Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

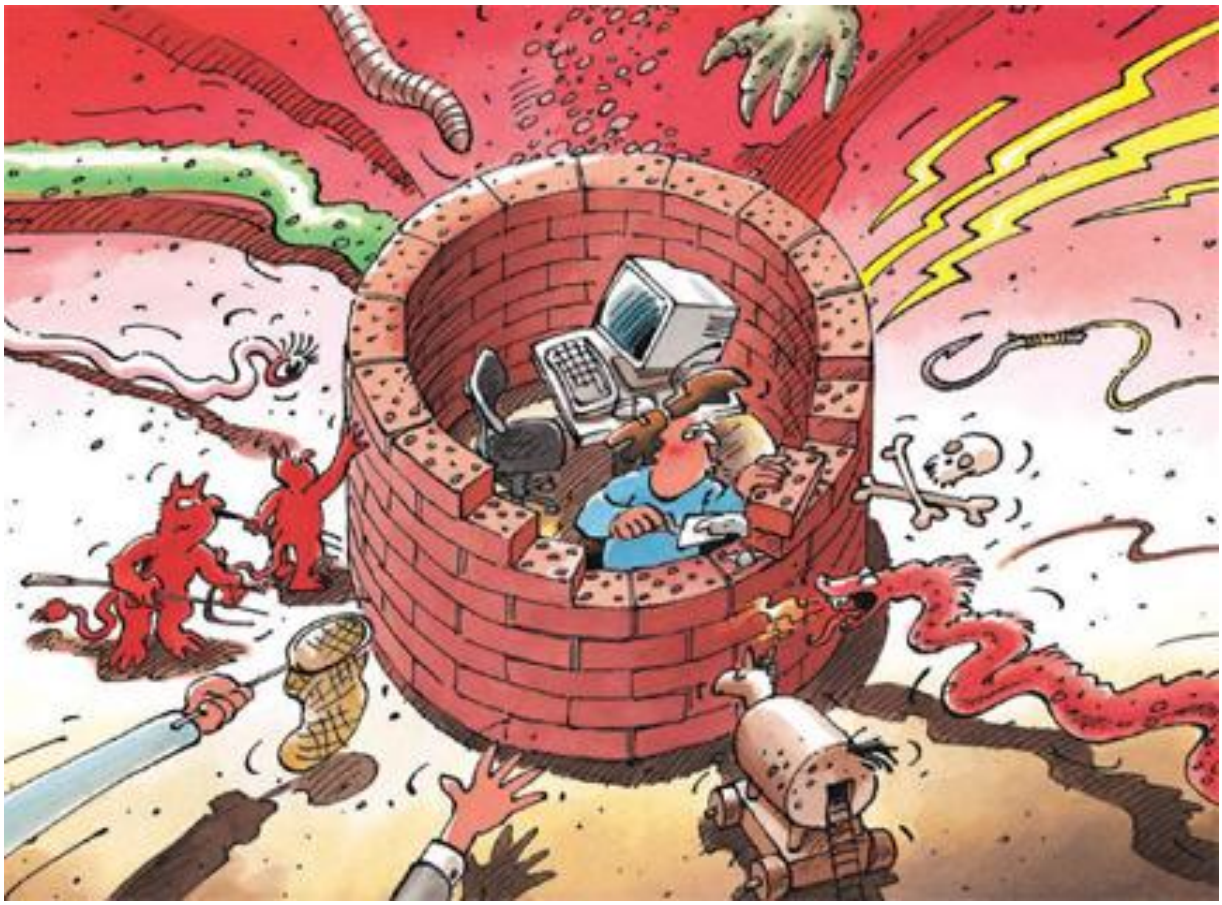
Organo strategia informatica della Confederazione OSIC
Servizio delle attività informative della Confederazione SIC

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

Sicurezza dell'informazione

Situazione in Svizzera e a livello internazionale

Rapporto semestrale 2010/I (gennaio - giugno)



Indice

1 Cardini dell’edizione 2010/I

Spionaggio con mezzi IT – Pericolo in aumento

Nel corso dell’ultimo semestre sono stati nuovamente resi noti alcuni casi di spionaggio, come ad esempio quelli ai danni di Google, Adobe e anche dell’ufficio del Dalai Lama. Thomas de Maizière, il ministro germanico degli interni, ha messo in guardia nel recente rapporto sulla tutela della Costituzione contro il pericolo di un crescente spionaggio economico. Ne sarebbero particolarmente minacciate le imprese economiche e i servizi pubblici. I casi di spionaggio rivelati non vanno considerati come singoli casi isolati; va invece osservata ad esempio la loro affinità dal profilo strutturale. Occorre pertanto un’analisi globale dei casi.

► Temi di attualità a livello internazionale: capitolo 4.1

► Tendenze / prospettive: capitolo 5.1

Complicazione delle disposizioni e delle configurazioni di protezione dei dati presso i servizi Internet

Gli offerenti di apparecchi supportati sulla grande rete, di servizi di comunicazione e di reti sociali su Internet facilitano la vita e offrono agli utenti il vantaggio di potersi collegare e scambiare informazioni più semplicemente. Tramite il rilevamento dei dati statistici le prestazioni di servizi possono essere continuamente migliorate e finanziate da un’offerta pubblicitaria (gratuita) sempre più mirata. Per questo motivo gli offerenti di simili applicazioni vogliono ottenere il maggior numero possibile di informazioni sui loro utenti. Chi intende tutelare la propria sfera privata deve sovente confrontarsi con paginate di parametri di sicurezza poco chiari e spesso non comprende quali siano le conseguenze di quale configurazione.

► Tendenze / prospettive: capitolo 5.3

Sistemi infettati e pagine Web – Le possibilità di MELANI

Nel mese di febbraio sono stati osservate e-mail contenenti software nocivo inviate in maniera mirata a persone del settore pubblico, come pure a istituti di formazione. MELANI ha potuto identificare il Command & Control Server della rete bot e informarne le competenti autorità estere. Questi attacchi non hanno avuto alcun successo in Svizzera.

► Temi di attualità a livello svizzero: capitolo 3.4

Per combattere l’abuso di indirizzi Internet svizzeri e tutelare gli utenti di Internet da un pericolo acuto, nel quadro della revisione dell’ordinanza concernente gli elementi d’indirizzo nel settore delle telecomunicazioni è stata introdotta una nuova disposizione in virtù della quale i nomi di dominio «.ch» possono essere bloccati a determinate condizioni.

► Temi di attualità a livello svizzero: capitolo 3.5

La Centrale d’annuncio e d’analisi per la sicurezza dell’informazione MELANI utilizza dal mese di aprile di quest’anno un checktool che verifica i siti Web CH quanto alla presenza di eventuali infezioni di pagine Web. Da un primo bilancio per i mesi di giugno – agosto 2010 emerge che sono state rintracciate complessivamente 148 pagine Web contenenti infezioni, cifra corrispondente allo 0.6 per mille dei domini CH esaminati.

► Temi di attualità a livello svizzero: capitolo 3.3

2 Introduzione

L'undicesimo rapporto semestrale (gennaio – giugno 2010) della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) spiega le principali tendenze nel campo dei pericoli e dei rischi che accompagnano le tecnologie dell'informazione e della comunicazione (TIC). Esso presenta un compendio degli avvenimenti in Svizzera e all'estero, illustra i principali sviluppi in ambito di prevenzione e presenta in sintesi le attività più importanti degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario** (**capitolo 6**) alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

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

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti della seconda metà del 2009. In merito il capitolo 3 tratta i temi nazionali, il capitolo 4 i temi internazionali.

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

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Comunicazione di lacune di sicurezza

Alcune *lacune di sicurezza* hanno destato in passato l'attenzione dei media, così ad esempio la lacuna di Internet Explorer nel gennaio del 2010. Ma anche le lacune a livello di Adobe Acrobat e di iPhone hanno fatto parlare di sé. Tali lacune di sicurezza sono soprattutto gravi quando non è facile adottare contromisure. A titolo di reazione alla lacuna di sicurezza di diverse versioni di Internet Explorer il Bundesamt für Sicherheit in der Informationstechnik (BSI) tedesco ha pertanto raccomandato nel gennaio del 2010 di non utilizzare per il momento il *browser* di Microsoft e di fare capo a un browser alternativo finché fosse disponibile un *patch*. Il motivo dell'allarme consisteva nel fatto che l'esecuzione di Internet Explorer nel «*modo protetto*» e la disattivazione dell'*Active Scripting* difficoltava gli attacchi, ma non poteva impedirli completamente. Nel BSI la pubblicazione di allarmi è regolata dalla legge e vi sono delle aspettative politiche per quanto attiene l'informazione verso i cittadini in merito alle lacune di sicurezza.

Sia in Germania che in Svizzera esiste un servizio federale di cui si osserva con particolare attenzione quali misure raccomanderà in caso di lacune di sicurezza. L'attenzione rivolta dai media alla raccomandazione del BSI di non più utilizzare Internet Explorer è stata pertanto enorme e ha coinvolto anche i media svizzeri. La difficoltà di una raccomandazione consiste tuttavia nel proporre una variante sicura, ma anche fattibile, a titolo di alternativa. È ovvio che le imprese non possono passare immediatamente a un'altra applicazione browser. Un simile passaggio va pianificato sul lungo tempo. Altrimenti sono garantiti hotline sovraccariche e collaboratori insicuri ed eventualmente innervositi. Nel caso della lacuna LNK del luglio 2010 – una lacuna che sfruttava un errore del Windows Shell nella valutazione dei parametri dei file LNK e PIF – si è ad esempio imposta a numerose imprese la questione se il *workaround* indicato, ovvero l'eliminazione[1] *dei simboli di collegamento*, fosse una soluzione praticabile. Grazie a questa soluzione d'emergenza l'eventuale software nocivo non ha più potuto arrecare alcun danno, ma si è dovuto prendere in considerazione il fatto che la sparizione dei simboli abituali creava forti insicurezze tra i collaboratori. Occorre sempre ponderare quali siano le dimensioni del potenziale di danno e della diffusione di software nocivo specifico e in quale rapporto esse siano con il dispendio per le misure raccomandate. Ogni impresa è in definitiva essa stessa responsabile di questa decisione. In simili casi MELANI cerca di fornire ai gestori di infrastrutture critiche informazioni di fondo che agevolano la presa di siffatte decisioni. Per eseguire un workaround è comunque sempre enormemente importante una buona comunicazione oltre che un rafforzamento del supporto.

MELANI fa in genere prova di riserbo in ambito di avvertimenti pubblici concernenti lacune di sicurezza. A motivo delle numerose lacune di sicurezza dei più diversi programmi ne risulterebbe un intorpidimento della sensibilità degli utenti. L'esperienza insegna altresì che solo un numero esiguo di utenti attua le raccomandazioni indicate, sia perché sono troppo complicate, sia perché sono vincolate a forti limitazioni. Ogni utente di Internet deve pertanto essere consapevole del fatto che tutti i programmi comportano vulnerabilità critiche, a volte anche non ancora di notorietà pubblica, ma già sfruttate. Queste ultime vengono perlopiù utilizzate a scopi di spionaggio e possono arrecare ingenti danni alle imprese e ai Governi.

[1] Successivamente i collegamenti sarebbero ancora sussistiti, ma avrebbero avuto tutti il medesimo aspetto e non avrebbero più potuto essere distinti da simboli diversi.

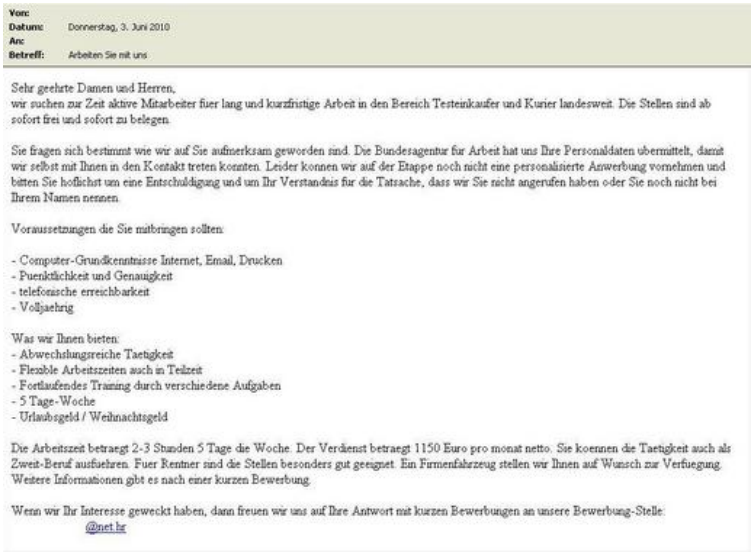
Una protezione di base ben strutturata è quindi imperativa.

Esistono inoltre programmi senza i quali l'attività produttiva quotidiana è impensabile e ai quali non si può o si può solo difficilmente rinunciare. Se un programma del genere è affetto da una lacuna di sicurezza, i rischi di sicurezza possono al massimo essere contrastati con misure di sostegno, formando ad esempio i collaboratori oppure bloccando i server e le e-mail contenenti notoriamente software nocivo. In questo contesto è altresì importante uno scambio di informazioni tra imprese e provider. Un siffatto scambio di informazioni tra gestori di infrastrutture critiche è possibile sulla base della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI. Sono tuttora in fase di test singoli portali analoghi di informazione per le PMI.

