano ancora casi di phishing classico. A tutte le imprese che operano in questo ramo (banche, ditte di aste online, ecc.) si consiglia di mantenere la prudenza e di continuare i loro sforzi di prevenzione.

Malware celato in file PDF

Un istituto finanziario svizzero è stato bersaglio di due diversi incidenti.

Il primo si è verificato all'inizio di settembre e concerneva un e-mail di *phishing* inviato in nome della banca svizzera. I suoi destinatari sono stati sollecitati a indicare i dati di login dei loro conti bancari. Questo attacco non era comunque in grado di eludere le misure di sicurezza del banking online di questo istituto e non mirava nemmeno direttamente i clienti dello stesso.

Il secondo incidente si è verificato nel contesto di un e-mail proveniente presumibilmente dal portale di informazione N-24, che pretendeva che l'istituto finanziario svizzero era stato derubato di 6 miliardi di euro nel corso di una rapina. Per poter leggere l'articolo nella sua integralità occorreva scaricare un documento PDF allegato all'e-mail – in realtà si trattava invece di malware, segnatamente di un *cavallo di Troia* della famiglia di malware Goldun.

4.2 Criminalità

Banche fittizie vogliono approfittare del buon nome della piazza finanziaria Svizzera

In Internet ci si imbatte continuamente in banche fittizie che pretendono di disporre di filiali in Svizzera o che si fregiano dell'aggettivo «swiss». Già nel 2003 hanno fatto la loro apparizione siti come «www.swissbankservices.com», «www.swissprivatebank.com» o «www.swissroyalbank.com». È evidente che si tenta di sfruttare l'immagine di istituto finanziario svizzero per adescare le vittime. Il rapporto «Wirtschaftskriminalität im Internet auf dem Vormarsch» del Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI (www.kobik.ch) si occupa in maniera approfondita di questa variante di truffa, che si è manifestata anche nel 2006.

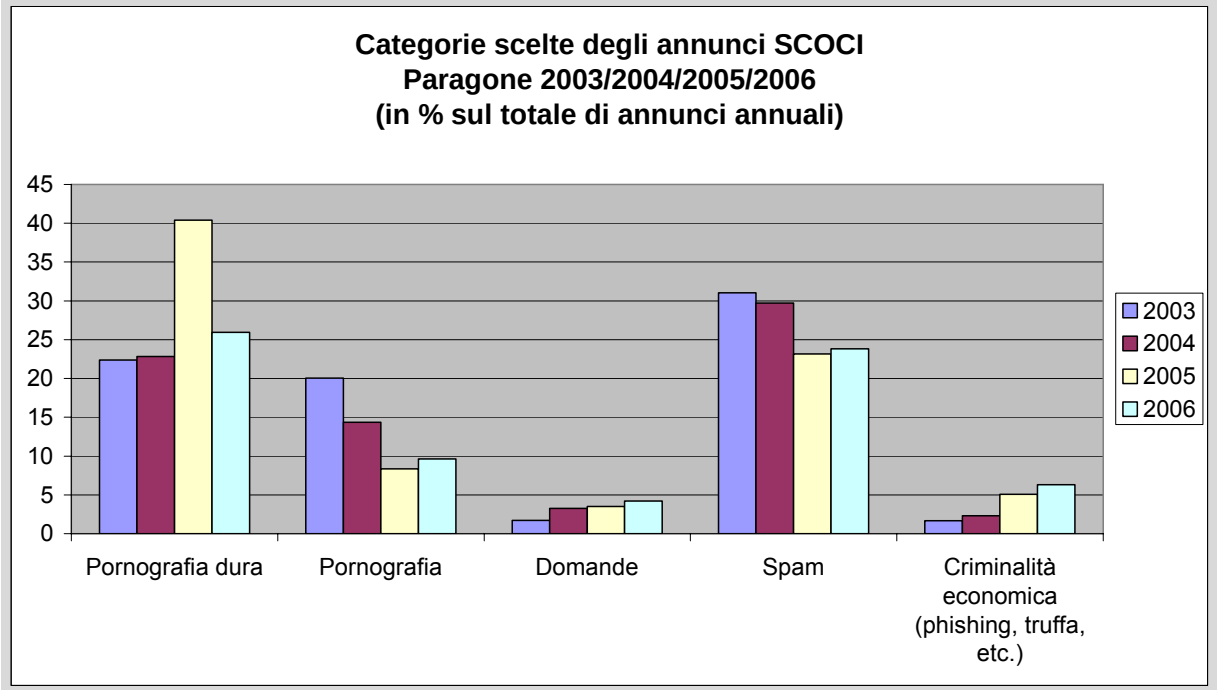
Secondo le informazioni pervenute da diverse fonti dietro la pagina Web «www.swiss-invest.biz» si celava ad esempio un istituto finanziario fittizio il cui obiettivo era di assumere «agenti finanziari». Tali agenti sono meglio conosciuti sotto la denominazione di «money mules». Si tratta di persone che contro il versamento di una commissione e mediante la

messa a disposizione dei loro propri conti bancari partecipano al trasferimento di denaro di provenienza illecita (→ riciclaggio di denaro, cfr. la sezione successiva). Un'ulteriore banca fittizia si è avvalsa dell'URL «www.rhssonline.com». Sul suo sito Web la banca si presentava come avente sede in Svizzera, mentre la sua offerta comprendeva i prodotti finanziari classici dell'e-banking. Veniva inoltre offerta la possibilità di aprire un conto bancario online.

Sono ancora disponibili posti di agente finanziario!

Lo scorso dicembre sono stati inviati a cittadini svizzeri e-mail in cui si ricercavano agenti finanziari. Gli e-mail provenivano da un fornitore fittizio di servizi finanziari denominato Porex GmbH, con sede a Sursee. L'agente finanziario doveva unicamente acconsentire al versamento di una determinata somma di denaro sul proprio conto, poteva conservare una percentuale della somma a titolo di provvigione per il servizio e doveva successivamente versare la differenza su un conto di terzi. La provvigione promessa poteva ammontare fino al 10% della somma ricevuta. Chi accettava si rendeva comunque colpevole di concorso in riciclaggio di denaro. Le somme da trasferire provenivano da conti depredati con l'ausilio di metodi fraudolenti di *phishing*. Nel secondo semestre del 2006 MELANI ha registrato numerosi casi analoghi. Oltre alla Porex, anche una ditta operante sotto il nome di Vicent Reality si è rivolta ai cittadini svizzeri. Questa impresa, che si spacciava per istituto finanziario attivo nel settore immobiliare, pretendeva in un e-mail che diversi clienti svizzeri si erano interessati all'acquisto di immobili sulla Costa Azzurra, in Grecia e in Spagna. Per perfezionare la conclusione del contratto sarebbe mancato unicamente un agente finanziario come mediatore.

Il servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI ha registrato a partire dal 2003 un aumento delle comunicazioni concernenti la criminalità economica su Internet. Questa tendenza è proseguita nel 2006 (cfr. grafico).



Condanna di un hacker per acquisizione illecita di dati

Per la prima volta dall'introduzione, nel 1995, dell'articolo 143 CP, un tribunale svizzero ha pronunciato una sentenza per acquisizione illecita di dati. Nel mese di dicembre un perito

informatico del Cantone di Berna è stato riconosciuto colpevole di acquisizione illecita e di distruzione di dati appartenenti ai suoi concorrenti e clienti.

Il collaboratore in questione della ditta Datasport aveva inviato tra il novembre del 2003 e il giugno del 2004 una dozzina di *cavalli di Troia* per spiare il comportamento della concorrenza e perturbarne l'andamento degli affari. Procedendo in tal modo avrebbe acceduto a 27'000 serie di dati sensibili e distrutto richieste di offerte negli e-mail in entrata delle ditte spiate. La polizia cantonale bernese è intervenuta dopo che una ditta ha effettuato una comunicazione perché sospettava di essere spiata. L'informatico condannato utilizzava un software acquistato da una ditta statunitense specializzata nello sviluppo di applicazioni di sorveglianza a distanza dei computer.

4.3 Diversi

Iniziativa dei provider svizzeri per lottare contro lo spam

I quattro maggiori Internet Service Provider (ISP) della Svizzera hanno dato il via a un'iniziativa comune di lotta contro lo *spam*. Nel mese di novembre Bluewin, Cablecom, Sunrise e Green hanno attivato una pagina Web live (www.stopspam.ch), sulla quale sono disponibili informazioni sul tema dello spam. La pagina Web contiene consigli sulla lotta contro lo spam e descrive misure tecniche pertinenti, come ad esempio l'attivazione dell'autentificazione SMPT all'invio di e-mail.