3.2 Ricerca di agenti finanziari a scopo di riciclaggio di denaro

Esistono ulteriormente persone che si lasciano indurre a farsi arruolare dai criminali come cosiddetti *«agenti finanziari»*, soprattutto quando il dispendio è minimo e non si esigono speciali qualificazioni: gli agenti finanziari devono disporre di un poco di tempo ogni giorno per farsi versare sul proprio conto denaro da trasferire a un terzo. Una determinata percentuale dell'importo trasferito può essere conservata come provvigione. Gli agenti finanziari, ovvero i corrieri, che si fanno utilizzare per riciclare denaro proveniente da truffe online, sono ricercati dai criminali. Gli agenti finanziari sono rari e possono essere utilizzati per una sola transazione perché in genere sono successivamente sgominati e annunciati all'autorità competente.

Dal mese di giugno 2010 ricompare in Svizzera un numero crescente di e-mail che reclamizzano simili attività di corriere, promettendo condizioni attraenti. Le persone che reagiscono a una siffatta offerta sono in genere rapidamente accreditate sul loro conto di una somma di denaro che devono poi trasferire all'estero, perlopiù per il tramite della ditta di trasferimento di fondi «Western Union». Chiunque collabora a simili «affari» e transazioni corre il rischio di una procedura penale per complicità nel riciclaggio di denaro (art. 305bis CP).



Von:
Datum: Donnerstag, 3. Juni 2010
An:
Betreff: Arbeiten Sie mit uns

Sehr geehrte Damen und Herren,
wir suchen zur Zeit aktive Mitarbeiter fuer lang und kurzfristige Arbeit in den Bereich Testeinkaufer und Kurier landesweit. Die Stellen sind ab sofort frei und sofort zu belegen.

Sie fragen sich bestimmt wie wir auf Sie aufmerksam geworden sind. Die Bundesagentur fur Arbeit hat uns Ihre Personaldaten ubermittelt, damit wir selbst mit Ihnen in den Kontakt treten konnten. Leider konnen wir auf der Etappe noch nicht eine personalisierte Anwerbung vornehmen und bitten Sie hoflichst um eine Entschuldigung und um Ihr Verstandeis fur die Tatsache, dass wir Sie nicht angerufen haben oder Sie noch nicht bei Ihrem Namen nennen.

Voraussetzungen die Sie mitbringen sollten:

- Computer-Grundkenntnisse Internet, Email, Drucken
- Puenktlichkeit und Genauigkeit
- telefonische erreichbarkeit
- Volljaehrig

Was wir Ihnen bieten:
- Abwechslungsreiche Taetigkeit
- Flexible Arbeitszeiten auch in Teilzeit
- Fortlaufendes Training durch verschiedene Aufgaben
- 5 Tage-Woche
- Urlaubsgeld / Weihnachtsgeld

Die Arbeitszeit betraegt 2-3 Stunden 5 Tage die Woche. Der Verdienst betraegt 1150 Euro pro monat netto. Sie koennen die Taetigkeit auch als Zweit-Beruf ausfuehren. Fuer Rentner sind die Stellen besonders gut geeignet. Ein Firmenfahrzeug stellen wir Ihnen auf Wunsch zur Verfuegung. Weitere Informationen gibt es nach einer kurzen Bewerbung.

Wenn wir Ihr Interesse geweckt haben, dann freuen wir uns auf Ihre Antwort mit kurzen Bewerbungen an unsere Bewerbung-Stelle:
@net.hr

Esempio di una e-mail di reclutamento di agenti finanziari

Simili offerte non sono diffuse soltanto tramite e-mail, ma sono reperibili su diverse pagine Internet, accanto a offerte serie di lavoro. Si raccomanda in principio di usare prudenza

quando si deve trasferire a persone sconosciute, mediante trasferimento in contanti, denaro ricevuto (intenzionalmente o per errore) in precedenza. In ogni caso le offerte che fanno balenare forti guadagni vanno considerate con prudenza. Anche su Internet vale in linea di massima la norma secondo la quale non è possibile guadagnare legalmente molto denaro senza un lavoro corrispondente. I propri conti bancari non dovrebbero mai essere messi a disposizione di terzi.

Il fatto che non soltanto i privati abbocchino a simili offerte di lavoro è illustrato dal caso di un collaboratore di un servizio sociale che ha intermediato una simile attività di agente finanziario a un disoccupato. È proprio nel settore dell'assistenza sociale/collocamento che è necessaria una particolare sensibilità a questa tematica perché altrimenti le persone che si trovano già in una situazione difficile sono esposte a un numero ancor maggiore di fastidi.

3.3 MELANI verifica se le pagine Web CH sono infettate

Dal mese di aprile di quest'anno la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI utilizza un tool di controllo che verifica la presenza di eventuali *infezioni di pagine Web* sulle pagine Web svizzere. A tale scopo il *codice sorgente* della pagina Web è verificato quanto alla presenza di firme conosciute, la pagina Web stessa è oggetto di una navigazione regolare e automatica e si analizza successivamente quali azioni sono provocate sul computer. Un elenco definisce le azioni lecite e vietate e fa scattare un allarme a seconda del caso.

Da un primo bilancio per i mesi di giugno – agosto 2010 emerge che sono stati rintracciati complessivamente 148 domini infettati, ciò che corrisponde allo 0.6 per mille dei domini CH verificati:

Domini CH, con pagine Web infettate	148
Domini CH ripuliti	116
Domini CH infettati	32
Totale dei domini CH verificati	237421

Al rilevamento di un'infezione di pagina Web la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ne informa il titolare della pagina Web o il provider, affinché essi possano avviare i passi necessari alla ripulitura. Dal mese di luglio 2010 MELANI dispone anche della possibilità di esigere da SWITCH il blocco di un dominio CH (cfr. il capitolo 3.4). Finora non è stato fatto uso di questa possibilità e anche in futuro MELANI vi ricorrerà soltanto quando tutte le altre misure meno incisive saranno rimaste senza risultato. Dato che le pagine Web in questione sono praticamente quasi tutte oggetto di hacking e che il titolare non è in genere a conoscenza del codice nocivo supplementare sulla sua pagina è possibile rimuovere una simile infezione anche in via bilaterale.

Esistono diverse possibilità di caricare pagine Web manipolate su un server Web. Nel caso della variante più sovente utilizzata si accede al server Web utilizzando dati di accesso FTP derubati. Successivamente si effettua automaticamente il login al conto con questi dati, si scarica una pagina Web (in genere una pagine di indice o un file Javarscript.js disponibile) sulla quale viene immesso clandestinamente il codice nocivo e che viene poi ricaricata. Ulteriori possibilità consistono nello sfruttamento delle vulnerabilità del *Content Management System (CMS)* o delle applicazioni Web installate sulla pagina Web, come pure il *Cross-Site Scripting* nel registri degli ospiti e nei forum. Lo sfruttamento della vulnerabilità dei cosiddetti server Ad, ossia dei server responsabili dell'inserimento di strisce pubblicitarie, costituisce un'ulteriore possibilità, che è al momento in crescita.

Modo di procedere per gli amministratori dopo il rilevamento di un'infezione di pagina Web

In generale: si tenta di infettare il computer del visitatore per il solo fatto della semplice navigazione su questa pagina. Raccomandiamo pertanto di analizzare direttamente il testo sorgente sul server e di non visitare questa pagina Web o di visitarla soltanto applicando le misure di sicurezza corrispondenti (disattivazione di Javascript e ActiveScripting, disattivazione della funzione IFrame, ecc.) fino all'eliminazione dell'infezione.

- Nell'ipotesi che *non sia disponibile alcun CMS e che i dati siano caricati sul server via FTP* la soluzione più semplice è di ricaricare sul server la pagina Web memorizzata localmente. Un'indicazione di quali pagine siano state compromesse può inoltre essere fornita dalla data alla quale la pagina è stata modificata per l'ultima volta. Tale data di modifica è visibile di volta in volta nei programmi FTP. Se nel corso degli ultimi tempi non è stata effettuata alcuna modifica ma la data di modifica fa concludere a una modifica recente questa circostanza costituisce un'indicazione di compromissione della pertinente pagina.
  Al termine è pure importante modificare la password e verificare se sul computer con il quale è amministrata la pagina Web si annida un cavallo di Troia.
- *Se l'amministrazione delle pagine Web è effettuata per il tramite di un CMS* occorre rintracciare dove il codice nocivo si è immesso clandestinamente. Sovente esso si annida in elementi ricorrenti, come l'intestazione o il piè di pagina. Il codice nocivo può però anche essere solidamente programmato nel CMS. Se l'ubicazione del codice nocivo non può essere rilevata e rimossa si raccomanda di ricorrere all'aiuto dello Hosting Provider.
  Importante: occorre assolutamente mantenere aggiornato il CMS e modificare anche in questo ambito i dati di accesso.
- Di recente sono anche stati colpiti con maggiore frequenza da infezioni di pagina Web gli *inserti pubblicitari*. Questi hanno una grande portata perché sono affissi su diverse pagine Web. In questo contesto è stato in particolare recentemente oggetto di attacchi il programma Ad OpenX.
  I server Ad devono assolutamente essere mantenuti aggiornati.

3.4 MELANI scopre una rete bot e inizia il takedown

Nella terza settimana di febbraio MELANI ottenne informazioni a proposito di un attacco mirato perpetrato attraverso l'invio di email infetti. Questi email furono inviati a esponenti del settore pubblico e a istituti di formazione.

Gli email, redatti in lingua inglese, contenevano un documento relativo a una conferenza della NATO che si sarebbe svolta a cavallo tra il 24 e il 25 febbraio 2010, dal titolo "C4I cooperation in South-Eastern Europe (SEE) – the new look". All'apertura di questo file, un codice nocivo infettava il computer rendendolo parte di una rete bot. Le funzioni primarie del codice erano di catturare dati di login per conti email e reti sociali.

Attraverso l'analisi del malware, MELANI è stata in grado di determinare il server di comando (Command- & Control Server), così come una vasta lista di sistemi infettati. Queste informazioni sono state in seguito inviate alle entità competenti in modo che si potesse avviare un take down della rete bot. In Svizzera questo attacco non ha prodotto alcuna vittima.

Nel caso specifico[2] gli email furono inviati a persone che frequentarono i medesimi istituti di formazione. Perché l'attacco fu indirizzato verso queste persone? Potrebbero aprirsi qui due interpretazioni: la prima è quella secondo la quale si voleva mirare queste persone, si è dunque svolto un lavoro di social engineering per raccogliere gli indirizzi delle persone che si volevano spiare. La seconda interpretazione è quella secondo la quale il confine tra crimine online e spionaggio si stia assottigliando. La tecnica qui esposta, l'attacco mirato, era l'esclusiva dello spionaggio. I criminali hanno capito che gli attacchi su larga scala sono sempre meno proficui, giacché producono molto rumore e conseguentemente una reazione più importante da parte di produttori di antivirus, ricercatori, esperti in sicurezza e altro. Gli attacchi silenziosi, sebbene raggiungano meno persone, sono più efficaci.

3.5 Blocco di nomi di dominio «.ch» in caso di sospetto di abuso

Per combattere l'abuso di indirizzi Internet svizzeri e tutelare gli utenti di Internet da gravi pericoli, all'atto della revisione dell'ordinanza del 6 ottobre 1997 concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT, RS 784.104) è stata introdotta una nuova disposizione. Conformemente a questa disposizione il gestore del registro di domini «.ch» (SWITCH) è tenuto a determinate condizioni a bloccare un nome di dominio e a sopprimere la corrispondente attribuzione a un *server di nomi*.
Conformemente al nuovo articolo 14*f* [bis] ORAT[3] un nome di dominio «.ch» può essere bloccato e la corrispondente attribuzione a un server di nomi può essere soppressa. Ne è il caso se sussiste il sospetto fondato che questo nome di dominio venga utilizzato per appropriarsi di dati degni di protezione tramite metodi illegali (cosiddetto *phishing*) oppure per diffondere software dannosi (cosiddetto *malware*). Queste misure devono inoltre essere richieste da un ente di lotta contro la cibercrimininalità riconosciuto dall'Ufficio federale delle comunicazioni (UFCOM). SWITCH può adottare autonomamente misure corrispondenti per la durata di cinque giorni lavorativi al massimo, ma le deve abrogare se non sono state confermate da un ente autorizzato a farne la richiesta.

All'atto del blocco di un nome di dominio si distinguono i seguenti modi di procedere: si impedisce che venga modificata la registrazione nell'infrastruttura amministrativa dell'attribuzione («congelamento» del record di dominio – la pagina Web rimane tuttavia accessibile) oppure si sopprime l'attribuzione a un server di nomi, con la conseguenza che dopo l'aggiornamento del *Domain Name System* (DNS) la pagina Web non può più essere chiamata immettendo il nome di dominio. Quest'ultima misura impedisce unicamente che l'utente di Internet subisca un danno dalla chiamata di questo indirizzo svizzero. I contenuti sui server Web non sono cancellati e gli autori possono sempre utilizzare un altro nome di dominio per accedere a questi contenuti. Si tratta quindi di una piccola misura destinata a migliorare le possibilità di difesa contro i pericoli in ambito di indirizzi Internet svizzeri e di protezione dell'utente di Internet che naviga su pagine Web «.ch».

Dal 15 giugno 2010 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) è un ente riconosciuto in questo ambito dall'Ufficio federale delle comunicazioni

---

[2] Altri casi simili sono stati individuati da altri enti nel corso del primo semestre 2010, come ad esempio l'email inviato a nome dell'Unione Europea dal titolo „Military operation of the EU NAVFOR Somalia" (http://contagiodump.blogspot.com/2010/08/cve-2010-1240-with-zeus-trojan.html), o quello inviato a nome del „National Intelligence Council", dal titolo „2020 Project" (http://krebsonsecurity.com/2010/02/zeus-attack-spoofs-nsa-targets-gov-and-mil/).

[3] http://www.admin.ch/ch/d/sr/784_104/a14bist.html (stato: 27 agosto 2010).

(UFCOM). D'ora in poi MELANI può richiedere a SWITCH il blocco e la soppressione della corrispondente attribuzione a un server di nomi dei nomi di dominio «.ch» in caso di sospetto fondato di phishing o di diffusione di malware.

MELANI farà uso unicamente con molto riserbo di questa possibilità e come ultima risorsa quando il pericolo non potrà essere diversamente bandito. Come già menzionato nell'ultimo rapporto semestrale, attualmente il malware è sovente diffuso per il tramite di pagine Web oggetto di hacking. In questi casi il problema potrà in genere essere risolto mediante presa di contatto con i gestori legittimi della pagina o con lo Hosting Provider. Fin da prima della revisione dell'ORAT MELANI aveva raggiunto numerosi successi con questo modo di procedere informale.

Consecutivamente a una modifica del contratto di registrazione dei nomi di dominio con SWITCH – modifica in virtù della quale un nome di dominio può essere utilizzato soltanto ad avvenuto pagamento degli emolumenti – dal 1° marzo 2009 le registrazioni abusive di nomi di dominio «.ch» sono praticamente sparite nel settore del phishing e fortemente diminuite in quello del malware.

3.6 Il Consiglio federale adotta il messaggio concernente la ratifica della Convenzione sulla cibercriminalità[4]

La Convezione del Consiglio d'Europa del 23 novembre 2001 sulla cibercriminalità[5] è la prima e finora la sola convenzione internazionale che si occupa di criminalità informatica e in rete. Gli Stati aderenti sono tenuti ad adeguare la propria legislazione alle sfide delle nuove tecnologie informatiche; si promuove d'altra parte un'armonizzazione della legislazione in materia di criminalità informatica. Sono inoltre adottate norme di procedura penale (concernenti in particolare il rilevamento delle prove e l'assunzione delle prove provenienti da dati elettronici), mentre la collaborazione tra le diverse Parti contraenti dovrà essere strutturata in maniera rapida ed efficiente quanto ai suoi iter. La Svizzera soddisfa già ampiamente i requisiti della Convenzione[6].

Sussiste altresì una necessità di intervento per quanto riguarda la fattispecie penale dell'accesso illegale a un sistema per l'elaborazione di dati (art. 143bis CP, cosiddetta fattispecie dello «hacking»). In merito si prevede di ampliare l'imputabilità in maniera analoga alla norma penale contro i *virus informatici* (art. 144bis n. 2 CP[7]): si rende colpevole chiunque si procaccia l'accesso a programmi, password o altri dati che sa o deve presumere destinati a penetrare successivamente in maniera illegale in un sistema di computer[8].

---

4 Dossier presso l'Ufficio federale di giustizia: http://www.bj.admin.ch/bj/de/home/themen/kriminalitaet/gesetzgebung/cybercrime__europarat.html (stato: 27 agosto 2010)

5 Convention on Cybercrime, ETS 185: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/ConventionOtherLg_en.asp (stato: 27 agosto 2010)

6 http://www.bj.admin.ch/bj/de/home/dokumentation/medieninformationen/2010/ref_2010-06-181.html (stato: 27 agosto 2010)

7 http://www.admin.ch/ch/d/sr/311_0/a144bis.html (stato: 27 agosto 2010)

8 Formulazione secondo il disegno di decreto federale: http://www.admin.ch/ch/i/ff/2010/4165.pdf (FF 2010 4165) (stato: 27 agosto 2010)

Secondo il messaggio del Consiglio federale[9] la vendita di dispositivi o di dati «*dual use*» continua a essere ammessa a determinate condizioni e se sono adottati determinati provvedimenti. I test di sicurezza sui sistemi informatici, i cosiddetti «vulnerability assessment», eseguiti dal gestore o da un terzo da questi incaricato, così come lo sviluppo di nuovi software a tale scopo sono considerati atti effettuati o predisposti dagli aventi diritto e rimangono impuniti. Non sono punibili le misure adottate per garantire la qualità dei sistemi propri e su incarico di terzi, mentre rimane legale la formazione di specialisti del settore della tecnologia dell'informazione, in cui viene discusso e concretizzato l'impiego di «hacking tools».

Al contrario è punibile (per l'atto in sé e per l'ulteriore utilizzo dei dati) la diffusione intenzionale o irresponsabile di programmi e altri dati, quando il loro contenuto sensibile, la cerchia dei destinatari o altre circostanze fanno apparire evidente l'impiego illecito di tali strumenti. La diffusione irresponsabile di strumenti di hacking tra persone inclini al crimine[10] non deve rimanere impunita. In questo senso permane ulteriormente possibile la «*reasonable disclosure*» in caso di lacune di sicurezza, mentre sarà vietata in futuro la «f*ull disclosure*».

Il disegno di ratifica del Consiglio federale è stato trasmesso al Parlamento e deve ora essere approvato dalle due Camere. La ratifica sottostà inoltre al referendum facoltativo in materia di trattati internazionali.

3.7 Pericolo di abuso conseguente alla dimenticanza di rinnovo di un nome a dominio

Il 10 giugno 2010 le pagine Web del gestore di rete via cavo Cablecom sono state raggiungibili solo limitatamente per un breve periodo. Ne è stata causa il mancato rinnovo del dominio cablecom.net, utilizzato come server di nomi per i servizi di Cablecom. Dopo la scoperta dell'omissione i domini sono stati immediatamente registrati per altri 10 anni.

Ciò che in questo caso non ha avuto gravi ripercussioni e ha provocato al massimo una risata, costituisce un problema che non va sottovalutato e che riguarda tutti i gruppi di imprese, ma anche le persone private che hanno una pagina Web. Esiste un mercato regolare dei nomi di dominio scaduti a prescindere dal mancato rinnovo della registrazione o dall'effettiva mancata utilizzazione dei domini. Costituiscono un problema particolarmente grave le pagine Web delle scuole che dopo essere divenute libere per l'*hosting* sono utilizzate da pagine a doppio senso.

In un altro caso che si è verificato in Svizzera, dopo che il dominio era stato liberato la pagina Web originale è stata copiata e riproposta sulla rete sotto il medesimo dominio. Tuttavia la vecchia pagina Web è stata dotata di diversi complementi, come ad esempio di pubblicità mediante cliccaggio – e vi è pure stato osservato software nocivo. Il vantaggio di questo abuso dei domini (squatter) è evidente: dato che il dominio è già noto esso sarà potenzialmente richiamato da numerosi visitatori. Inoltre molti link si collegano già (rispettivamente ancora) a questa pagina Web. Il danno per l'impresa sono una perdita di reputazione, un dispendio di tempo e di denaro per recuperare i domini, come pure la perdita di clienti potenziali.

[9] http://www.admin.ch/ch/i/ff/2010/4119.pdf (stato: 27 agosto 2010)

[10] Il settore pubblico di Internet deve indubbiamente essere incluso in questo caso.

Ci si scorda anche sovente che tutte le e-mail inviate al dominio precedente possono essere senz'altro lette dal nuovo proprietario del dominio, senza neppure avere bisogno di conoscere l'indirizzo e-mail esatto. Per il tramite della funzione «catch all» tutte le e-mail inviate a un dominio sono captate e trasmesse a un indirizzo centrale.

A tutti i proprietari di domini si applica la regola di badare a rinnovare e anche a pagare tempestivamente i singoli domini[11]. Anche quando un dominio è cessato volontariamente occorre essere consapevoli del fatto che qualsiasi persona con un qualunque modello di affari – sia anche dubbio – può fare affari avvalendosi di questo indirizzo.

3.8 Lo hacking e le sue ripercussioni fisiche sull'esempio dell'automobile

3.8.1 Emittente disturbatrice ad Arbon

L'anno scorso chi parcheggiava il proprio veicolo nella zona sud della città vecchia di Arbon era sovente confrontato con il problema dell'impossibilità di aprire il proprio veicolo a chiusura elettronica. Nel mese di febbraio di quest'anno gli specialisti dell'Ufficio federale delle comunicazioni (UFCOM) hanno potuto rintracciare il problema. Un vecchio altoparlante via radio trasmetteva sulla frequenza utilizzata dalle chiavi delle automobili. Le chiavi radiocomandate delle automobili funzionano nella fascia di frequenza compresa tra 433.0-434.79 MHz, anche denominata *Industrial, Scientific and Medical Band (ISM Band)*[12][13]. In questa fascia di frequenza operano però anche altre applicazioni senza fili, come ad esempio le stazioni radio meteorologiche, gli altoparlanti via radio o gli impianti di cuffie. In questa fascia di frequenza possono anche trasmettere i radioamatori – con una potenza ben superiore a quella della chiavi radiocomandate. Tutte queste applicazioni radio possono fare sì che l'impianto ricevente dell'automobile in attesa del segnale della chiave sia disturbato o non funzioni più.

In questo caso l'interferenza era involontaria. I criminali fanno però uso di questa possibilità di disturbo per scassinare le automobili. Se si invia un segnale di disturbo nel momento esatto in cui si chiude l'automobile e il proprietario del veicolo non controlla se quest'ultimo sia effettivamente chiuso, le porte sono aperte ai criminali, che possono tranquillamente cercare oggetti di valore all'interno dei veicolo.

---

[11] Diversi servizi di registrazione si riservano espressamente la facoltà di liberare i domini in casi di mancato pagamento degli emolumenti. Così facendo essi si risparmiano le spese di una procedura dispendiosa e costosa di diffida.

[12] http://www.bakom.admin.ch/themen/frequenzen/00652/00653/index.html?lang=de (stato: 27 agosto 2010)

[13] http://de.wikipedia.org/wiki/ISM-Band: Sono designate come bande ISM (Industrial, Scientific and Medical Band) le fasce di frequenza che possono essere utilizzate dalle apparecchiature ad alta frequenza dell'industria, del mondo scientifico, della medicina e in ambito domestico e simile. Le apparecchiature ISM corrispondenti come forni a microonde e apparecchiature mediche di radioterapia a onde corte necessitano unicamente di un'omologazione generale. Alcune bande ISM sono ad esempio utilizzate anche per le trasmissioni audio e video o per la trasmissioni di dati via WLAN o Bluetooth, senza che la loro utilizzazione necessiti di un'attribuzione singola di frequenza. Esse non sono però applicazioni ISM e sottostanno a prescrizioni proprie. L'utilizzazione in comune, specialmente nella bande di frequenze sovente utilizzate, come la banda dei 433 MHz e quella dei 2,4 GHz può facilmente provocare interferenze tra le diverse apparecchiature. (stato: 27 agosto 2010)

3.8.2 100 automobili inibite via radio

Un sistema di bloccaggio della messa in moto comandato via telefonia mobile consente di bloccare l'automobile in caso di furto. Questo sistema può anche essere utilizzato sui computer portatili, in modo da poter bloccare a distanza il laptop, cancellarne addirittura i dati e formattare il disco rigido. Tramite la funzione MobileMe fin da oggi è possibile resettare a distanza l'iPhone o l'iPad da qualsiasi computer[14].

Il fatto che nemmeno questi sistemi siano immuni da manipolazioni è ovvio. È quanto è successo proprio negli USA nel corso dell'ultimo semestre. Un ex collaboratore di un autosalone ha paralizzato via Internet oltre 100 veicoli appartenenti alla clientela. Avvalendosi del sistema «Webtech-Plus» utilizzato in questo caso i rivenditori di automobili possono impedire di avviare il motore ai clienti che non pagano puntualmente le rate di finanziamento o di leasing.

Simili prestazioni di servizi, come la gestione centralizzata del blocco della messa in moto o il blocco di accesso di computer mobili o di telefoni mobili saranno vieppiù offerte in futuro. Sebbene siano di per sé una buona cosa e significhino un vantaggio in termini di sicurezza, questi servizi celano anche alcuni pericoli perché questi tool sono comandati a livello centrale. Sono quindi possibili manipolazioni aventi grandi ripercussioni. Come illustrato dall'esempio qui sopra non si tratta in ogni caso di un hacking del sistema, ma di un collaboratore o di un ex collaboratore che manipola intenzionalmente o con un comportamento errato il sistema.

3.8.3 Manipolazione di automobili moderne

Nella automobili moderne è integrata una quantità sempre maggiore di elettronica. Pressoché tutto il controllo è gestito dal sistema di bordo. Non meraviglia quindi che un'automobile possa divenire esposta agli attacchi degli hacker. Per il momento si tratta ancora di un'utopia. Ciononostante nel corso dell'ultimo semestre ricercatori delle università americane hanno dimostrato come ci si possa introdurre nel sistema di bordo di un'automobile in corsa e assumerne il controllo. In questo caso si impedisce ad esempio al conducente di azionare i freni, rispettivamente di avviare o di spegnere il motore. La sola cosa che non poté essere ripresa fu lo sterzo perché in questo caso esso funzionava ancora meccanicamente.

Dato che le automobili attuali non dispongono ancora di un collegamento radio al sistema di bordo, nel caso di questo test si è reso necessario un collegamento via cavo all'automobile, ovvero il manipolatore doveva essere seduto lui stesso nel veicolo oppure un simile collegamento radio doveva dapprima essere installato manualmente. Ma se in futuro i sistemi di bordo fossero collegati a Internet sarebbe aperta la porta alle manipolazioni.