5 Situazione attuale dell'infrastruttura TIC a livello internazionale

5.1 Avarie

Il traffico Internet nell'Asia del Sudest paralizzato dai danni di un terremoto

Il 26 dicembre 2006 un terremoto nell'area antistante Taiwan ha danneggiato tra l'altro i cavi sottomarini attraverso i quali sono effettuati i collegamenti telefonici, di dati e Internet. Successivamente oltre 100 milioni di persone colpite hanno subito notevoli pregiudizi al traffico Internet.

Durante numerosi giorni gli utenti della Cina, di Taiwan, di Singapore e della Corea del Sud sono stati limitati in maniera massiccia nei loro collegamenti Internet a pagine Web estere. L'interruzione ha toccato palesemente anche importanti servizi finanziari e imprese. A titolo di esempio la Reuters Group PLC Kunden non ha più potuto approvvigionare la clientela

della Corea del Sud e di Hongkong con i dati finanziari più aggiornati. I lavori di riparazione si sono estesi su più settimane, mentre i collegamenti hanno potuto essere ristabiliti solo gradualmente[7].

Questo incidente illustra il grado di dipendenza da Internet raggiunto nel frattempo da intere aree economiche. Le ripercussioni sull'economia delle regioni interessate sono notevoli e difficilmente prevedibili in caso di compromissione dei collegamenti critici o dei nodi delle reti globali di comunicazione.

5.2 Attacchi

Esempi di vettori di attacco: Instant Messaging, e-mail, lacune di sicurezza dei plug-in dei browser, pagine Web di «Social Networking», download di software

Alcuni vettori di attacco sono combinati in misura crescente dagli aggressori. Nel secondo semestre del 2006 si è ad esempio assistito ad attacchi tramite i servizi di Instant Messaging (IM) che contenevano direttamente *malware* nell'attachment («Pipeline» in settembre) oppure link su pagine Web appositamente predisposte («Heartworm», anche in settembre). I messaggi IM davano l'impressione di provenire da contatti amici e invitavano a cliccare sull'attachment o sul link (cfr. in merito al social engineering i capitoli 2.1 e 6). Chi seguiva le indicazioni del messaggio aggregava a sua insaputa il proprio computer a una *rete bot*[8].

È pure ampiamente diffuso un software che si spaccia in modo diverso da quello che è realmente (*cavallo di Troia*). A titolo di esempio un malware si è spacciato per *plug-in* del browser Firefox. In un altro caso un determinato mediaplayer doveva essere scaricato da un sito pornografico per poter presuntamente visionare i film. Invece del mediaplayer la vittima installava un malware che poteva essere utilizzato per spiare o a fini di *phishing* («Zcodec», fine agosto). In entrambi gli esempi le vittime sono state adescate applicando tecniche di social engineering tramite messaggi di spam.

Nel corso dei mesi di luglio e di dicembre un malware ha fatto la sua apparizione su «MySpace», la più famosa pagina Web di Social Networking. L'infezione in luglio era avvenuta avvalendosi di una pubblicità tramite banner, che sfruttava una lacuna di sicurezza. L'attacco in dicembre si è invece avvalso di una lacuna di sicurezza del Quick-Time-Player di Apple[9].

Le pagine Web con contenuti generati dagli utenti costituiscono praticamente un invito a farsi sfruttare dai criminali. Nel caso delle pagine Web usuali si constata che mentre in preceden-

[7] Cfr. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006860; http://www.heise.de/newsticker/meldung/83007 (stato: 15.2.07).
[8] Cfr. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003623&source=rss_news50 (stato: 8.2.07).
[9] Cfr. http://www.heise.de/newsticker/meldung/75707, http://www.securityfocus.com/news/11427; http://www.theregister.co.uk/2006/08/10/fsocial_sites_breed_malware/; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005607&intsrc=hm_list (stato: 8.2.07).

za ne erano toccate soltanto quelle contenenti quasi esclusivamente offerte dubbie, ora vengono parimenti predisposte pagine Web con offerte serie. In settembre la presenza in Internet di Samsung negli Stati Uniti è stata compromessa e utilizzata in maniera abusiva per diffondere malware; nel mese di dicembre il server Web di Asus è stato utilizzato abusivamente per scopi identici. Si scoprono con sempre maggiore frequenza lacune di sicurezza nelle applicazioni Web, ragione per la quale lo sfruttamento abusivo di pagine Web dovrebbe aumentare nei prossimi tempi[10].

In genere gli aggressori si concentrano sempre più sulle applicazioni o sui driver per hardware e meno sui sistemi operativi, che sono tendenzialmente più sicuri. Nel corso dell'ultimo semestre sono ad esempio state sfruttate le lacune di sicurezza dell'Acrobat Reader e del Flash-Player di Adobe, del Quick-Time-Player di Apple o dei driver delle carte *WLAN* (cfr. il contributo separato per quanto concerne le lacune di sicurezza dei prodotti Microsoft)[11].

Problematico è pure il fatto che i software antivirus divengono sempre meno affidabili. Ne sono motivo le numerose varianti che gli sviluppatori di malware producono a intervalli sempre più brevi. Non appena una variante è scoperta e registrata nelle firme antivirus gli aggressori utilizzano già la variante successiva. A titolo di esempio nel mese di novembre sono apparse oltre 1000 varianti di «Warezov» o «Stratio», un malware utilizzato per l'invio di spam[12].

I metodi di attacco sono maggiormente combinati: è apparso un numero sempre più grande di e-mail e di messaggi IM con link su pagine Web appositamente predisposte.

A motivo della forte presenza di lacune di sicurezza nelle applicazioni Web e della crescente popolarità delle pagine Web con contenuti generati dagli utenti (che possono per corrispondenza essere facilmente manipolati), il malware si manifesta con maggiore frequenza su homepage legittime e ufficiali. In combinazione con l'aumento delle lacune di sicurezza nelle applicazioni e nei plug-in aumenta la probabilità di infezione da malware nel quadro della normale navigazione.

Il capitolo 2.4 presenta una valutazione di queste minacce. Il capitolo 2.1 tematizza le tecniche di social engineering utilizzate mentre il capitolo 6 illustra le modalità di protezione contro questi pericoli.

Nuovi exploit di lacune di sicurezza dei prodotti Microsoft – Impiego per lo spionaggio economico mirato, anche in Svizzera

Alcune lacune di sicurezza sono state scoperte soltanto a causa di *0-Day-Exploits*, come ad esempio quelle di Microsoft PowerPoint in luglio[13], di Internet Explorer in settembre[14] e quelle di Word, addirittura a più riprese in dicembre[15]. Dopo l'annuncio e la soppressione delle lacune di sicurezza da parte di Microsoft – di volta in volta il secondo martedì di ogni mese

[10] Cfr. http://www.theregister.co.uk/2006/09/18/web_vulnerabilities (stato: 7.2.07).
[11] Cfr. p.es. http://www.theregister.co.uk/2006/08/04/hackers_bypass_os/ (stato: 7.2.07).
[12] Cfr. http://www.sophos.com/virusinfo/whitepapers/sophos-security-threats-2007_wsrus (stato: 7.2.07).
[13] Cfr. http://isc.sans.org/diary.html?storyid=1484 (stato: 12.2.07).
[14] Cfr. http://www.heise.de/newsticker/meldung/78372; http://isc.sans.org/diary.html?storyid=1727 (stato: 12.2.07).
[15] Cfr. http://www.heise.de/newsticker/meldung/82521; http://blogs.technet.com/msrc/archive/2006/12/15/update-on-current-vulnerability-reports.aspx; http://isc.sans.org/diary.html?storyid=1940 (stato: 12.2.07).

(«Patch-Tuesday») – sono apparsi nel giro di poche ore *exploit* che sfruttavano anche le lacune di sicurezza rese note[16].

Gli attacchi che sfruttano la lacune di sicurezza di Office sono in genere sferrati in modo mirato e, secondo Microsoft, concernono solo poche vittime prescelte[17]. Queste lacune di sicurezza sono in particolare frequentemente sfruttate nel quadro degli attacchi mirati di spionaggio economico e industriale, da lungo tempo in provenienza costante dall'Asia settentrionale e denominati «Titan Rain» (cfr. anche l'ultimo Rapporto semestrale). Nel secondo semestre del 2006 questi attacchi si sono ad esempio manifestati negli USA contro lo State Department, il Commerce Department o il Naval War College.[18] Anche in Svizzera si sono nuovamente verificati attacchi di questo genere contro l'industria d'armamento.

Nel 2007 ci si devono nuovamente aspettare lacune di sicurezza e 0-Day-Exploits contro i prodotti Microsoft Office e Internet Explorer. In genere ne dovrebbe risultare per corrispondenza un aumento degli attacchi mirati di spionaggio contro gli esercenti di *infrastrutture critiche*, i Governi e i fornitori governativi (specialmente dell'industria d'armamento). La Svizzera ne dovrebbe essere colpita in misura identica agli altri Paesi industrializzati occidentali.