3.9 La Svizzera dispone ora di identità digitali (SuisseID)

Con la «legge federale del 19 dicembre 2003 sui servizi di certificazione nel campo della firma elettronica» (Legge sulla firma elettronica, FiEle; RS 943.03)[15] è stato istituita in Svizzera la base legale per offrire servizi di certificazione nel settore della *firma elettronica* e riconoscerli a livello statale. Dato che i certificati conformi alla FiEle possono essere utilizzati

[14] http://www.apple.com/mobileme/features/find-my-iphone.html (stato: 27 agosto 2010)

[15] http://www.admin.ch/ch/d/sr/c943_03.html (stato: 27 agosto 2010)

unicamente per le firme elettroniche qualificate, nel quadro di una SuisseID questi certificati sono rilasciati unitamente a un certificato che può anche essere utilizzato ai fini di autentificazione e quindi come documento elettronico standardizzato di identità. Diviene così possibile accedere alle offerte di tutta una serie di offerenti di prestazioni di servizi online e comprovare senza dubbi nei loro confronti di essere la persona che pretendiamo di essere. Oltre che da alcuni offerenti privati l'utilizzo della SuisseID è per il momento accettato dai seguenti uffici federali: Ufficio federale di giustizia (portale del casellario giudiziale), Regìa federale degli alcool (richieste di distillazione e annuncio di quantitativi di produzione e di vendita in vista della tassazione), Amministrazione federale delle contribuzioni (diversi servizi in ambito di imposta sul valore aggiunto) e Amministrazione federale delle dogane (rimborsi e verifiche d'esercizio).

Fino a fine 2010 (rispettivamente fino a esaurimento delle scorte) la Confederazione sovvenziona in ragione di 65.-- franchi l'acquisto a titolo privato di una SuisseID (Smartcard o chiavetta USB) e intende promuovere per questo tramite la diffusione della SuisseID.

Al momento non esistono studi su eventuali rischi di sicurezza relativi alla SuisseID. La tecnologia utilizzata corrisponde tuttavia agli standard attuali generalmente riconosciuti. Potrebbero nondimeno risultare dei rischi dal fatto che la SuisseID riunisce in un unico chip l'autentificazione e la firma digitale qualificata. Questo ad esempio se il titolare della SuisseID utilizza per motivi di comodità il medesimo *codice PIN* sia per l'autentificazione, sia per l'apposizione di una firma legalmente valida. Come nel caso di ogni altra tecnologia di sicurezza il comportamento di utilizzazione deve essere integrato in un approccio globale. Nonostante legislazioni progredite le firme elettroniche qualificate non sono finora riuscite a farsi strada e ad affermarsi nella prassi né a livello nazionale, né a livello internazionale. Occorre attendere per sapere se la SuisseID avrà dato il giusto impulso in merito.

3.10 Necessità di un miglioramento dell'identificazione degli utenti mobili di Internet

Con la rapida proliferazione degli smartphone e degli accessi mobili a Internet è fortemente aumentato il volume dei collegamenti a Internet. Affinché non sia necessario un proprio *indirizzo IP* per ogni apparecchiatura, gli offerenti di telefonia mobile puntano sulla Network-Address-Port-Translation (NAPT). In questo senso parecchie migliaia di utenti utilizzano il medesimo indirizzo IP ma *porte* diverse. Per identificare un collegamento e il suo utente sono tipicamente necessari l'indirizzo IP, la data e l'ora. Questi dati sono peraltro memorizzati regolarmente nei file di log dei servizi Web. Per identificare un utente mobile dovrebbe essere noto anche il numero della porta. Questo dato viene però registrato raramente. Da questo punto di vista va anche preso in considerazione l'obbligo di registrazione delle carte prepagate *wireless* postulato dal Parlamento[16]. Va pure caldeggiato l'obbligo anch'esso postulato di garantire un'identificazione del partecipante anche all'interno delle reti private (ossia dietro un unico indirizzo IP), ma non va perso di vista che a seconda delle circostanze è necessario all'identificazione un numero maggiore di dati di quello normalmente disponibile. Si terrà conto di questa circostanza nel quadro della revisione in corso[17] della legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) [18] e nella struttura delle relative

[16] http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20073627 (stato: 27 agosto 2010)

[17] http://www.bj.admin.ch/bj/de/home/themen/sicherheit/gesetzgebung/fernmeldeueberwachung.html (stato: 27 agosto 2010)

[18] http://www.admin.ch/ch/d/sr/c780_1.html (stato: 27 agosto 2010)

disposizioni di esecuzione.

3.11 Hacker molestano l'UDC e l'Unione europea

A fine 2009/inizio 2010 la pagina Web della sezione UDC della Città di Zurigo è stata deturpata a più riprese. Vi è apparsa la scritta «26C3 - Here be Dragons». Vi è anche stato inserito un video YouTube con riferimento all'iniziativa concernente il divieto di costruzione di minareti. Il video si rifà alla pubblicità di un produttore svizzero di caramelle alle erbe, conosciuto con lo slogan pubblicitario «Chi le ha inventate?». «Here be Dragons» era lo slogan del 26° congresso del Chaos Computerclub (CCC) a Berlino. Il congresso in questione si svolge ogni volta tra Natale e Capodanno e attira fino a 3000 hacker, geek, artisti in rete, protettori dei dati ecc. Dopo essere stata ripristinata, la pagina Web è stata nuovamente deturpata, questa volta con un video scherzoso intitolato «300 – SVP must die», inspirato al film «300». Si ritiene che per procedere a questo deturpamento sia stata sfruttata una lacuna del Content Management System.

Screenshot della pagina compromessa dell'UDC[19].

Già immediatamente dopo l'iniziativa sul divieto della costruzione di minareti sono state oggetto di hacking oltre 5000 pagine, fra le quali quelle dei partiti UDC locali e dei giovani UDC. Dietro questi attacchi si presumono però autori provenienti prevalentemente dallo spazio turco. In questo caso gli aggressori dovrebbero provenire dallo spazio germanico o svizzero tedesco ed essere partecipanti al congresso del CCC. La pagina Web è comunque stata elencata come obiettivo del CCC. Non è però ancora noto chi si celi dietro questo attacco. Non è stata sporta alcuna querela penale.

Un altro caso ha fatto titoli cubitali nel gennaio del 2010 Una lacuna del *cross site scripting* della pagina Web della presidenza spagnola dell'Unione europea «www.eu2010.es» ha consentito per il tramite di un link predisposto di sostituire la fotografia del presidente Zapatero sulla pagina frontale del sito Web con una fotografia del comico Rowan Atkinson (alias Mr. Bean)[20]. Questo Script-Inject, che ha scaricato la fotografia di Mr. Bean da un altro server, è stato presumibilmente immesso clandestinamente attraverso la funzione di ricerca della pagina. Il link così predisposto è stato distribuito su più canali. In considerazione della sua forte risonanza la pagina ha attirato una folla di curiosi.

---

[19] Fonte: http://yfrog.com/j5svpp (stato: 27 agosto 2010)

[20] http://www.la-moncloa.es/IDIOMAS/9/ActualidadHome/2009-2/04012010_AttackOnSpanishEuPresidencyWebsite_Communique.htm (stato: 27 agosto 2010)

Screenshot dopo la chiamata del link predisposto.

Nel caso di un attacco cross site scripting (XSS) il server Web non è oggetto di un attacco in senso vero e proprio. Lo si sfrutta abusivamente soltanto per introdurre clandestinamente un contenuto estraneo sulla pagina Web attraverso il browser dell'utente. La pagina Web vera e propria non è modificata. Nella maggior parte dei casi questo metodo è utilizzato per accedere ai dati di login e di carte di credito, introducendo una pagina di phishing in un indirizzo Web degno di fiducia. Questa funzionalità errata è causata da una cattiva o mancata verifica dei campo di immissione. Se nel caso ad esempio di un campo interattivo non viene filtrato il *codice HTML* della funzione di ricerca di una pagina Web, la pagina dei risultati viene interpretata dal browser. Vi si possono pertanto introdurre clandestinamente immagini, ma anche formulari completi. Lo XSS fa parte delle più frequenti procedure di attacco al Web.

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Florilegio di casi di spionaggio nel semestre 1/2010

Nel corso dell'ultimo semestre sono stati resi noti alcuni casi di spionaggio, come ad esempio quelli ai danni di Google, di Adobe e dell'ufficio del Dalai Lama. Thomas de Maizière, il ministro germanico degli interni, ha messo in guardia nel recente rapporto sulla tutela della Costituzione contro il pericolo di un crescente spionaggio economico. Ne sarebbero particolarmente minacciate le imprese economiche e i servizi pubblici. Il Bundesamt für Verfassungsschutz ha classificato come molto elevato il pericolo di spionaggio industriale in Germania da parte della Russia e della Cina[21]. I casi di spionaggio rivelati non vanno considerati come singoli casi isolati; va invece osservata ad esempio la loro affinità dal profilo strutturale. Il capitolo 5 ne dà ulteriori chiarimenti.

4.1.1 Google annuncia ciberattacchi

All'inizio dell'anno Google ha reso noto di essere vittima di attacchi mirati di hacking. Sembra che nel medesimo caso siano anche state colpite imprese dei settori di Internet, della finanza

[21] Rapporto 2009 sulla tutela della Costituzione in Germania: http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2009/ (stato: 27 agosto 2010)

e militare. Secondo le dichiarazioni di Google gli attacchi sono stati perpetrati nel periodo dal 9 dicembre al 10 gennaio e sono stati diretti contro Google e almeno una ventina di altre imprese. Questi attacchi di hacking sarebbero stati estremamente sviluppati e mirati. Nel caso di Google l'attacco sarebbe stato soprattutto diretto contro i conti di Google-Mail. Al centro dell'attacco sarebbero stati i conti di attivisti cinesi dei diritti dell'uomo. Gli hacker non sarebbero però riusciti ad accedere a dati sensibili. In due casi, come risulta dalle ricerche di Google, gli hacker sarebbero almeno riusciti a visualizzare la posta in entrata. I contenuti delle e-mail non avrebbero tuttavia potuto essere richiamati. Si sarebbe inoltre constatato che alcuni conti Google-Mail di attivisti statunitensi, europei e cinesi dei diritti dell'uomo sarebbero spiati da lungo tempo. Non vi si sarebbe acceduto con l'ausilio di software nocivo, bensì mediante *phishing* nei confronti dei titolari dei conti.

Le e-mail sono inoltre sovente inviate alle imprese e ai servizi pubblici unitamente a file PDF appositamente predisposti. Una ditta svizzera ha ad esempio ricevuto documenti PDF contenenti codice nocivo inviati in maniera mirata. In questo caso sarebbe stata sfruttata una lacuna di sicurezza già pubblicata il 15 dicembre 2009, ma colmata soltanto all'inizio di gennaio del 2010. Si constata che diversamente da quanto accadeva in precedenza nel caso di attacchi mirati di hacking si ricorre perlopiù a file PDF piuttosto che a documenti Office.

Gli attacchi di questo genere sono noti da lungo tempo e variamente documentati: rinviamo ad esempio al «Tracking Ghostnet» del marzo 2009[22] o allo studio della ditta Northrop per la US-China Economic and Security Review Commission dell'ottobre 2009 («Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation»)[23]. L'attacco annunciato da Google è tecnicamente maturo, ma dal profilo della sua complessità tecnica può essere paragonato ad esempio all'attacco al DFAE.

4.1.2 «Shadows in the Cloud»: rete cinese di spionaggio

Il 6 aprile 2010 i gruppi «Information Warfare Monitor» e «Shadowserver Foundation» hanno pubblicato un rapporto intitolato «Shadows in the Cloud»[24]. Il rapporto tratta della attività di spionaggio ai danni di ONG tibetane e dell'ufficio del Dalai Lama eseguite con l'ausilio di mezzi TIC. Dopo il «Tracking Ghostnet – Investigating a Cyber Espionnage Network» questo è il secondo rapporto di questi autori su possibili attività cinesi di spionaggio ai danni di obiettivi corrispondenti.

Fin dal 2005 il New York Times aveva pubblicato un rapporto del FBI relativo a un'operazione denominata «Titan Rain». In questo caso si trattava di sistemi di computer infettati delle autorità US dai quali erano stati prelevati documenti e informazioni su un lungo periodo di tempo. Come possibile autore era stata additata la Cina. Anche in Svizzera si sono verificati da allora simili attacchi ai danni dell'industria dell'armamento e di servizi del Governo. In questi casi gli aggressori hanno inviato documenti appositamente predisposti sotto il nome di un falso mittente a persone chiave delle pertinenti imprese. Le informazioni erano confezionate su misura per i destinatari, circostanza che presupponeva il procacciamento preliminare di informazioni da parte dei servizi segreti.

Il rapporto in questione è un complemento in base agli accertamenti nel caso «GhostNet».

---

[22] Tracking Ghostnet: http://www.tracking-ghost.net (stato: 27 agosto 2010)

[23] Studio Northrop: http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (stato: 27 agosto 2010)

[24] Shadows in the Cloud - http://shadows-in-the-cloud.net/ (stato: 27 agosto 2010)

Gli scienziati hanno scoperto che su alcuni dei computer infettati era stato installato anche altro malware. Ciò ha condotto alla scoperta di un'ulteriore rete di spionaggio. È stato possibile identificare vittime in oltre 36 Paesi; la maggior parte delle persone colpite si trovano in India. Secondo il rapporto sono stati individuati 115 sistemi di computer colpiti in Svizzera. Non ne sono invece state toccate imprese di maggiori dimensioni e gestori di infrastrutture critiche di informazione.