Nel caso degli attacchi in provenienza dall'Asia settentrionale le vittime dovrebbero essere maggiormente infettate anche per il tramite di pagine Web, di rilievo per il settore specialistico dei collaboratori, appositamente predisposte sfruttando le lacune di sicurezza di Office.

Il capitolo 2.1 tratta del social engineering, mentre il capitolo 6 tematizza le possibile misure di prevenzione contro simili attacchi.

USA: il numero di serie perdute di dati con contenuti personali supera la barra dei 100 milioni.

Come reso noto a metà dicembre 2006 dalla «Privacy Rights Clearing House» statunitense, dall'inizio del 2005 sono andati perduti i dati personali di oltre 100 milioni di cittadini[19]. Ne sono motivo gli attacchi, i furti di laptop o le perdite dei media di back-up. Negli USA ne sono particolarmente toccati il settore della sanità e i servizi governativi[20]. Secondo uno studio solo una percentuale minima delle persone toccate sono poi effettivamente vittima di un furto di identità[21].

Nel corso del mese di agosto è stato ad esempio reso noto che una banca statunitense e l'US Department of Transportation avevano smarrito dati personali della clientela perché erano stati rubati dei laptop. Pochi giorno dopo AT&T comunicava che in seguito alla com-

[16] Cfr.: http://blog.washingtonpost.com/securityfix/2006/10/patch_tuesday_exploit_thursday.html. Una serie di articoli del Washington Post presenta una buona sintesi della problematica e statistiche sulle lacune di sicurezza individuate: http://blog.washingtonpost.com/securityfix/2007/01/microsoft_achilles_heel_offic_1.html; http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html; http://blog.washingtonpost.com/securityfix/2007/01/cricital_microsoft_mozilla_pat.html (stato: 12.2.07).

[17] Cfr. una presa di posizione di Microsoft: http://blogs.technet.com/msrc/archive/2006/12/08/what-very-limited-targeted-attacks-means.aspx (stato: 12.2.07).

[18] Cfr. http://www.cnn.com//2006/US/07/11/state.hackers.ap/index.html; http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501781.html; http://washingtontimes.com/national/20061130-103049-5042r.htm (stato: 12.2.07).

[19] Cfr. http://www.privacyrights.org/ar/ChronDataBreaches.htm (stato: 12.2.07).

[20] Cfr. http://www.gao.gov/new.items/d06676.pdf; http://oversight.house.gov/Documents/20061013145352-82231.pdf (stato: 12.2.07).

[21] Cfr. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003343 (stato: 12.2.07).

promissione di alcuni dei suoi Webshop erano stati derubati i dati relativi alle carte di credito di circa 19'000 clienti[22]. Nel mese di dicembre la University of California/Los Angeles (UCLA) ha reso noto che in seguito a un attacco di hacker erano stati rivelati i dati personali di oltre 800'000 impiegati, studenti e docenti[23]. Sempre in dicembre Boeing ha perso i dati personali di 382'000 impiegati in seguito al furto di un laptop[24].

Secondo MELANI gli incidenti negli USA illustrano una tendenza che dovrebbe acquistare maggiore importanza anche in Svizzera. La criminalità informatica si interessa a tutti i tipi di dati personali con i quali è possibile fare denaro (nell'underground).

Anche se si verificano con maggiore frequenza attacchi mirati contro i Webshop o le banche dati, la maggior parte delle perdite di dati personali è dovuta a perdite o furti di apparecchiature mobili. Alle imprese che elaborano dati sensibili si raccomanda pertanto di cifrare i dati memorizzati su apparecchiature mobili (in particolare laptop, PDA, ma anche nastri di back-up). Agli esercenti di Webshop si raccomanda di mantenere aggiornate le loro applicazioni Web e di proteggere specialmente i dati concernenti le carte di credito. Il «Centre for the Protection of National Infrastructure CPNI» britannico (ex NISCC) fornisce indicazioni utili in merito[25].

USA: i sistemi di un impianto di depurazione infettati dal laptop di un impiegato

All'inzio dell'ottobre 2006 gli hacker hanno potuto accedere ai sistemi di computer di una centrale idrica di Harrisburg, Pennsylvania (USA) tramite un laptop infettato. Il laptop di un impiegato è stato infettato con *malware* via Internet, consentendo così di assumerne il controllo. È probabile che gli aggressori abbiano successivamente installato *spyware* sul computer per spiare dati sensibili. Anche se secondo le affermazione dell'FBI la centrale idrica non è stata oggetto di un attacco mirato, ma è stato piuttosto il laptop a subire un'infezione casuale, sarebbe comunque stata ipotizzabile una perturbazione dell'impianto di controllo della centrale idrica. A titolo di esempio sarebbe stata possibile una manipolazione del contenuto di cloro dell'acqua potabile[26].

I sistemi «*Supervisory Control and Data Acquisition*» *(SCADA),* concepiti per la sorveglianza e il pilotaggio degli impianti industriali, poggiano in misura crescente su tecnologie e protocolli standard di Internet e sono collegati a Internet. I sistemi SCADA sono pertanto esposti a minacce comparabili a quelle che conosciamo in Internet. Gli sforzi di protezione adeguata degli impianti industriali pilotati con sistemi SCADA devono essere proseguiti.

Il «Centre for the Protection of National Infrastructure (CPNI)» britannico " ha pubblicato una serie di raccomandazioni in forma di best-practices per l'impiego dei sistemi SCADA[27].

---

[22] Cfr. http://www.computerworld.com/action/article.de?command=viewArticleBasic&articleId=9002828 nonché http://www.heise.de/newsticker/meldung/77455 (stato: 12.2.07).

[23] Cfr. http://www.heise.de/newsticker/meldung/82437 (stato: 12.2.07).

[24] Cfr. http://www.computerworld.com/action/article.de?command=viewArticleBasic&articleId=9006098 (stato: 12.2.07).

[25] Cfr. http://www.niscc.gov.uk/ProtectingYourAssets/ElectronicSecurity/applications.aspx (stato: 15.2.07).

[26] Cfr. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004659 (stato: 12.2.07).

[27] Cfr. http://www.cpni.gov.uk/Products/guidelines.aspx (stato: 12.2.07).

5.3 Criminalità

Phishing / furto di identità: valutazione dei costi nonché principali incidenti (elusione dell'autentificazione a due fattori / RockPhish)

Nel corso del secondo semestre del 2006 il *Phishing* e il *furto di identità* hanno registrato un aumento sebbene le perdite siano tuttora di minore entità se paragonate alle perdite dovute alle truffe tradizionali[28]. È in genere difficile enumerare i costi. Senza operare una distinzione tra furti di identità online e furti di identità tradizionali, gli USA e la Gran Bretagna stimano i costi degli ultimi anni in parecchi miliardi di dollari[29]. Non si dispone di stime paragonabili per la Svizzera.

Nel mese di luglio è stato sferrato negli USA un efficace attacco *Man-in-the-Middle* contro il portale di e-banking della Citibank, protetto da un'*autentificazione a due fattori*, e questo tipo di attacco è così stato reso noto per la prima volta a un vasto pubblico. Nel caso dell'autentificazione a due fattori il cliente non deve annunciarsi unicamente con un nome di utente e una password, ma deve fornire ulteriori indicazioni, come ad esempio un numero di stralcio oppure, come nel caso della Citibank, un codice rigenerato regolarmente da un Hardware-Token. Nel caso dell'attacco alla Citibank la vittima è stata attirata tramite e-mail su una pagina di phishing. Questa pagina istituiva in sottofondo un collegamento con il server di e-banking della Citibank. Mentre il cliente credeva di comunicare con la banca, il server di phishing (operando come «uomo in mezzo») registrava le sue indicazioni e le comunicava in nome del cliente al server della banca tramite il collegamento istituito in precedenza. Dopo aver effettuato con successo il login il cliente riceveva un messaggio di perturbazione mentre l'aggressore poteva effettuare transazioni in nome della vittima[30].

L'aumento delle pagine di phishing nel corso del secondo semestre è stato da più parti attribuito al «RockPhish». Chi o cosa sia esattamente il «RockPhish» rimane controverso – nei rapporti il «RockPhish» è designato sia come tool automatizzato per l'allestimento di pagine phishing, sia come gruppo di hacker di cui si presume la presenza dietro la metà circa dei maggiori attacchi di phishing[31]. Il «RockPhish» è in grado di mascherare l'ubicazione del server di phishing, deviando inizialmente il traffico su un *bot*. L'ubicazione vera e propria del server di phishing può quindi essere camuffata efficacemente – se un bot viene disattivato gli aggressori possono semplicemente deviare le future vittime sulla pagina di phishing tuttora in funzione per il tramite di un nuovo bot. Dal profilo dell'e-mail di phishing è come se per ogni vittima fosse creato un proprio URL di phishing[32].

I capitoli 2.3 (situazione attuale) e 3.1 (tendenze) presentano una valutazione di MELANI sul furto di identità e il phishing; ulteriori esempi figurano nei capitoli 4.1 e 4.2.

[28] Cfr. p.es. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004429 (stato: 13.2.07).
[29] Cfr. http://www.ftc.gov/os/2003/synovatereport.pdf; http://www.identity-theft.org.uk (stato: 13.2.07).
[30] Cfr. http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html (stato: 13.2.07).
[31] Cfr. p.es. http://en.wikipedia.org/wiki/Rock_Phish (stato: 13.2.07).
[32] Cfr. in merito al «RockPhish» (stato: 13.2.07):
http://blog.washingtonpost.com/securityfix/2006/12/phishing_scams_soared_in_octob.html;
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005958; nonché
http://www.heise.de/tp/r4/artikel/23/23964/1.html.

Criminalità informatica e criminalità organizzata: si è affermato il mercato underground con commercio e divisione delle attività – partecipanti in aumento e sempre più giovani

Nel corso del 2006 la criminalità informatica si è sviluppata definitivamente in un'attività criminale diffusa. Anche la criminalità organizzata ha scoperto da tempo che le sue manovre affermate – in particolare le truffe, i furti o le estorsioni – possono essere svolte con rischi minori nello spazio virtuale. A tale scopo vengono reclutati sempre più hacker esperti ma anche teenager, sui quali la criminalità informatica esercita evidentemente una grande forza di attrazione. Gli specialisti IT sono reclutati direttamente durante i loro studi, talvolta con metodi dubbi. Numerosi criminali informatici possono vivere delle loro attività ed esercitano la loro «professione» nelle ore di ufficio, come «qualsiasi lavoratore»[33].

Si è costituito un mercato underground per il commercio, lo scambio di informazioni, il reclutamento e la collaborazione. La scena è organizzata in funzione della divisione del lavoro: esistono specialisti che ricercano le *lacune di sicurezza*, le vendono o sviluppano relativi *exploit*. Altri invece si occupano invece dello sviluppo di *malware* e lavorano in comune e con mezzi professionali a varianti sempre nuove. I *Botherder* si concentrano sulla creazione e la manutenzione di reti bot che danno successivamente in locazione – sia per attacchi di *Distributed Denial of Service (DDoS)*, l'invio di *spam*, la diffusione di malware, *adware* e *spyware,* sia per lo spionaggio sui computer aggregati alla rete bot. Gli spammer si specializzano nell'invio di spam e nello sviluppo di e-mail che sfuggono ai filtri antispam. Per quanto concerne il riciclaggio di denaro (il trasferimento di denaro da conti incriminati), nonché l'ordinazione e l'inoltro di articoli per il tramite di numeri derubati di carte di credito o di conti E-Bay, la scena si avvale di specialisti o di persone ignare assoldate a tale scopo. Sono pure oggetto di contrattazione informazioni sulle lacune di sicurezza, exploit (si afferma che nel mese di dicembre un exploit per Windows Vista sia stato offerto per US$ 50'000), malware a scopo di furto (ad es. *cavalli di Troia* specializzati nel furto di dati, per somme comprese tra US$ 1'000 – 5'000), malware per la creazione di reti bot (US$ 5'000 – 20'000), dati derubati (carte di credito con PIN per circa US$ 500, licenze di circolazione US per US$ 150, carte di credito con codice di sicurezza e data di scadenza per acquisti online, tra US$ 7 e 25), ore di locazione di reti bot, consulenza in materia di spamming e molto altro ancora[34].

Il capitolo 3.2 presenta una valutazione del mercato underground della criminalità informatica.

[33] Cfr.: http://www.mcafee.com/us/local_content/white-papers/threat_center/wp_virtual_criminology_report_2007.zip; http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html; http://www.washingtonpost.com/wp-dyn/content/article/2006/12/26/AR2006122600922.html (stato: 7.2.07).

[34] Cfr. http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf; http://www.theregister.co.uk/2006/12/12/cybercrook_xmas_wish_list/; http://www.heise.de/newsticker/meldung/82679 (stato per tutti: 07.02.07).

5.4 Terrorismo

Forum di al Qaïda con glorificazione del terrore anche in tedesco / sempre più pagine Internet in tedesco sulla fabbricazione di bombe

Due anni fa il «Global Islamic Media Front» (GIMF) era quasi stato dichiarato come l'agenzia stampa ufficiale di al Qaïda – nel frattempo non è chiaro se esista effettivamente un contatto diretto tra il GIMF e al Qaïda. Nel corso del mese di agosto è stato reso noto che fin dal maggio del 2006 il GIMF esercitava una pagina Web in tedesco. Per il tramite di questa pagina vengono messi a disposizione in tedesco, con solo pochi giorni di ritardo, i video più recenti, le comunicazioni e le novità di al Qaïda in Iraq. Le traduzioni sono di buona qualità, ragione per la quale occorre partire dal presupposto che non si tratta di traduzioni automatiche[35].

La ditta germanica «Pan Amp», specializzata nello sviluppo di software di sicurezza e di filtraggio, ha d'altra parte comunicato nel mese di dicembre di avere scoperto in Internet oltre 200'000 manuali di fabbricazione di bombe in tedesco. Si può trovare di tutto, dalla bomba in forma di lettera alla bomba con la quale si possono fare saltare in aria i treni[36].

Già negli ultimi due Rapporti semestrali era stato sottolineato che la minaccia da parte del terrorismo informatico - ossia attacchi contro Internet o contro *infrastrutture critiche nazionali* con mezzi delle tecnologie dell'informazione - era sopravvalutata. I terroristi sfruttano Internet a scopi di propaganda, di ideologizzazione, di procacciamento di risorse e di comunicazione.

Sebbene l'indipendenza della ditta «Pan Amp» possa essere posta in forse a causa del suo campo di attività (filtraggio e sorveglianza in Internet), le sue affermazioni forniscono comunque un'indicazione sulla serietà del problema: anche per i simpatizzanti in lingua tedesca è sempre facile trovare le risorse necessarie in Internet. Se si considera simultaneamente il fatto che soprattutto in Europa sussiste un potenziale di estremizzazione e di ideologizzazione, occorre partire dal presupposto che questa evoluzione comporta un ampliamento della cerchia di destinatari potenziali di simili messaggi.

USA: il settore finanziario avvertito di un attacco di al Qaïda contro i sistemi bancari

A fine novembre il Computer Emergency Readiness Team (US-CERT) del Department of Homeland Security (DHS) statunitense ha avvertito il settore finanziario americano della minaccia di un attacco di al Qaïda contro i portali americani di commercio di azioni e le pagine Web delle banche. Come dichiarato dal DHS, l'avvertimento è stato dato a puro titolo cautelare e senza indicazione concreta di un pericolo imminente[37]. Non si è verificato alcun attacco.

L'avvertimento è stato motivato dalla scoperta di un appello intitolato «The Electronic Battle of Guantanamo», inserito il 27 novembre su un forum jihadista protetto da password. Il Ministero statunitense dell'economia e delle finanze avrebbe dovuto essere oggetto di attacchi di *Denial-of-Service (DoS)* per vendicare i musulmani incarcerati nella prigione di Guantanamo-

[35] Cfr. http://www.spiegel.de/politik/deutschland/0,1518,434203,00.html (stato: 13.2.07).
[36] Cfr. http://www.heise.de/newsticker/meldung/82108 (stato: 13.2.07).
[37] Cfr. http://money.cnn.com/2006/11/30/news/economy/al_qaeda/;
http://www.spiegel.de/netzwelt/web/0,1518,451862,00.html (stato per entrambi: 14.2.07).

Bay, sull'isola di Cuba. Gli attacchi avrebbero dovuto iniziare il 1° dicembre e protrarsi fino a fine anno. Simultaneamente l'autore dell'appello esortava i propri fratelli a usare prudenza nella manipolazione dei propri dati personali e a utilizzare possibilmente software anonimo[38]. Il 5 dicembre è stato reso noto sul pertinente forum che l'attacco era stato interrotto perché il settore finanziario ne era stato avvertito precocemente. Le violente reazioni nei media avrebbero comunque palesato quanto potessero essere efficaci gli attacchi a pagine Web di rilevo per l'economia occidentale[39].

È molto improbabile che le cerchie terroristiche dispongano già del know-how necessario a un attacco contro le infrastrutture critiche tramite Internet. Anche in questo caso sarebbero state necessarie grandi conoscenze per un attacco efficace. Non è però da escludere che in futuro il terrorismo possa procurarsi know-how in questo ambito. Per il momento questa acquisizione di know-how si concentra sull'utilizzazione sicura di Internet piuttosto che sugli attacchi contro Internet.