4.1.3 La bella amica su Facebook dei soldati di élite

In numerosi Paesi le *reti sociali* si rivelano un rischio di sicurezza per gli eserciti. I soldati comunicano via Internet le più svariate informazioni e non è raro che forniscano indicazioni utili ai loro avversari. Le campagne di sensibilizzazione possono neutralizzare solo in maniera limitata questa problematica mentre i divieti sono talvolta controproducenti[25].

All'inizio dell'anno un soldato israeliano ha annunciato su Facebook l'ultimo ingaggio della sua unità prima del congedo a domicilio, indicandone il giorno e il villaggio in Cisgiordania. Questo ha avuto per conseguenza l'annullamento del piano di operazione e il rinvio del soldato colpevole dinanzi al tribunale[26].

Poco tempo dopo è stato reso noto che una splendida giovane ragazza aveva fatto amicizia col soldato su Facebook e gli aveva carpito i suoi segreti. Secondo un comunicato stampa oltre 200 soldati di élite sono incappati in questa trappola[27]. Sotto il falso profilo si cela presumibilmente la milizia sciita libanese Hezbollah.

Si può speculare se questa storia sia vera o se faccia soltanto parte di una vasta campagna di sensibilizzazione dell'esercito[28]. D'altra parte si rimprovera a Israele di procurarsi esso stesso informatori tra le file dei suoi nemici con l'aiuto di Internet e delle reti sociali[29].

4.2 La conferenza tedesca dei ministri dell'interno pianifica misure contro la cibercriminalità

Gli scorsi 27 e 28 maggio 2010 si è riunita per la sua seduta primaverile la Conferenza tedesca dei ministri degli interni e dei senatori dei Länder (IMK). Alla vigilia il presidente della Conferenza, il senatore degli interni di Amburgo Akthaus, aveva annunciato alla stampa che l'IMK intendeva varare un pacchetto di misure per far fronte alla crescente minaccia da parte

---

[25] http://news.bbc.co.uk/2/hi/8540236.stm; http://www.scmagazineus.com/army-ends-ban-on-facebook-flickr-other-social-media-sites/article/138392/; http://www.computerworld.com/s/article/9136255/Marines_solidify_ban_on_Facebook_Twitter; http://www.marinecorpstimes.com/news/2010/02/military_socialmedia_update_022610w/ (stato: 27 agosto 2010)

[26] http://computer.t-online.de/israel-facebook-eintrag-verhindert-militaeraktion/id_40993294/index; http://www.sueddeutsche.de/digital/israel-dank-facebook-nachricht-im-militaergefaengnis-1.15999; http://news.bbc.co.uk/2/hi/middle_east/8549099.stm (stato: 27 agosto 2010)

[27] http://www.blick.ch/news/ausland/soldaten-ueber-facebook-ausspioniert-147053; http://www.spiegel.de/politik/ausland/0,1518,694582,00.html (stato: 27 agosto 2010)

[28] http://www.independent.co.uk/news/world/middle-east/israel-warns-of-facebook-spies-1687139.html; http://news.bbc.co.uk/2/hi/7343238.stm (stato: 27 agosto 2010)

[29] http://www.theregister.co.uk/2010/04/07/facebook_spying_gaza/; http://news.bbc.co.uk/2/hi/middle_east/8585775.stm (stato: 27 agosto 2010)

della criminalità in rete. In merito sarebbe previsto un servizio centrale Internet verso il quale sarebbero convogliate tutte le informazioni dello Stato federale e dei Länder. Oltre a specialisti delle autorità di sicurezza vi sarebbero anche rappresentati esperti del settore Internet. In una seconda fase verrebbe istituito un corrispondente servizio internazionale di emergenza. Si dovrebbe inoltre promuovere a livello di UE un obbligo di comunicazione degli attacchi di hacker, di nuovi tipi di virus e di serie di truffe sulla rete. D'altra parte i ministri degli interni pianificano nel senso di un approccio preventivo una vasta campagna di informazione sui rischi di Internet. Una campagna corrispondente è già stata avviata ad Amburgo alla fine del mese di aprile.

L'IMK ha posto mano all'attuazione della decisione presa dal suo competente gruppo di lavoro in merito al rapporto «Strategie zur Bekämpfung der Informations- und Kommunikations-Kriminalität» e dei passi intrapresi da tale gruppo di lavoro in vista dell'esame ed eventualmente dell'attuazione delle raccomandazioni di intervento contenute nel rapporto.

La minaccia in provenienza dal fenomeno della cibercriminalità costituisce attualmente una delle principali sfide nella lotta e nella prevenzione contro il crimine. Dato che l'approccio prevalentemente perseguito finora, ossia quello di un miglioramento della collaborazione tra le singole forze regionali e nazionali di polizia, non ha raggiunto i successi promessi, si esaminano ora percorsi alternativi. La cibercriminalità non si ferma alle frontiere dello Stato e le vittime di un reato si trovano sovente in luoghi diversi. Conoscenze approfondite della situazione attuale, una visione d'insieme degli eventi concreti, come pure una coordinazione delle risorse disponibili sono imprescindibili ai fini di un perseguimento penale efficiente. Si muove in questa direzione anche la Commissione dell'UE, che prospetta l'istituzione di un'unità di polizia operante contro la cibercriminalità a livello europeo.

Le autorità del perseguimento penale devono collaborare in seno a partenariati pubblico-privato con l'economia privata, gli utenti di Internet, le associazioni delle vittime per tracciare un quadro possibilmente preciso della situazione, tutelare gli utenti e perseguire i criminali. In ambito di cibercriminalità i metodi usuali di inchiesta e di assunzione delle prove della polizia sono applicabili soltanto in maniera limitata. Una lotta efficace esige anche una prevenzione mediante la sensibilizzazione e l'informazione dei cittadini, delle istituzioni e delle organizzazioni.

4.3 Carte EC ovvero il bug 2010

Sono passati dieci anni da quando il mondo intero si chiedeva con ansia se i computer avessero potuto superare senza danni il cambiamento di secolo. La problematica del 2000 ha tenuto col fiato sospeso alcuni produttori di software e di hardware, ma alla fine non è successo niente, tutto si è svolto senza problemi. Dieci anni dopo si è però manifestato un problema di data completamente inaspettato: a contare dal 1° gennaio 2010 i distributori automatici tedeschi di denaro e i terminali del commercio al dettaglio hanno incontrato problemi con l'elaborazione dei cosiddetti *chip EMV*. In seguito a un errore di programmazione la cifra dell'anno 2010 non ha potuto essere elaborata correttamente. Si stima che ne siano state colpite circa 30 milioni di carte. Il produttore francese Gemalto ha riconosciuto l'errore. Affinché le carte potessero nuovamente funzionare entro tempi brevi i distributori automatici e i terminali di pagamento sono stati riprogrammati in maniera tale che alla lettura della carta si potesse nuovamente accedere esclusivamente ai dati integrati nella striscia magnetica. Dato che questa riprogrammazione non è stata effettuata all'estero, alcuni utenti ingegnosi hanno avuto l'idea di ricoprire il chip con un nastro adesivo per forzare un ripiego sulla striscia magnetica. Questo metodo comportava però anche il potenziale di distruggere l'apparecchio di lettura.

Per impedire una sostituzione costosa delle carte si è provveduto alla riprogrammazione e alla riparazione del software del chip sui distributori automatici e su speciali apparecchi di lettura delle carte. A tale scopo il software sulla carta deve dapprima essere liberato per il tramite di una chiave segreta. Questa chiave è trasmessa su un canale sicuro al distributore automatico. Diversamente dalla striscia magnetica il chip può essere protetto efficacemente contro la duplicazione e impedisce il cosiddetto skimming.

Nel caso di questo modo di procedere si è criticato il fatto che al momento in cui si è verificata questa avaria non siano stati consultati né il Bundesamt für Sicherheit in der Informationstechnik (BSI), né la Finanzmarktaufsicht (BaFin). [30]

Un'importante caratteristica delle carte a chip è costituita dal fatto che dopo l'installazione del software non dovrebbero di per sé essere possibili modifiche successive. Le carte a chip possono invero essere modificate, seppure con un grande dispendio. A tale scopo è prevista una chiave di riprogrammazione. Ciò non pone soltanto la questione di un'adeguata cifratura e sicurezza tra la banca e il cliente finale, ma anche la questione generale di chi possiede questa chiave e di tutto ciò che può essere fatto con la carta di credito da chi possiede la chiave.

4.4 Mariposa

A cavallo tra il 2009 e il 2010 il gruppo Defence Intelligence[31] ha individuato una rete bot che attraverso le analisi che si sono susseguite, è risultata essere una delle reti più estese mai scoperte. Un *sinkhole* effettuato tra dicembre 2009 e febbraio 2010 ha dato la possibilità di registrare 11 milioni di indirizzi IP unici. Il nome Mariposa ("farfalla" in spagnolo) è stato dato alla rete in quanto per la creazione del botnet è stato utilizzato il malware kit Butterfly. L'utilizzo del termine in spagnolo è dovuto al fatto che gli operatori della rete sono risultati essere spagnoli.

Scopo principale della botnet è stato quello di rubare dati sensibili salvati sui computer infettati: informazioni su conti, nomi di utenti, password e dettagli sui conti bancari online. Su una parte dei computer infettati veniva in aggiunta scaricato un malware per effettuare attacchi di DDoS (distribute denial of service). Vittime di questa rete sono stati i clienti delle 40 maggiori banche mondiali e computer all'interno di almeno la metà delle imprese Fortune 1'000. Le vittime si trovavano sparse in 190 Paesi.

Il malware kit Butterfly è stato scritto da un hacker di nome Iserdo. Il giovane di 23 anni è stato recentemente arrestato a Maribor, in Slovenia[32]. I *botherder* invece sono stati arrestati ad inizio anno in Spagna. L'azione condotta dalla Guardia Civil[33] ha portato all'arresto di tre cittadini spagnoli, identificati con lo pseudonimo usato in rete e l'età: Netkairo, 31, Johnny Loleante, 30, e Ostiator, 25.

La giustizia spagnola si è comunque ritrovata a dover fare i conti con il codice penale del proprio paese. Infatti secondo il capitano Cesar Lorenzana[34], vice capo della divisione

[30] http://www.faz.net/s/Rub645F7F43865344D198A672E313F3D2C3/Doc~EB6DD9EEC40AA4E1FB4EB70152FD024D2~ATpl~Ecommon~Sspezial.html (stato: 27 agosto 2010)

[31] http://defintel.com

[32] http://www.theregister.co.uk/2010/07/28/mariposa_vxer_ciffed/

[33] Oltre alle forze dell'ordine si era costituito il "Mariposa Working Group", che era composto da Defence Intelligence, Panda Security, Neustar, Directi, Georgia Tech Information Security Center e altri ricercatori.

[34] http://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/

crimine tecnologico della Guardia Civil, in Spagna non è reato possedere e gestire una rete bot o distribuire codice nocivo. L'unico capo d'accusa imputabile sarebbe quello di furto di dati.

Aneddoto curioso in questa vicenda. Due mesi dopo il loro arresto, due degli esercenti di Mariposa, Netkairo e Ostiator, si sono presentati negli uffici di Panda Security, uno dei membri del Mariposa Working Group, per cercare lavoro. Presentarsi con un biglietto da visita come esercente di rete bot non è forse stata la strategia migliore per ottenere un posto di lavoro.

4.5 Google raccoglie per errore dati di utenza del WLAN

Durante le sue carrellate per Google Street View, Google ha anche registrato *dati WLAN*. In merito Google non si è limitato agli *indirizzi MAC* e agli *SSID* dei router WLAN, ma ha registrato anche i dati di utenza trasmessi. Per dati di utenza si intende il traffico generale in Internet, trasmesso da e a un router wireless, ma a tal fine il traffico dei dati non deve essere cifrato. Se ne è il caso si possono leggere in chiaro le password.

Un sviluppatore di software di Google ha integrato la registrazione di dati di utenza nel software di registrazione video di Street View. Ciò costituisce una violazione delle norme di protezione dei dati interne all'impresa. Lo sviluppatore è ora esposto alle conseguenza del suo atto. Il Ministero pubblico di Amburgo ha inoltre avviato il 19 maggio 2010 una procedura di inchiesta per raccolta di dati nei confronti di Google.

È un fatto indiscutibile: chi esercita un router WLAN deve cifrarlo sufficientemente perché altrimenti corre il rischio che un terzo qualsiasi registri i dati o abusi del router a scopi criminali. Non fa alcuna differenza il fatto che in questo caso i dati di utenza vengano raccolti sistematicamente. Ma un'impresa che fa soldi con informazioni pubbliche e personali assume per l'appunto una responsabilità particolare in questo contesto. Sono in particolare necessarie una comunicazione aperta e chiare direttive ai collaboratori sulle modalità di gestione dai dati.

Ma anche in presenza di chiare direttive ci si dovrà vieppiù porre la questione in futuro di ciò che è accessibile al pubblico e di ciò che è privato. Questo passaggio è sempre più fluido e non si ferma al recinto di casa. Questa discussione deve essere fatta e non soltanto da quando Google Street View – ma anche Facebook, Twitter e compagnia vi forniscono la loro parte di contributo. Nel caso di tutti questi servizi si esige da parte dell'utente un'elevata competenza in termini di informazione che esso in parte non possiede (ancora).