«Technical Mujahid» e «Mujahideen Secrets»: rivista periodica su questioni tecniche e software per la sicurezza dei computer e di Internet sui forum islamici

Il 28 novembre 2006 è stata diffusa per la prima volta nel quadro di un forum jihadista protetto da password una rivista denominata «Technical Mujahid» e focalizzata sulla tecnologia dell'informazione e sulla sicurezza. Essa è pubblicata da un gruppo denominato «Al-Fajr Information Center», che ha già pubblicato a più riprese video violenti. In futuro la rivista dovrà essere pubblicata periodicamente. Secondo gli editori il motivo della pubblicazione va ricercato in un appello di supporto tecnico da parte del capo di al Qaïda in Iraq. La rivista sottolinea parimenti la necessità e la grande utilità di Internet per la jihad.

La rivista, che constava di 64 pagine, conteneva articoli sulla sicurezza dei computer e in Internet, sui sistemi satellitari GPS e sulla cifratura e l'editing di video. Sono tra l'altro pubblicati contributi con titoli come «The Technique of Concealing Files from View» oppure «How to Protect your Files, Even if Your Device was Penetrated», che esprimono i timori dei terroristi nei confronti della sorveglianza sulle tecnologie dell'informazione. La rivista conteneva parimenti link sui tool necessari a una navigazione anonima in Internet e alla salvaguardia sicura dei dati, nonché un articolo su Pretty Good Privacy (PGP), un software per la cifratura degli e-mail[40].

Il 1° gennaio 2007 «Global Islamic Media Front» (GIMF) ha peraltro reso nota la disponibilità prossima di un pacchetto di software denominato «Mujahideen Secrets». Secondo quanto comunicato si tratterebbe del primo «programma informatico islamico» per uno scambio sicuro di informazioni tramite Internet; esso metterebbe a disposizione degli utenti algoritmi di cifratura con chiave simmetriche (256bit) e asimmetriche (2048bit), nonché tool di compressione dei dati[41].

---

[38] Cfr. http://siteinstitute.org/bin/articles.cgi?ID=publications231106&Category=publications&Subcategory=0 (stato: 14.2.07).

[39] Cfr. http://www.memri.org/bin/opener_latest.cgi?ID=IA32907 (stato: 28.02.07).

[40] Cfr. http://www.siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0; http://memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP137506 (stato: 14.2.07).

[41] Cfr. http://memri.org/bin/articles.cgi?Page=subjects&Area=iwmp&ID=SP140707 (stato: 14.2.07).

Entrambi questi esempi illustrano un evidente accresciuto interesse degli estremisti jihadisti per i temi di tecnologia dell'informazione. Per questi estremisti assumono attualmente grande rilievo le questioni di modalità di comunicazione sicura in Internet, di camuffamento e di cifratura dei dati e di migliore protezione contro la sorveglianza e il perseguimento penale.

Se la cerchie jihadiste si avvolgono in maggiore misura di queste conoscenze c'è da aspettarsi che numerose misure di politica di sicurezza per sorvegliare Internet – come quelle attualmente in discussione in seno all'UE e soprattutto in Germania – possano fallire il loro obiettivo vero e proprio di lotta preventiva contro il terrorismo.

6 Prevenzione

Fulcro: social engineering

In generale

Il *social engineering* presenta una grande varietà. Poiché grazie al miglioramento delle misure di sicurezza oggi basta perlopiù un intervento dell'utente per avviare un programma, gli aggressori tentano con sempre maggiore frequenza di sfruttare l'uomo come elemento più debole. Che si tratti di indurre qualcuno a rivelare i suoi dati di login, a installare un programma o addirittura a effettuare un pagamento anticipato a uno sconosciuto, i metodi applicati sono costantemente adeguati e migliorati. I social engineers tentano di sfruttare un momento di sorpresa della vittima per fare appello alla sua disponibilità all'aiuto, per giocare con i suoi timori e per minacciarlo. Il campo di intervento degli aggressori non ha praticamente frontiere. È quanto illustra un esperimento che ha fatto scalpore nella stampa lo scorso semestre: una ditta ha verificato se i suoi collaboratori sapevano individuare gli attacchi di social engineering[42]. La particolarità dell'esperimento descritto in questa sede consiste nel fatto che i collaboratori erano stati informati in precedenza dell'esecuzione della verifica. È stato nondimeno possibile ingannare una parte dei collaboratori distribuendo memory stick USB sul terreno antistante la ditta. Numerosi collaboratori li hanno successivamente inseriti nei computer aziendali. Così facendo hanno installato un programma di spionaggio, garantendo in tal modo agli aggressori l'accesso teorico ai dati aziendali. Questo esempio evidenzia che una sensibilizzazione unica dei collaboratori non basta, ma che occorre una sensibilizzazione regolare e adeguata, che tenga anche conto delle nuove tendenze e dei nuovi metodi.

Le soluzioni tecniche non offrono una protezione completa

Le soluzioni tecniche proteggono solo in misura limitata contro gli attacchi di social engineering. «Anyone who thinks that security products alone offer true security is settling for the illusion of security (chiunque pensi che i prodotti di sicurezza offrano da soli un'autentica sicurezza si accontenta dell'illusione della sicurezza)» ammonisce ad esempio in merito Ke-

[42] Cfr. http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1 (stato: 19.2.07).

vin Mitnick, uno dei più celebri ex hacker[43]. I programmi antivirus o i filtri di spam offrono senz'altro una sicurezza di base contro la maggior parte del *malware* con il qual viene propagato il social engineering. Ma proprio per questo in caso di attacchi mirati di spionaggio il rilevamento automatico è praticamente impossibile. I programmi di spionaggio utilizzati a questo scopo sono sviluppati in un numero molto elevato di varianti e volutamente diffusi solo in numero ridotto, per cui i programmi antivirus non sono sempre in grado di individuarli. La fiducia cieca nei programmi di protezione è pertanto controproducente. L'idea che la tecnica possa risolvere tutto può infondere una falsa sensazione di sicurezza al collaboratore e quindi ridurne la prudenza.

Caratteristiche generali di rilevamento

Nella maggior parte dei casi l'aggressore tenta di sfruttare il momento di sorpresa. Sovente si spaccia per una persona conosciuta e, nelle grandi imprese, come collega di lavoro, collaboratore o tecnico di servizio (personalmente sconosciuto) di un fornitore di fiducia o di un'impresa rinomata. Nel caso dell'attacco con malware il messaggio trasmesso fa stato di fatti concernenti il campo di attività del destinatario – solitamente rilevati in precedenza – e utilizza il pertinente gergo specializzato. Si impone di norma prudenza se il messaggio contiene l'invito a effettuare un'azione e tale invito è abbinato a un inganno, a un'estorsione, a un'intimidazione, a una minaccia, a un appello alla disponibilità all'aiuto o allo sfruttamento dell'ingenuità. Gli attacchi non sono unicamente perpetrati tramite e-mail – si sono anche osservati attacchi per telefono o SMS.

Per indurre la vittima a compiere determinate azioni deve essere istituito un contesto di fiducia. Le informazioni personali sulla ditta o su una determinata persona necessitate dall'aggressore non sono ad esempio reperibili unicamente nel cestino della carta delle imprese. Tutti hanno già vissuto l'esperienza la mattina in treno dello scambio a voce sommessa di informazioni confidenziali. Anche in Internet sono reperibili indicazioni su impiegati o imprese. A volte è possibile reperire tutto un curriculum vitae o una homepage privata con dati personali di un collaboratore. Possono essere parimenti di grande utilità per l'aggressore i rapporti di gestione, gli elenchi telefonici (interni), gli organigrammi, le relazioni pubblicate dalla stampa, i rapporti di borsa e numerose altre informazioni di facile ottenimento sull'impresa da attaccare.

Gli indirizzi dei mittenti possono essere facilmente falsificati mentre – come descritto più sopra – le informazioni personali concernenti la vittima possono essere facilmente raccolte. L'identificazione sicura di simili attacchi è difficile anche in caso di buone conoscenze, ragione per la quale occorre intimare ai collaboratori di rivolgersi al (presunto) mittente in caso di dubbio.