4.6 Una sola banda è responsabile dei due terzi di tutti gli attacchi di phishing

Secondo l'ultimo rapporto trimestrale del 2009[35] dell'Anti Phishing Working Group (APWG), la rete bot "Avalanche" è stata responsabile del 66% di tutti gli attacchi di phishing registrati negli ultimi sei mesi. Dietro il nome Avalanche si cela una delle più importanti gang operanti nel settore del phishing. Attraverso la rete bot, la gang ha ospitato i due terzi di pagine di phishing registrate nel secondo semestre del 2009 (84'250 su 126'697).

[35] http://www.apwg.org/reports/apwg_report_Q4_2009.pdf

Alcuni esperti di sicurezza credono che dietro alla rete bot Avalanche vi sia lo stesso gruppo criminale chiamato Rock Phish[36]. Le tecniche usate dalle due gang sono simili: la registrazione regolare dei nomi a dominio, l'uso di tecniche quali il fast-flux e l'inserimento di 6 siti per ogni nome a dominio. Avalanche fu visto per la prima volta sul finire del 2008, periodo durante il quale Rock Phish era scomparso dalla scena. Secondo il rapporto di APWG, Avalanche usa la stessa tecnica di Rock Phish ma migliorata e più sofisticata.

4.7 Avaria del dominio «.de»

Il 12 maggio 2010 un'*avaria DNS* a livello di domini top level presso il servizio tedesco di registrazione DENIC ha avuto per effetto l'impossibilità parziale di accedere alle pagine Web «.de». In quanto servizio centrale di registrazione DENIC gestisce oltre 13 milioni di domini[37]. I domini top level di altri Paesi e i domini come «.com» o «.net» non ne sono stati toccati, sebbene la dipendenza dei diversi servizi possa aver causato avarie anche al di là della Germania. Ne è in particolare il caso allorquando le pagine «.com» sono proposte per il tramite di server DNS «.de». Si specula che l'avaria sia connessa al trasloco del servizio di registrazione da Amsterdam a Francoforte. L'avaria di un servizio DNS non colpisce però soltanto la navigazione sul World Wide Web ma, circostanza più grave, l'infrastruttura e-mail perché le e-mail non raggiungono più i loro destinatari.

I server DNS svolgono un ruolo importante in Internet, se non il ruolo più importante. Essi costituiscono l'anello di congiunzione tra gli indirizzi IP, compresi dai computer, e i nomi di dominio che l'uomo può semplicemente annotarsi. Questa circostanza è stata osservata anche dai criminali, ragione per la quale dirigono attacchi DDoS efficaci direttamente contro i server di nomi, rendendo quindi irraggiungibili tutte le pagine Web proposte per il tramite di questi server DNS. Attualmente non esistono possibilità di difendersi da questi attacchi. Un altro scenario è costituito dalla manipolazione delle chiamate DNS. In questo contesto la vittima che immette correttamente un indirizzo Web è ad esempio dirottata su un server manipolato: si tratta del cosiddetto DNS spoofing.

4.8 L'introduzione della conservazione dei dati ai fini di prevenzione viola la legge fondamentale tedesca

Conformemente alla legislazione più recente gli offerenti di servizi di telecomunicazione in Germania sono tenuti a registrare tutti i dati necessari a ricostruire chi, quando, per quanto tempo, con chi, da dove comunica o ha tentato di comunicare. Non possono invece essere registrati il contenuto della comunicazione e le pagine Internet chiamate dall'utente. La Corte costituzionale germanica (BVerfG) ha statuito con sentenza del 2 marzo 2010 (1 BvR 256/08)[38] che nella forma introdotta le disposizioni controverse relative alla *conservazione dei dati ai fini di prevenzione*[39] violano la legge fondamentale (tale è il nome della Costituzione germanica) e sono quindi nulle.

---

[36] Per saperne di più sul gruppo RockPhish si può consultare il rapporto semestrale 2006/II di MELANI (http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=de)

[37] http://www.heise.de/netze/meldung/DNS-Fehler-legen-Domain-de-lahm-3-Update-999068.html (stato: 27 agosto 2010)

[38] http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (stato: 27 agosto 2010)

[39] §§ 113*a* e 113*b* TKG (Telekommunikationsgesetz) e § 100*g* StPO (Strafprozessordnung).

Secondo la BVerfG la conservazione dei dati ai fini di prevenzione non è in linea di massima anticostituzionale – ma deve essere strutturata nell'osservanza del principio di proporzionalità: occorre effettuare una limitazione sufficiente degli scopi di utilizzazione dei dati e si deve garantire la sicurezza dei dati presso l'impresa che li conserva. Sono inoltre necessarie regolamentazioni con norme chiare per quanto riguarda la trasparenza della trasmissione dei dati e la protezione giuridica. La Corte non ha quindi respinto la conservazione dei dati ai fini di prevenzione, ma unicamente censurato la sua attuazione.

La memorizzazione dei dati a prescindere dall'evento – che consente di attribuire un indirizzo IP al titolare di un collegamento Internet – può senz'altro essere costituzionale. Questi dati tuttavia non possono essere utilizzati illimitatamente. Il legislatore deve disciplinare i diritti di informazione dell'autorità. Ora il Governo federale deve migliorare la legge e introdurvi norme conformi alla legge fondamentale.

In Svizzera le norme relative alla conservazione e all'edizione dei dati da parte degli offerenti di servizi di telecomunicazione figurano nella legge sulle telecomunicazioni[40], nell'ordinanza sui servizi di telecomunicazione[41] nonché nella legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni[42] e nella pertinente ordinanza[43]. La legislazione sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni è attualmente in fase di revisione[44].

4.9 Attacco hacker allo scambio di quote di emissioni / Carpiti i dati di accesso di imprese

Il commercio di cosiddetti certificati di emissione è un importante strumento di riduzione delle emissioni inquinanti. Le regole dell'economia di mercato devono indurre le economie pubbliche e le singole imprese a produrre di volta in volta sempre meno emissioni consecutive alla combustione di agenti energetici fossili: i certificati di emissione in eccesso che non sono utilizzati dalle imprese possono essere venduti ad altre imprese che gravano sull'ambiente oltre la misura consentita nel quadro di sistemi commerciali appositamente istituiti.

Il 2 febbraio 2010 degli aggressori sono riusciti per mezzo di un semplice attacco di phishing ad accedere ai dati di accesso di utenti di servizi di scambio di quote di emissioni. L'e-mail di phishing è stata camuffata come comunicazione (avvertimento di attacco di hacker) del servizio germanico di scambio di quote di emissioni che invitava i destinatari a cliccare su un link per poi registrasi nuovamente con i dati di utente/password.

I truffatori hanno venduto i diritti di inquinamento derubati; successivamente il registro ufficiale dello scambio di quote di emissioni è rimasto paralizzato in ampie parti di Europa. Il registro nazionale svizzero dello scambio di quote di emissioni dell'Ufficio federale dell'ambiente (UFAM) ha sensibilizzato la propria clientela con un apposito avvertimento sulla sua pagina Web.

---

[40] LTC, RS 784.10: http://www.admin.ch/ch/i/rs/c784_10.html (stato: 27 agosto 2010)

[41] OST, RS 784.101.1: http://www.admin.ch/ch/i/rs/c784_101_1.html (stato: 27 agosto 2010)

[42] LSCPT, RS 780.1: http://www.admin.ch/ch/i/rs/c780_1.html (stato: 27 agosto 2010)

[43] OSCPT, RS 780.11: http://www.admin.ch/ch/i/rs/c780_11.html (stato: 27 agosto 2010)

[44] http://www.bj.admin.ch/bj/de/home/themen/sicherheit/gesetzgebung/fernmeldeueberwachung.html (stato: 27 agosto 2010)

Nel caso di questo attacco è degno di nota non tanto il procedimento tecnico quanto l'obiettivo prescelto. In Svizzera gli attacchi phishing nei confronti di fornitori di servizi finanziari sono praticamente estinti. Ciononostante questo metodo gode di grande favore da parte degli aggressori, che operano nella maggior parte a partire dell'Africa settentrionale. Gli obiettivi degli attacchi sono illimitati se tali obiettivi sono unicamente protetti dal login e dalla password e se consentono di far soldi. Ne sono soprattutto colpiti i gestori di carte di credito, i provider di e-mail e le piattaforme di asta.

4.10 Microsoft preannuncia un servizio di annuncio dei dati di accesso derubati

Nel corso del primo semestre 2010, il produttore di software Microsoft ha annunciato l'inaugurazione di un centro per l'annuncio di furto di identità e furto di dati. L'Internet Fraud Alert Center[45], capitanato da Microsoft ma gestito dalla National Cyber-Forensics & Training Alliance[46], ha lo scopo di riunire le principali potenziali vittime di furto di dati o di identità, come istituti finanziari e e-commerce, con ricercatori e agenzie governative, nell'intento di condividere informazioni riguardanti questi reati, di modo che la reazione possa essere rapida e efficace. Ad esempio se un ricercatore entrasse in possesso di dati come numeri di carte di credito rubate (ad esempio individuando un drop server di una rete bot), esso potrebbe inviare questi dati all'Internet Fraud Alert Center, il quale si preoccuperebbe in seguito di trasmette le informazioni agli enti coinvolti.

4.11 Hacking di un server DNS: pornografia e adware dietro i domini governativi

Secondo quanto riportato da Sunbelt[47], affiliati del sito web FLVDirect sono riusciti a piratare i domain name servers di alcuni siti governativi americani (.gov). Lo scopo è stato quello di reindirizzare gli utenti di questi siti governativi[48] verso il sito di adware FLVDirect e quello pornografico XXXBlackBook.com. I criminali hanno inoltre creato nuovi sub domain, come tubes-1911.empria-kansas.gov, utilizzati anch'essi per il reindirizzamento.

5 Tendenze / Prospettive

5.1 Spionaggio e furto di dati in stile TIC

Dal 2005, data della pubblicazione del primo rapporto semestrale di MELANI, il furto di dati è un tema ricorrente. Il procacciamento illecito di dati è effettuato per mero interesse finanziario e criminale o nel quadro dello spionaggio sostenuto dagli Stati. Il tema come tale

[45] https://www.ifraudalert.org/default.aspx

[46] http://www.ncfta.net/main/home/

[47] http://sunbeltblog.blogspot.com/2010/07/flvdirect-affiliates-hacking-government.html

[48] Tra questi siti figurano: yaceycountync.gov, uppersiouxcommunity-nsn.gov, woodfin-nc.gov, dumontnj.gov, emporia-kansas.gov

ha conosciuto una seconda primavera mediatica con gli attacchi a Google e ad altre imprese TIC, abbondantemente commentati dalla stampa e dalle cerchie specializzate alla fine del 2009 e all'inizio del 2010 sotto la denominazione «Operation Aurora». In questo contesto le cerchie della comunità per la sicurezza TIC hanno sottoposto questo tipo di attacco mirato, basato su malware, a un *branding* culminato nel concetto di «Advanced Persistent Threat (APT)». Il tutto si è accompagnato a numerosi commenti tecnici che invitavano a preparasi a simili attacchi volti a procurarsi informazioni e dati. Questa presa di coscienza, che a fine 2009 si è affermata anche presso le imprese di sicurezza TIC, è meritevole ma non muta nulla al fatto che siffatte attività di spionaggio siano già da anni all'ordine del giorno.

Fin dal 2005 il New York Times ha pubblicato un rapporto relativo a un'operazione dell'FBI denominata «Titan Rain». Nella fattispecie si trattava di sistemi di computer infettati delle autorità US dai quali venivano carpiti da lungo tempo documenti e informazioni. Come possibile autore di presumeva la Cina. A un primo esame poco importa che questa supposizione sia o no pertinente. Si tratta invece di rendere chiaro che gli autori che si celano dietro questi misfatti non si accontentano né si accontenteranno di un solo attacco. Lo spionaggio è un processo sul lungo termine, che vive della costruzione e dello sfruttamento di fonti e del posizionamento di nuove fonti, non da ultimo nell'ipotesi che gli attuali fornitori di informazioni siano scoperti o sostituiti. Questa metodologia fondamentale dello spionaggio è valida anche nel mondo delle TIC.

Un'organizzazione, rispettivamente uno Stato che si è posto come obiettivo di accedere a informazioni classificate di un altro Stato o di una determinata organizzazione dovrà a tale scopo erigere in una forma o nell'altra un'infrastruttura o una base operativa. Le persone che controllano le fonti sono però soltanto una parte del tutto. I documenti carpiti devono essere visionati e valutati; in base a questo le fonti dovranno essere informate in merito al genere di informazioni ulteriormente necessitate e alle altre organizzazioni e autorità che presentano un interesse. Un simile meccanismo comporta altresì l'inconveniente di rendere difficoltoso il cambiamento di determinati processi, procedimenti e risorse, ragione per la quale nelle loro azioni si ravvisa sovente un analogo modello di base, che si tratti nel mondo reale delle modalità di acquisizione delle fonti, della maniera di controllarle o delle installazioni fisiche frontali in loco. Anche nel mondo delle TIC – dove di per sé non deve essere acquisita nessuna fonte umana e nel quale la tecnica consente taluni rapidi adeguamenti e creatività – sono nondimeno ravvisabili parti immutate dell'infrastruttura complessiva e dei modi di procedere.