Il caso speciale del phishing

Un altro tipo speciale di social engineering è il cosiddetto *phishing*. Oltre allo sfruttamento del momento di sorpresa, si incute timore alla vittima minacciando nella maggior parte dei casi il blocco del conto. Lo scorso anno sono apparsi sempre più sul mercato programmi destinati a mettere in guardia le vittime dalle pagine di phishing. L'ultimo Rapporto semestrale ha abbordato il tema in maniera dettagliata. Con il release di Internet Explorer 7 si aggiunge ora un nuovo programma. Il nuovo Internet Explorer dovrebbe essere in grado di riconoscere un grande numero di pagine fraudolente grazie ai suoi filtri phishing. Ma anche in questo caso la

[43] Mitnick, Kevin & Simon, William L., «The Art of Deception: Controlling the Human Element of Security», Hungry Mind Inc., 2002.

fiducia cieca in simili filtri comporta un pericolo. I programmi anti-phishing sono senz'altro utili ma non sono in grado di riconoscere fin dall'inizio tutte le pagine. La responsabilità finale incombe all'utente. Occorre pertanto definire modi di comportamento semplici e facili da ricordare. In questo senso l'immissione manuale della pagina di e-banking nella riga di indirizzo del browser rappresenta una protezione buona e semplice. È pure importante ricordare che un istituto finanziario non inviterà mai la propria clientela a comunicargli tramite e-mail i dati di login, la password e il TAN.

Direttive e User-Awareness

Per l'aggressore è molto importante raccogliere prima dell'attacco tutti i dati possibili sull'impresa e i suoi collaboratori. Tramite una formazione mirata dei collaboratori – ma anche una manipolazione restrittiva dei loro dati personali in Internet – è possibile limitare la disponibilità di simili informazioni per l'aggressore. Ogni collaboratore dovrebbe sapere quali informazioni possono essere utilizzate in quale maniera. Un sistema corrispondente di classificazione deve essere semplice e chiaro. Oltre alla manipolazione sicura delle risorse informatiche, l'helpdesk dovrebbe ad esempio seguire precise direttive su chi può avere accesso a quali dati e a quali condizioni. Tali direttive dovrebbero essere osservate anche quando si è sotto pressione o in caso di eventi eccezionali. È parimenti opportuna l'introduzione della semplice norma di rivolgersi al (presunto) mittente in caso di dubbio.

Problema: difesa contro lo spionaggio mirato

Nel caso appunto degli attacchi mirati di spionaggio sono sovente inviati e-mail contenenti fatture, offerte, rapporti o news (con l'apparenza dell'autenticità). Se si aprono questi documenti vengono sfruttate anche lacune di sicurezza fino ad allora sconosciute. Se poi il computer è collegato a Internet viene operato un trasferimento involontario dei dati. Questi tipi di attacchi di social engineering sono di difficile rilevamento perché nel quadro della sua attività quotidiana il collaboratore ha il compito di ricevere documenti simili. In questi casi anche le norme di comportamento possono fallire. Le misure come l'interruzione del collegamento a Internet o la verifica in una macchina virtuale di tutti i documenti entranti possono essere d'ausilio per limitare ulteriormente queste minacce. Esistono già soluzioni commerciali sul mercato. Nel quadro di una formazione regolare i collaboratori non dovrebbero inoltre essere informati soltanto in merito agli attacchi, ma anche essere istruiti su chi devono informare in caso di dubbio – anche per quanto concerne i crash di sistema, il rallentamento delle stazioni di lavoro o altri comportamenti anormali del PC.

Nuovi mezzi di comunicazione, nuovi pericoli

I nuovi programmi e mezzi di comunicazione comportano sovente anche nuovi vettori di attacco. Nel corso degli ultimi mesi l'*Instant Messaging (IM)* o il *Voice over IP (VoIP)* hanno acquistato maggiore importanza come vettori di attacco. Sovente queste tecnologie sono applicate in maniera troppo noncurante nelle imprese, sebbene proprio questo mezzo di comunicazione possa essere utilizzato proficuamente per il social engineering. Le imprese devono esaminare con molta attenzione quali servizi intendono mettere a disposizione dei loro collaboratori. Nella relativa decisione devono essere ponderate la necessità di un aumento della produttività e considerazioni in fatto di sicurezza.

- Norme comprensibili e incisive di comportamento contribuiscono grandemente alla protezione dei dati confidenziali (dell'impresa).
- Ogni utente/collaboratore può contribuire alla sicurezza con il proprio comportamento.

- Formazioni e test regolari e adeguati alle tendenze di maggiore attualità aiutano a sensibilizzare gli impiegati e a rilevare i pericoli possibili.
- Le misure tecniche rientrano nella protezione di base, ma non possono ricoprire tutti i vettori di attacco.
- I nuovi mezzi di comunicazione schiudono nuove possibilità, ma comportano in genere anche nuovi pericoli.
- Attualmente si osservano sempre più attacchi basati su e-mail. È quindi particolarmente importante una sensibilizzazione che comporti anche una manipolazione prudente degli e-mail.

7 Attività / informazioni

7.1 Stati

Germania: conservazione preventiva dei dati a prescindere dai sospetti, banca dati antiterrorismo e legge sulla protezione dello Stato

Come già menzionato nell'ultimo Rapporto semestrale, nel contesto della lotta contro il terrorismo sono state adottate negli USA e in Germania misure per migliorare la sorveglianza su Internet. Il dibattito è incentrato sulla conservazione di determinati dati, nonché sul loro scambio con diverse autorità in materia di sicurezza. Nel quadro della sua presidenza di turno dell'UE nel primo semestre del 2007, la Germania vorrebbe promuovere una più intensa sorveglianza su Internet e una più forte interconnessione delle banche dati di ricerca a livello europeo.

Nel novembre del 2006 il ministro germanico della giustizia ha presentato un disegno di legge concernente il nuovo ordinamento della sorveglianza sulle telecomunicazioni. Ha suscitato in particolare opposizioni la proposta di trasposizione della direttive dell'UE sulla conservazione dai dati a prescindere dai sospetti (cfr. in merito alla direttiva dell'UE il Rapporto semestrale 2005/II).[44] La direttiva prescrive agli Stati membri dell'UE di conservare per una durata compresa tra 6 e 24 mesi i dati di collegamento e di ubicazione relativi alle comunicazioni telefoniche e all'invio di SMS e di e-mail[45]. Il disegno di legge germanico prevede una durata di conservazione di 6 mesi. La legge dovrebbe essere adottata dal Bundestag verso la metà del 2007. Gli esponenti del movimento per i diritti civili, i fautori della protezione dei dati e i politici dell'opposizione giudicano anticostituzionale il disegno di legge, mentre

[44] Cfr. http://www.bmj.bund.de/enid/968152a666b778952bc9da769d9fb82a,6f1ad6706d635f6964092d0933313733093a095f7472636964092d0933303334/Pressemitteilungen_und_Reden/Pressemitteilungen_58.html (stato: 19.2.07).

[45] Cfr. Rapporto semestrale MELANI 2006/I, capitolo 8: http://www.melani.admin.ch/dokumentation/00123/00124/00162/index.html?lang=de (stato: 19.2.07).

l'«Arbeitskreis Vorratsdatenspeicherung»[46] invita tutti i cittadini preoccupati da questa legislazione ad aderire a una «querela collettiva» online.

All'inzio di dicembre 2006 il Bundestag ha deciso la creazione di una banca dati antiterrorismo, destinata a fungere da banca dati comune delle autorità di polizia e dei servizi di informazione del Governo federale e dei Länder. La legge che ne costituisce la base legale è entrata in vigore a fine 2006[47]. La banca dati antiterrorismo deve rendere possibile lo scambio di dati e quindi una più stretta collaborazione tra le diverse autorità in materia di sicurezza. La banca dati antiterrorismo è violentemente controversa. Il ministro degli interni Wolfgang Schäuble la considera uno «strumento irrinunciabile di lotta contro il terrore» e sottolinea la necessità per lo Stato liberale di diritto di essere in grado di garantire la sicurezza dei suoi cittadini[48]. Gli oppositori criticano soprattutto la minaccia che essa rappresenta per la separazione tra servizi di polizia e servizi di informazione prevista dalla legge, come pure il fatto che la banca dati non è esplicitamente destinata alla sola lotta contro il terrorismo internazionale, ma anche ad «altri scopi»[49].

Come primo Land germanico, il Nord Reno-Westfalia ha adottato a fine dicembre 2006 una modifica della legge sulla protezione dello Stato destinata a offrire una base legale sicura per effettuare nascostamente perquisizioni di computer privati in caso di sospetto di reati estremistici[50]. Queste cosiddette perquisizioni online equiparano l'acceso al computer all'intercettazione telefonica da parte degli organi di protezione dello Stato. In questo contesto sarà introdotto clandestinamente *malware* nei computer delle persone sospettate per perquisire i documenti che vi sono memorizzati. I sostenitori della nuova legge ritengono il controllo su Internet necessario per ottenere informazioni sui piani di attentati, di attentati suicidi o di fabbricazione di bombe[51].

A livello federale anche il Ministero degli interni prevede nell'ambito del «Programm zur Stärkung der inneren Sicherheit» un'estensione delle risorse e delle competenze del Bundeskriminalamt per le inchieste su Internet. In questo ambito anche le perquisizioni online svolgeranno un ruolo importante. In seno al Bundeskriminalamt viene inoltre istituito un servizio di monitoring e di analisi di Internet (IMAS), destinato a rafforzare la lotta contro il terrorismo tramite la sorveglianza e l'analisi di pertinenti pagine Internet[52]. La legittimità della nuova legislazione è comunque aspramente controversa. Non si è soprattutto in chiaro se lo spionaggio di dati memorizzati su un computer è compatibile con la legge germanica. Già nel novembre 2006 il Bundesgerichtshof aveva dichiarato illegali le perquisizioni online di sistemi di computer perché mancavano dell'indispensabile base legale[53].

---

[46] Cfr. http://www.vorratsdatenspeicherung.de (stato: 19.2.07).
[47] Cfr. http://bundesrecht.juris.de/bundesrecht/atdg/gesamt.pdf (stato: 19.2.07).
[48] Cfr. (stato: 19.2.07)
http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2006/09/Antiterrordatei.html.
[49] Cfr. http://bundesrecht.juris.de/bundesrecht/atdg/gesamt.pdf, paragrafo 6 (stato: 19.2.07).
[50] Cfr.
http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/XMMGVB0638.pdf?von=620&bis=621;
http://www.landtag.nrw.de/portal/WWW/P/Presse/Oeffentlichkeitsarbeit/Informationen/2006/12/2012_Plenum_aktuell.jsp (stato: 19.2.07).
[51] Cfr. http://www.heise.de/newsticker/meldung/82814; http://www.nzz.ch/2006/12/21/al/articleERN8M.html (stato: 19.2.07).
[52] Cfr.
http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2006/11/Programm__zur__Staerkung__der__Inneren__Sicherheit.html; http://www.sueddeutsche.de/computer/artikel/965/93872/;
http://www.heise.de/newsticker/meldung/82154 (stato: 19.2.07).
[53] Cfr. http://www.heise.de/newsticker/meldung/82341 (stato: 19.2.07).

Per quanto concerne la situazione in Svizzera sul fronte della conservazione preventiva dei dati, i provider devono conservare per sei mesi determinati dati di collegamento a Internet. È in corso un dibattito su un eventuale inasprimento delle norme; in questo contesto il Consiglio federale è favorevole a un innalzamento della durata di conservazione.

Le perquisizioni online senza sospetto concreto sono finora vietate in Svizzera. L'accesso ai computer è nondimeno previsto dalla nuova legge sulle misure per la salvaguardia della sicurezza interna (LMSI). Questa misura è però applicabile unicamente in casi eccezionali e a severe condizioni. Al termine dell'operazione la persona interessata dovrebbe inoltre essere informata in merito alla sorveglianza effettuata. L'esame del disegno di legge è tuttora in corso alle Camere federali.

Il capitolo 5.4 contiene una valutazione di MELANI sull'utilizzazione di Internet da parte delle cerchie terroristiche nonché riflessioni sui loro preparativi per controbattere la sorveglianza su Internet.

EU: Rafforzamento di Europol / ampliamento della sorveglianza su Internet

La Commissione europea prevede di estendere le competenze dell'Ufficio europeo di polizia (Europol). Devono tra l'altro essere rese possibili una migliore lotta contro la criminalità informatica e un'elaborazione centralizzata e più efficiente dei dati conservati presso Europol.

Il mandato di Europol deve essere esteso alla totalità del settore delle forme gravi di criminalità. Pertanto questa autorità deve estendere il suo campo di attività anche al settore della criminalità informatica e della sorveglianza su Internet. La Commissione propone inoltre di migliorare l'elaborazione dei dati conservati presso Europol. In determinati casi una possibilità potrebbe consistere nella creazione, da parte di Europol, di una banca dati delle pagine Internet dalle quali potrebbe risultare una minaccia[54].

Già nel quadro dell'allestimento del programma «Check the Web» nella primavera del 2006 diversi Stati dell'UE avevano raggiunto un'intesa sull'istituzione di una sorveglianza transfrontaliera su Internet con la partecipazione di Europol[55]. Presso Europol va allestito un portale di informazione attraverso il quale gli Stati membri possano scambiarsi informazioni. In questo contesto è parimenti prevista l'introduzione di un sistema comune di informazione sui visti. Nel quadro della sua presidenza di turno dell'UE la Germania promuoverà lo scambio di informazioni e la sorveglianza su Internet a livello dell'UE.

MELANI considera utile e necessario alla garanzia della sicurezza interna un scambio efficiente di informazioni a livello internazionale che garantisca nel contempo la protezione dei dati. Va parimenti caldeggiata una collaborazione a livello europeo in materia di osservazione e di analisi di pertinenti pagine di Internet.

[54] Cfr. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/1861&format=HTML&aged=0&language=DE&guiLanguage=en; http://www.heise.de/newsticker/meldung/82820 (stato: 19.2.07).

[55] Cfr. Rapporto semestrale MELANI 2006/I, capitolo 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/00162/index.html?lang=de (stato: 19.2.07).

Germania e Gran Bretagna: riforme delle legislazioni penali in materia informatica

Alla fine del 2006 la Germania e la Gran Bretagna hanno varato dei disegni di legge che si prefiggono tra l'altro un'estensione della fattispecie del reato di «hacking». D'ora in poi saranno vietate anche la produzione e la diffusione di «Hacker-Tools» e la commissione di attacchi *Denial-of-Service (DoS)*. Entrambe le leggi nazionali dovranno essere adeguate al decreto quadro dell'UE sugli attacchi ai sistemi informatici nonché alla convezione sulla criminalità informatica del Consiglio d'Europa[56].

Nella Gran Bretagna è stata simultaneamente adottata una nuova legge che include il *phishing* nel reato di truffa e punisce pertanto anche il mero tentativo di phishing[57].

Entrambi i disegni di legge sono oggetti di aspre critiche. Si teme principalmente una «sovracriminalizzazione» di software utilizzato anche per analizzare lacune di sicurezza e quindi indispensabile al ramo settoriale della sicurezza IT. Si temono inoltre problemi di sicurezza del diritto in caso di produzione e di diffusione di software. Anche MELANI ritiene problematico rendere illegale la produzione e la diffusione di software necessario anzitutto anche per poter valutare la vulnerabilità e la sicurezza dei sistemi di informazione.

Gli USA ratificano la convenzione sulla criminalità informatica del Consiglio d'Europa e vi aderiscono a contare dal 1° gennaio 2007

A fine settembre 2006 il senato degli USA ha ratificato, dopo un ritardo iniziale, la convenzione sulla criminalità informatica del Consiglio d'Europa. Gli USA sono quindi il sedicesimo Stato che ha ratificato la convenzione[58].

La convenzione è il primo trattato internazionale nel campo della lotta alla criminalità informatica. Gli Stati contraenti si impegnano ad adeguare ai progressi delle tecnologie dell'informazione il loro diritto penale e la loro procedura penale, nonché le disposizioni in materia di collaborazione internazionale in ambito penale.

La criminalità in Internet è un problema transfrontaliero. Una della principali difficoltà della lotta è costituita dalla diversità delle singole legislazioni nazionali. In vista di una lotta efficace sono determinanti adeguamenti di legge e una maggiore collaborazione internazionale (cfr. anche in merito i capitoli 3.2 e 5.3). La convenzione sulla criminalità informatica del Consiglio d'Europa è uno strumento molto promettente. La Svizzera ha firmato la convenzione nel 2001, ma non l'ha ancora ratificata[59].

---

[56] Cfr. http://www.bmj.bund.de/enid/2f99c147790664d0475a936f509414f9,792f747072657373656617274696b656c5f6964092d0932353638093a096d795f79656172092d0932303036093a096d795f6d6f6e7468092d093039093a095f7472636964092d0932353638/Presse/Pressemitteilungen_58.html; http://www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en.pdf (stato: 19.2.07).

[57] Cfr. http://www.opsi.gov.uk/ACTS/acts2006/ukpga_20060035_en.pdf (stato: 19.2.07).

[58] Cfr. http://www.state.gov/r/pa/prs/ps/2006/73353.htm; http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=2/14/2007&CL=GER (stato: 19.2.07).

[59] Cfr. (stato: 19.2.07) http://www.ejpd.admin.ch/ejpd/de/home/themen/kriminalitaet/cybercrime/ref_cybercrime__europarat.html.

USA: il DHS istituisce un responsabile della sicurezza informatica

Nel settembre del 2006 il Department of Homeland Security (DHS) ha istituito dopo lunghi tentennamenti un responsabile della sicurezza informatica che opera per la prima volta con il rango di supplente del capodipartimento. In questo senso gli USA saranno in grado di meglio proteggere da eventuali attacchi informatici le loro i*nfrastrutture critiche di informazione*. Questa funzione è quindi occupata per la prima volta a distanza di 14 mesi dalla sua istituzione da parte del Congresso, nel luglio del 2005[60].