Nel mondo di Internet e delle TIC costituisce piuttosto una rarità ciò che fa parte dello standard di controspionaggio di ogni Stato o impresa, segnatamente la messa in relazione di determinati eventi per individuarne le affinità e quindi assegnare tali eventi a un complesso generale. Questa circostanza potrebbe essere dovuta all'approccio classico in ambito di sicurezza TIC, dove occorre anzitutto porre rimedio a un sistema infettato o a un singolo evento (cosiddetto incident) per garantire in maniera possibilmente rapida l'ulteriore operabilità. È rara o non accade mai la messa in relazione di siffatti incident con un evento su un periodo relativamente lungo. Anche nel senso di un rendiconto rapido simili singoli eventi, come Aurora, GhostNet, Titan Rain, l'attacco al DFAE e altri, sono certo riportati dai media, ma in genere come singoli casi a sé stanti di spionaggio con l'ausilio delle TIC. Nel quadro di un'osservazione più attenta molti di questi eventi potrebbero essere raggruppati in pochi ma importanti e complessi casi che fornirebbero informazioni su chi, come e dove esattamente utilizza le TIC a scopo di spionaggio e di furto dei dati. Ciò consente un'osservazione più precisa ed equilibrata di queste cerchie di sospetti e quindi un impiego informato di mezzi preventivi perché rende possibile una migliore valutazione della situazione di base di minaccia. La differenziazione tra attacchi criminali non mirati e attacchi individuali adeguati in maniera specifica è sovente difficile per gli analisti non sperimentati.

A livello di Confederazione e per quanto riguarda le infrastrutture critiche della Svizzera rientra nei compiti della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione

MELANI effettuare una siffatta valutazione dei singoli eventi e allestire nella misura del possibile un quadro generale di un simile complesso di casi. Anche negli altri Paesi la tendenza va in direzione della messa in relazione di simili eventi TIC per poter definire e individuare con maggiore precisione le organizzazioni che si celano dietro di essi. Ed è proprio nel campo delle imprese private – esposte alla minaccia latente di spionaggio – che si raccomanda la costituzione di capacità che vadano oltre il disbrigo classico degli incident nel settore IT. Esse consentono di mettere a disposizione basi decisionali di livello strategico, riferite non soltanto al settore TIC, ma anche alla tutela delle informazioni e dei dati in generale.

5.2 Cessazione del Windows XP – Update-Service

Microsoft ha annunciato nel corso del primo semestre la fine del supporto di Windows XP SP2[49] (13 luglio 2010) e di Windows Vista (13 aprile 2010) senza Service Pack. Windows XP è sul mercato dall'ottobre del 2001 e rimane tuttora la versione di Windows maggiormente diffusa[50]. Secondo l'impresa di statistica StatCounter il 53 per cento degli utenti utilizzerebbe ancora Windows XP, mentre le quote di mercato di Windows 7 e di Windows Vista sarebbero pressoché identiche con il 20%. A partire da ora per XP rimane il solo supporto, a condizione che sia installato il Service Pack 3. Microsoft prevede di cessare definitivamente il supporto di Windows XP nell'aprile 2014. Secondo la ditta Gartner[51] ci si deve aspettare che già a fine 2012 le nuove versioni di numerose applicazioni non supportino più XP.

Come nel caso dello hardware anche in quello del software esiste soltanto un periodo limitato di garanzia e anche i pezzi di ricambio non sono disponibili eternamente. Windows XP si è però affermato in maniera così forte presso le imprese e i privati da rendere impensabile per il momento una sua cessazione totale e globale. È un fatto sorprendente se si pensa alla rapidità dell'evoluzione in ambito TIC nel corso degli ultimi anni. La fine di XP giungerà comunque irrimediabilmente e proprio perché nel caso delle imprese un cambiamento di software deve essere pianificato sul lungo termine e non può essere effettuato dall'oggi all'indomani, si esige prudenza in questo ambito affinché rimanga tempo sufficiente per pianificare ed eseguire test. Nel caso però delle apparecchiature di comando, come ad esempio nel contesto della produzione industriale, delle università o degli ospedali, non sarà in parte possibile o solo difficilmente possibile migrare tempestivamente su un altro sistema operativo perché il software e le carte di comando devono essere poste in sintonia con il pertinente sistema operativo e in parte anche essere certificati.

Oltre alla situazione delle imprese va però presa in considerazione anche quella dei privati. Nel loro caso non si cambia in genere il sistema operativo, ma si sostituisce il vecchio computer con uno nuovo, sul quale è installato un (nuovo) sistema operativo. L'importante è che si tratti di un sistema funzionante. Per quale motivo si dovrebbe smaltire un computer funzionante? Il problema che si presenta nella fattispecie è che al termine del ciclo di vita non ci sono più gli aggiornamenti critici di sicurezza. Ciò significa che le nuove lacune di sicurezza non possono più essere colmate. Se fino al 2014 Windows XP dovesse ancora possedere una quota di mercato superiore alla media ne potrebbe però risultare un grande problema.

[49] There is no Service Pack 3 for the 64-bit version of Windows XP. If you are running the 64-bit version of Windows XP with Service Pack 2, you are on the latest service pack and will continue to be eligible for support and receive updates until April 8, 2014. Fonte: http://windows.microsoft.com/en-us/windows/help/learn-how-to-install-windows-xp-service-pack-3-sp3 (stato: 27 agosto 2010)

[50] http://support.microsoft.com/gp/lifesupsps (stato: 27 agosto 2010)

[51] http://www.cio.de/knowledgecenter/pc-support/2236656/index1.html (stato: 27 agosto 2010)

Un prospetto della durata di vita dei singoli prodotti Windows è disponibile su:

http://support.microsoft.com/gp/lifeselect

5.3 I dati di Davide e Golia

Gli apparecchi supportati tramite Internet (*Smartphones, eBook-Reader*, ecc.), le reti sociali e altri servizi di comunicazione Internet facilitano la vita e offrono agli utenti il vantaggio di potersi collegare e scambiare informazioni più semplicemente. Tramite il rilevamento dei dati statistici le prestazioni di servizi possono essere continuamente migliorate e finanziate da un'offerta pubblicitaria (gratuita) sempre più mirata. Per questo motivo gli offerenti di simili applicazioni vogliono ottenere il maggior numero possibile di informazioni sui loro utenti. Chi intende tutelare la propria sfera privata deve sovente confrontarsi con paginate di parametri di sicurezza poco chiari e spesso non comprende quali siano le conseguenze di quale configurazione. Sono inoltre sviluppate costantemente nuove possibilità di messa in relazione e di valutazione di raccolte di dati. Anche quando si decide scientemente quali dati rivelare all'offerente di prestazioni Internet si perde sovente il controllo di quanto avviene con questi dati. Il rilevamento, l'elaborazione e lo sfruttamento dei dati è raramente trasparente. Una serie di dati rilevata oggi per un determinato scopo può rendere possibile domani informazioni inaspettate se posta in relazione con nuovi dati. Dato che in Svizzera vige la libertà contrattuale gli offerenti e gli acquirenti/utenti possono in linea di massima convenire qualsiasi cosa nel quadro dell'ordinamento giuridico perché nessuno è obbligato ad acquistare un determinato prodotto o a ricorrere a una determinata prestazione di servizi. Le modifiche delle condizioni di utilizzazione (Terms & Conditons) o delle disposizioni in materia di protezione dei dati (Privacy Policy) possono tipicamente essere decise unilateralmente dall'offerente, senza tener conto del cliente. A chi non è d'accordo con le nuove condizioni non rimane in genere che la possibilità di disdire il servizio corrispondente o di non più utilizzare il prodotto. Sembra però dubbio che chi cura i propri contatti quasi esclusivamente attraverso le reti sociali possa o voglia disdire questo servizio oppure che l'utilizzatore di uno smartphone voglia restituire il suo gadget prediletto perché l'offerente si riserva ampi diritti di rilevamento, elaborazione e sfruttamento dei dati. Numerose persone non si danno affatto la pena di leggere paginate di condizioni, scritte in maniera complicata. È tipico voler utilizzare un prodotto o un servizio senza consacrare ore alla lettura di un testo noioso o a una configurazione eccessiva e pensare: «Ciò che figura nelle condizioni generali avrà pure una sua logica e la configurazione di base non è sicuramente da buttare». Gli utenti devono invece assumere la loro propria responsabilità e mantenersi al corrente. Ciò significa soprattutto leggere il testo scritto in caratteri piccoli e sincerarsi che si intende rendere accessibile una determinata informazione. Gli utenti devono agire nella consapevolezza che per il tramite dei loro dati si possono allestire ampi profili di personalità, che «pagano» le offerte (gratuite) con i loro dati personali rivelati in contropartita. Gli offerenti di simili servizi generano le loro entrate mediante la pubblicità. Tali entrate aumentano quante più persone ricorrono al servizio e quanto più è mirata l'analisi dei fabbisogni degli utenti. I modelli di affari poggiano sulla riflessione che gli utenti sono disposti a mettere a disposizione informazioni quando ne ricevono un prodotto utile che facilita la loro vita: il modo più semplice di rimanere in contatto con i propri amici, la ricetta perfetta per la cena, il ristorante adatto nei dintorni oppure offerte interessanti passeggiando in città. Nella ricerca del maggior numero possibile di utenti e di occasioni di pubblicità gli offerenti mettono continuamente a disposizione nuove applicazioni.

Va anche osservato che sovente si diffondono anche dati di terzi: nell'elenco degli indirizzi figurano indicazioni dettagliate sui contatti e anche in album non pubblici sono messe a disposizione dell'offerente fotografie di amici e conoscenti. In questo contesto va rilevato che i programmi di riconoscimento dei volti migliorano costantemente e che numerosi smartphone con funzione GPS provvedono le fotografie scattate di un cosiddetto geotag che

indica con esattezza le coordinate del luogo dello scatto. Si schiudono così possibilità ancora inimmaginabili poco tempo fa caricando fotografie su Internet. Oltre ai loro vantaggi incontestabili, anche i servizi basati sulla localizzazione[52], che consentono di comunicare agli amici l'attuale luogo di soggiorno, celano pericoli che nella migliore delle ipotesi procurano soltanto leggeri inconvenienti, ma nella peggiore delle ipotesi l'effrazione della propria casa (dalla quale si è manifestamente assenti)[53].

I principali offerenti attuali di reti sociali e di servizi analoghi provengono in maggioranza dallo spazio statunitense, dove sono in genere assenti norme di protezione dei dati di obbligatorietà generale. Le disposizioni più severe in materia di protezione dei dati vigenti negli Stati europei vanno solitamente a scapito dei diritti dei cittadini e della competitività delle imprese nostrane che offrono prestazioni di servizi paragonabili. Non rimane da sperare che grazie alla maggiore sensibilizzazione dei cittadini nel campo della cura dei dati personali il mercato si apra a favore di prodotti e di offerte rispettosi della protezione dei dati.

5.4 Servizi Web – Problemi di base per il legislatore

Gli sviluppi tecnologici e sociali creano in continuazione nuove possibilità e nuovi rischi. Sovente si postulano nuove leggi se consecutivamente a questi cambiamenti insorgono problemi. I politici e i privati soccombono all'illusione che grazie alla legislazione si possa vietare Street View, controllare Facebook oppure rendere inaccessibili in Internet i contenuti malvisti. Anche se simili misure sono in linea di massima ipotizzabili, nel contesto dell'attuazione e dell'esecuzione del nuovo diritto si pone la questione della proporzionalità. Una regolamentazione eccessiva potrebbe intralciare l'economia e limitare le possibilità legittime degli utenti. Un divieto accompagnato da una sanzione è efficace soltanto se può essere e se viene eseguito.

Le leggi devono essere formulate in maniera generale e astratta e neutrale dal profilo della tecnologia. Anche nel caso delle misure di un regolatore va osservato che una formulazione troppo restrittiva non ricopre gli eventuali sviluppi futuri[54], mentre norme troppo generali consentono un ampio margine di manovra, diminuendo la certezza del diritto. La cosa diviene problematica quando si trattano in maniera particolare offerte o servizi specifici o si emanano leggi concernenti applicazioni concrete: Google Street View non è l'unico servizio che offre immagini di vie residenziali e Facebook non è la sola rete sociale. Né una legge su Street View né una regolamentazione di Facebook ricoprirebbero tutti i servizi corrispondenti – senza poi parlare dell'eseguibilità.

Il diritto si attiene in linea di massima al principio di territorialità. Le norme svizzere non si applicano imperativamente alle fattispecie in Internet. A titolo di esempio non appena è data partecipazione di un'impresa estera occorre dapprima chiarire se si applica il diritto svizzero, se è competente un'autorità svizzera e quali siano le modalità di esecuzione di eventuali decisioni. Se per esempio una rete sociale statunitense si rendesse colpevole di gravi

---

[52] Ad esempio servizi basati sul GPS come Foursquare, Gowalla, Facebook Places o Google Latitude – ma anche tramite le comunicazioni Twitter o lo stato Facebook sono regolarmente rivelati i luoghi di soggiorno.

[53] http://pleaserobme.com/ (stato: 27 agosto 2010)

[54] Così nel caso dell'ordinanza del 31 ottobre 2001 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT, RS 780.11: http://www.admin.ch/ch/i/rs/c780_11.html), secondo la quale il solo provider di Internet deve poter sorvegliare la casella di posta elettronica dei suoi clienti – i meri offerenti di posta elettronica non sono apparentemente contemplati. Questa circostanza potrebbe essere riconducibile al fatto che a quel momento i conti di posta elettronica erano principalmente offerti dai provider di Internet e che i meri fornitori di posta elettronica erano praticamente sconosciuti in Svizzera.

violazioni della protezione dei dati ai sensi della legislazione svizzera, ma non ledesse il diritto statunitense, il consumatore svizzero non avrebbe alcuna possibilità di difendersi.

Il legislatore può invero imporre all'offerente di infrastrutture[55] e di prestazioni di servizi autorizzate[56] l'obbligo legale di controllare e di filtrare tutti i contenuti e di sottoporre a un esame severo i clienti prima di stringere relazioni commerciali per tutelare a titolo preventivo i consumatori svizzeri. A tale scopo si dovrebbe però istituire un apparato di censura come in uno Stato totalitario e tutte le misure dovrebbero essere pagate a più caro prezzo soltanto per constatare alla fine che la piazza economica Svizzera ha perso enormemente in termini di attrattiva e che la protezione dei consumatori interdetti perseguita per questo tramite permane lacunosa. Sarebbero altamente più efficienti processi chiari che definiscano le modalità per controbattere gli abusi constatati e le risorse da destinare a tale scopo[57].

In questo contesto si rinvia all'intervento parlamentare[58] volto a vietare le offerte pornografiche commerciali sui cellulari (come reca il titolo della mozione – mentre nel testo si parla in genere di «dispositivi di telecomunicazione»[59]) nell'intento di proteggere i giovani. A titolo di variante la mozione chiede di «obbligare i fornitori di prestazioni del servizio universale a bloccare tutte le comunicazioni verso servizi a valore aggiunto con contenuti erotici o pornografici per i minori di 16 anni, nonché di imporre ai fornitori di servizi a valore aggiunto di non offrire ai minori di 16 anni contenuti erotici o pornografici». Tutto questo sebbene secondo l'ordinamento giuridico in vigore[60] chiunque offre, mostra, lascia o rende accessibile pornografia a una persona minore di sedici anni è punibile, sia che agisca per scopo di lucro o a titolo gratuito, sia online oppure offline. Nel caso specifico appunto della pornografia un'impresa sarebbe punibile a contare dal momento in cui giunge a conoscenza del fatto e non ne impedisce l'accesso. A seconda delle circostanze le imprese di intermediazione rimangono impunite nelle altre fattispecie. Si dovrebbe quindi chiarire la questione a partire da quale momento e quale tipo di responsabilità si può attribuire a una mera impresa di intermediazione[61] alla quale non può essere tipicamente imputata a titolo primario la conoscenza del contenuto intermediato o trasmesso.

Anche la conservazione dei dati ai fini di prevenzione oggetto di recenti vivi dibattiti in Germania costituisce un interessante esempio di approccio dei problemi che si pongono al legislatore: da parte delle cerchie dei difensori dei diritti civili si adducono la protezione dei dati e il sospetto generale, mentre la polizia e le associazioni di vittime esigono un mezzo per combattere l'anonimato e considerano sovente la protezione dei dati come una protezione dei colpevoli. Anche in questo caso si tratta di raggiungere un sano equilibrio tra i diversi interessi e di trovare una soluzione praticabile. Sebbene anche secondo la normativa[62] censurata dal Bundesverfassungsgericht la registrazione delle pagine Web visitate da un utente non sia consentita, proprio questi dati possono rivelarsi determinanti ai fini dell'identificazione nel caso degli utenti mobili (dove più persone condividono il medesimo indirizzo)[63], dato che con i mezzi ordinari (indirizzo IP e ora) non si può accertare

---

55 Ad esempio provider di Internet.

56 Ad esempio le imprese che detengono numeri brevi SMS e intermediano servizi per questo tramite.

57 Come il bloccaggio dei numeri brevi SMS o il bloccaggio di nomi di dominio, cfr. il capitolo 3.5.

58 http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20063884 (stato: 27 agosto 2010)

59 Questa formulazione è altresì comprensiva dell'Internet. – Non dovrebbe però essere nelle intenzioni dell'autore della mozione consentire in Internet soltanto (ma pur sempre) la pornografia gratuita.

60 Art. 197 cpv. 1 del Codice penale (CP, RS 311.0): http://www.admin.ch/ch/i/rs/311_0/a197.html (stato: 27 agosto 2010)

61 Provider di Internet, imprese di telecomunicazione, detentori di numeri SMS a valore aggiunto, gestori di sistemi di pagamento online, ecc.

62 Cfr. il capitolo 4.8

63 Cfr. il capitolo 3.10

univocamente quale partecipante a una determinata chat room abbia imperversato.

È in ambito per l'appunto di infrastrutture di informazione e di comunicazione che una limitazione della cerchia degli autori oppure una chiara determinazione della localizzazione degli autori sono estremamente difficili. Internet come mezzo delittuoso per raggiungere l'obiettivo è globalmente inerente e anche una differenziazione tra attori statali e privati è in parte impossibile. Per questo motivo i tentativi a livello di legislazione vanno sovente in direzione del controllo o della punizione di cosiddetti atti preliminari. Tuttavia proprio nel settore delle TIC un simile approccio fallisce per il fatto che i mezzi utilizzati sono praticamente sempre mezzi dual use, ossia mezzi che possono essere impiegati per proteggere ma anche per nuocere. Dal punto di vista della proporzionalità questi approcci ostacolano a seconda dei casi l'uso legittimo e innovativo delle nuove tecnologie. In definitiva l'uso delle tecnologie disponibili è ovunque lo stesso e solo l'intenzione decide in merito all'abuso o no. Il progetto di ratifica della convenzione sulla cibercriminalità tenta di conformarsi a questa circostanza[64].

[64] Cfr. il capitolo 3.6.

6 Glossario

Il presente glossario contiene tutti i concetti che figurano in caratteri corsivi nel testo. Un glossario completo è disponibile in: http://www.melani.admin.ch/glossar/index.html?lang=it.

Active Scripting	Una tecnologia sviluppata da Microsoft, che consente di caricare piccoli programmi – i cosiddetti ActiveX Controls – sul computer del visitatore al momento della visualizzazione di pagine Web, dove vengono poi eseguiti. Essi permettono di convertire diversi effetti e funzioni. Purtroppo questa tecnologia viene sovente sfruttata in modo abusivo e rappresenta pertanto un rischio per la sicurezza. A titolo d'esempio, sul computer vengono scaricati ed eseguiti Dialer. I problemi di Active-X concernono unicamente Internet Explorer dato che gli altri browser non supportano questa tecnologia.
Ad-Server	Gli Ad-Server sono utilizzati per misurare il successo della pubblicità su Internet. Sia il server fisico sul quale gira un software Ad-Server, sia tale software possono essere designati come Ad-Server.
Banda ISM	Per bande ISM (Industrial, Scientific and Medical Band) si intendono fasce di frequenze che possono essere utilizzate dalle apparecchiature ad alta frequenza nell'industria, nella medicina, in ambito domestico e analogo. Le apparecchiature ISM corrispondenti, come i forni a microonde e le apparecchiature mediche necessitano soltanto di un'omologazione generale.
Browser	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Netscape, Opera, Firefox e Safari.
Certificato digitale	Per certificato digitale si intendono dati strutturati che confermano il proprietario come pure altre caratteristiche di una chiave pubblica.
Chip EMV	L'abbreviazione EMV designa una specificazione delle carte di pagamento munite di un chip processore. Le lettere EMV stanno per le tre società che hanno sviluppato lo standard: Europay International (attualmente MasterCard Europe), MasterCard e VISA.
Codice HTML	HyperText Markup Language Le pagine Web sono elaborate in HTML. È così possibile definire le proprietà delle pagine Web (ad es. struttura della pagina, disposizione, link su altre pagine ecc.). Dato che HTML è basato sui caratteri ASCII, una pagina HTML può essere elaborata con un qualsiasi programma di elaborazione dei testi.
Codice PIN	Il numero personale di identificazione (PIN) o numero segreto

	è un numero conosciuto soltanto da una o poche persone e con il quale queste persone possono autentificarsi nei confronti di una macchina.
Codice sorgente	Il concetto di codice fonte, denominato anche codice sorgente (inglese: source code) designa in informatica la parte di un programma informatico scritto in linguaggio di programmazio-ne che può essere letta dall'uomo.
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
Conservazione dei dati ai fini di prevenzione	Memorizzazione su un determinato periodo di tempo di dati necessari per ricostruire chi, quando, per quanto tempo, con chi, da dove ha comunicato o tentato di comunicare.
Content Management System (CMS)	Un «Content Management System» (acronimo CMS, in italiano «sistema di gestione dei contenuti») è un sistema che rende possibile e organizza la produzione e l?elaborazione comune di contenuti, consistenti in documenti di testo e multimediali, in genere destinati al World Wide Web. Un autore può servirsi di un simile sistema anche senza conoscenze di programmazione o di HTML. In questo caso il contenuto informativo da presentare è detto «content» (contenuto).
Cross-Site-Scripting	Il Cross-Site Scripting (XSS) designa lo sfruttamento di una lacuna di sicurezza del computer nell'applicazione Web, nel senso che le informazioni di un contesto nel quale non sono degne di fiducia sono inserite in un altro contesto dove sono classificate come degne di fiducia.
DDoS	Attacco Distributed-Denial-of-Service Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
DNS	Domain Name System. Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
Dual Use	Dual Use è un concetto preso a prestito dall'inglese, principalmente utilizzato nel controllo delle esportazioni, che designa l'utilizzabilità di principio di un bene economico.
Fast Flux	Fast Flux è una tecnica DNS utilizzata dalle reti bot per ripartire e quindi dissimulare su diversi host le pagine phishing o le pagine che diffondono malware. Se un computer subisce un?avaria il computer successivo colma la breccia.
File PDF	Il Portable Document Format (PDF) è un formato di file per documenti indipendente dalla piattaforma, sviluppato e pubblicato nel 1993 dalla ditta Adobe Systems.

Financial agent	A financial agent works as a legal money broker and thus engages in financial transfers. Recently, this term has been used in connection with illegal financial transactions.
Firma elettronica	Per firma elettronica si intendono dati abbinati a informazioni elettroniche per il tramite delle quali si può identificare il firmatario, rispettivamente l'esecutore della firma, e verificare l'integrità delle informazioni elettroniche firmate.
FTP	FTP (File Transfer Protocol) è un protocollo di rete per la trasmissione di dati tramite reti TCP/IP. FTP può ad esempio essere utilizzato per caricare pagine Web su un server Web.
Full Disclosure	Pubblicazione integrale dei dettagli di una lacuna di sicurezza.
GPS	Il Global Positioning System (GPS), denominato ufficialmente NAVSTAR GPS, è un sistema globale di navigazione satellitare per determinare la posizione e misurare il tempo.
Host	È stato ed è tuttora utilizzato in ambito di IT soprattutto dagli elaboratori con grandi capacità di calcolo (ambiente bancario). Oggi serve anche a designare sistemi di computer di minori dimensioni (computer di utenti privati, server Web ecc.).
Indirizzo IP	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
Indirizzo MAC	Media Access Control Indirizzo hardware di un adattatore di rete per la sua identificazione univoca a livello mondiale. L'indirizzo MAC è scritto nella ROM dell'adattatore dai singoli fabbricanti (esempio: 00:0d:93:ff:fe:a1:96:72).
Infezione di pagine Web	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo scopo di diffondere il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
Infrastruttura critica	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.
Lacuna di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.

Lettore eBook	Un lettore eBook è un apparecchio portatile con il quale è possibile leggere libri memorizzati elettronicamente (eBooks).
Attacco Man-in-the-middle-/ Man-in-the-Browser	Attacco Man-in-the-Middle Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in grado di seguire o di modificare lo scambio di dati.
Modo protetto	In Internet Explorer ad esempio il modo protetto è una caratteristica grazie alla quale si rende difficile l'installazione sul computer di un software nocivo.
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza. Vedi anche Hotfix.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato.
Porta	Una porta è una parte di un indirizzo che assegna segmenti di dati a un protocollo di rete. Questo concetto è ad esempio previsto in TCP, UDP e SCTP per indirizzare i protocolli agli strati superiori del modello OSI.
Reasonable Disclosure	Pubblicazione ragionevole dei dettagli di una lacuna di sicurezza. Nell'ipotesi ideale pubblicazione in maniera tale da coadiuvare l'utente ad adottare misure di sicurezza e da impedire ai criminali di sfruttare la lacuna.
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.
Reti sociali	Una rete sociale consiste di un qualsiasi gruppo di persone connesse tra loro da diversi legami sociali attraverso l'uso di Internet.
Server dei nomi	Un server dei nomi è un server che offre la risoluzione dei nomi. La risoluzione dei nomi è una procedura che consente di risolvere i nomi dei calcolatori, rispettivamente dei servizi, in un indirizzo elaborabile dal computer; cfr. anche Domain Name System (DNS)
Simboli di collegamento	I simboli di collegamento sono piccole grafiche che aprono il programma desiderato quando vengono cliccate.
Sinkhole	Metodo per dirottare le reti bot su un determinato Command & Control Server al quale si ha accesso per ottenere il maggior numero di informazioni possibili sui sistemi infettati.

Smartphone	Uno Smartphone è un telefono mobile efficiente che amplia la funzionalità di un telefono mobile con quelle di un Personal Digital Assistant (PDA).
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.
Sottodominio	Si designa sottodominio un dominio che si situa al di sotto di un altro dominio nella gerarchia.
SSID	Service Set Identifier Identifica il nome di rete del WLAN. Tutt gli Access Points e i dispositivi finali del WLAN devono utilizzare il medesimo SSID per poter comunicare tra di loro.
Token	Componente hardware che genera un fattore di autenticazione (vedi Autenticazione a due fattori) (ad es. SmartCard, token USB, SecureID ecc.).
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.
Wireless (WLAN)	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.
Workaround	Per Workaround si intende l'aggiramento di un problema conosciuto all'interno di un sistema tecnico mediante una costruzione ausiliare. Si tratta di una soluzione provvisoria che non sopprime la causa vera e propria dell'errore.