Nel febbraio del 2006 il DHS ha effettuato un esercizio denominato «Cyber Storm Exercise», nel cui ambito è stato simulato un attacco informatico contro le infrastrutture critiche di informazione degli USA[61]. In questo contesto è stata nuovamente rilevata l'assenza negli USA di una chiara strategia, nonché di un coordinamento delle misure in caso di emergenza. Il nuovo responsabile della sicurezza informatica dovrà ora implementare una nuova strategia in collaborazione con l'economia privata e allestire un piano di protezione in caso di emergenza[62].

7.2 Economia privata

Svizzera: PostFinance introduce SmartCards per l'autentificazione in ambito di e-banking

PostFinance sostituirà sui suoi sistemi di e-banking Yellownet gli elenchi di stralcio per l'autentificazione con un'autentificazione tramite SmartCard. A contare dal marzo 2007 Postfinance consegnerà gratuitamente alla sua clientela gli indispensabili lettori di carte. Per il tramite di questa misura tecnica potrà essere ridotto il pericolo di attacchi *phishing*.

Questo procedimento tecnico garantisce che il cliente non potrà essere indotto a divulgare a un phisher la totalità dei suoi dati di login.

---

[60] Cfr. http://www.dhs.gov/xnews/releases/pr_1158759756150.shtm nonché le considerazione nel Rapporto semestrale MELANI 2005/II, capitolo 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html?lang=de (stato: 19.2.07).

[61] Cfr. http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm (stato: 19.2.07).

[62] Cfr. http://www.washingtonpost.com/wp-dyn/content/article/2006/09/18/AR2006091800928.html (stato: 19.2.07).

8 Basi legali

Germania: l'assenza di cifratura del WLAN può comportare conseguenze legali

A fine 2005 era possibile scaricare file audio da un computer di Amburgo collegato a una rete senza fili non sicura. Gli esercenti della rete senza fili (WLAN) sono stati individuati e diffidati dal proprietario dei diritti. La diffida è però stata respinta adducendo il motivo che un terzo ignoto aveva offerto i file musicali per il tramite di un WLAN non sicuro. Il conglomerato musicale ha richiesto con esito positivo l'adozione di un provvedimento provvisorio al Landgericht. Nella sua sentenza il tribunale si rifà ai principi della responsabilità del perturbatore. Anche gli offerenti di servizi che forniscono un contributo immediato alla violazione del diritto per il solo fatto della concessione dell'accesso a contenuti di terzi devono essere qualificati come perturbatori. Chiunque esercita senza fili il proprio collegamento Internet deve provvedere alla sicurezza del suo router; nell'ipotesi contraria esso contravviene ai suoi obblighi ragionevoli di verifica. Secondo il giudice, in quanto esercente dell'accesso il convenuto avrebbe avuto l'obbligo di informarsi sulle modalità di prevenire simili violazioni.

In Germania la sentenza del Landgericht di Amburgo potrebbe schiudere nuove dimensioni alle questioni di responsabilità. Essa non è comunque ancora stata confermata dal Bundesgerichtshof. Anche in Svizzera un conglomerato musicale potrebbe fare valere i suoi diritti invocando il diritto d'autore. E anche in Svizzera il fatto di rendere accessibili al pubblico prodotti protetti dal diritto d'autore e di diffonderli senza autorizzazione viola la legislazione in materia di diritto d'autore.

Secondo le valutazioni del Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI) in Svizzera non è attualmente ipotizzabile il perseguimento penale dell'esercente di un WLAN in un caso del genere. Anche una responsabilità ai sensi dell'articolo 41 del Codice delle obbligazioni non è attualmente pensabile in Svizzera. Ciò non significa però che la problematica delle reti senza fili aperte non sia fonte di difficoltà. Lo SCOCI ha già registrato i primi casi di utilizzazione di WLAN aperti per la commissione di reati. Si tratta nella fattispecie di estorsioni, di molestie sessuali e di scaricamento di pornografia infantile.

Germania: sentenze nei confronti di agenti finanziari

Nel corso del secondo semestre anche nell'area di lingua tedesca sono stati viepiù ricercati agenti finanziari per trasferire all'estero denaro proveniente dal *phishing* (cfr. anche il capitolo 4.2). In questo contesto esistono ora diverse sentenze di tribunali germanici.

L'Oberlandgericht di Amburgo ha giudicato che i clienti delle banche che mettono i loro conti a disposizione per il versamento di denaro proveniente da attacchi di phishing e che prelevano questo denaro in vista del suo trasferimento ulteriore devono restituire queste somme al pertinente istituto finanziario. Il cliente non può neppure obiettare che la banca avrebbe potuto impedire i prelievi in contanti. Tutto è partito da prelievi in contanti per un valore di circa 33'000 euro. La banca, dopo averne ricevuto comunicazione da una persona danneggiata, ha effettuato una verifica del conto dell'attrice, che si è conclusa con lo storno degli accrediti. Successivamente l'istituto di credito ha chiuso il conto ed esatto la restituzione dei circa 33'000 euro. La cliente ha reagito con una querela, esigendo dal canto suo l'accredito della totalità della somma.

Il phishing di dati relativi ai conti può però anche concludersi con una pena privativa di libertà se il titolare del conto funge da mediatore del truffatore. I tribunali considerano questa fatti-

specie come riciclaggio punibile di denaro. Un 46enne di Meersburg è stato condannato dal tribunale di Überlingen a una pena pecuniaria di 30 unità giornaliere per aver tentato di effettuare tramite il suo conto trasferimenti all'estero, predisposti illegalmente da terzi. Sconosciuti si erano procurati illegalmente tramite phishing l'accesso ai dati bancari della persona danneggiata e quindi versato queste somme di denaro sul conto dell'imputato. Quest'ultimo doveva prelevare il denaro in contanti e trasferirlo all'estero tramite la Western Union, dopo deduzione di una provvigione dell'8,5%

È probabile che anche in Svizzera parecchie persone abbiano reagito consapevolmente o inconsapevolmente alle offerte di lavoro dei truffatori phishing e abbiano operato come agenti finanziari. Si vedrà poi se anche in Svizzera si giungerà a condanne penali. In Svizzera non esistono ancora precedenti in materia.

9 Glossario

Il presente glossario contiene tutti i concetti evidenziati *in corsivo* nel rapporto. Un glossario completo è disponibile in: http://www.melani.admin.ch/glossar/index.html?lang=de.

0-day-exploit	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
Adware	L'adware, una combinazione delle parole advertisement e software, viene sovente utilizzato a scopi pubblicitari, nel senso che le abitudini di navigazione dell'utente sono registrate e sfruttate per offrire prodotti corrispondenti (ad es. tramite link).
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	Procedura di login che oltre al nome di utente e alle password esige un ulteriore (secondo fattore) da parte dell'utente. Si utilizzano diverse varianti: elenchi di stralcio, codici generati da un hardware-token, codici elaborati con procedure crittografiche, dati biometrici. L'autentificazione a due fattori esige due dei tre elementi di base «qualcosa che si sa» (ad es. password), «qualcosa che si ha» (ad es. security token) o «qualcosa che si è» (dati biometrici).
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.
Botherder	Esercente di una *rete bot.*

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.
Critical Infrastructure Protection / Critical Information Infrastructure Protection (CIP / CIIP)	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.
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere – ossia sul vostro computer.
Furto di identità	Furto o utilizzazione abusiva di dati personali (password, dati per l'identificazione di persone private, segreti aziendali, dichiarazioni di imposta, dati relativi a carte di credito, informazioni sui conti ecc.) da parte di terzi.
Instant Messaging (IM)	Servizio che consente di comunicare (chat) in tempo reale con altri partecipanti e sovente anche di scambiare file. Milioni di utenti nel mondo intero sono registrati presso i servizi IM esistenti (AOL, MSN, ICQ, Yahoo ecc.).
IP Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
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.
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.
Plug-In	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.
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Social Engineering	Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni.
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche gli e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
Spear Phishing	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
Spyware	Lo spyware è destinato a raccogliere all'insaputa dell'utente informazioni sulle sue abitudini di navigazione oppure sulle configurazioni di sistema per trasmetterle a un indirizzo predefinito.
Verme informatico	Diversamente dai *virus*, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfruttano piuttosto le lacune di sicurezza o gli errori di configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro.
Vettore di attacco	Percorso utilizzato o tecnica applicata da un aggressore per penetrare in un sistema di computer.
Virus	Un programma informatico capace di autoreplicarsi e provvisto di funzioni nocive, che si aggancia a un programma ospite o a un file ospite per diffondersi.
Voice over IP (VoIP)	Telefonia tramite il protocollo Internet (IP). I protocolli utilizzati con maggiore frequenza sono: H.323 e SIP.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.