Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

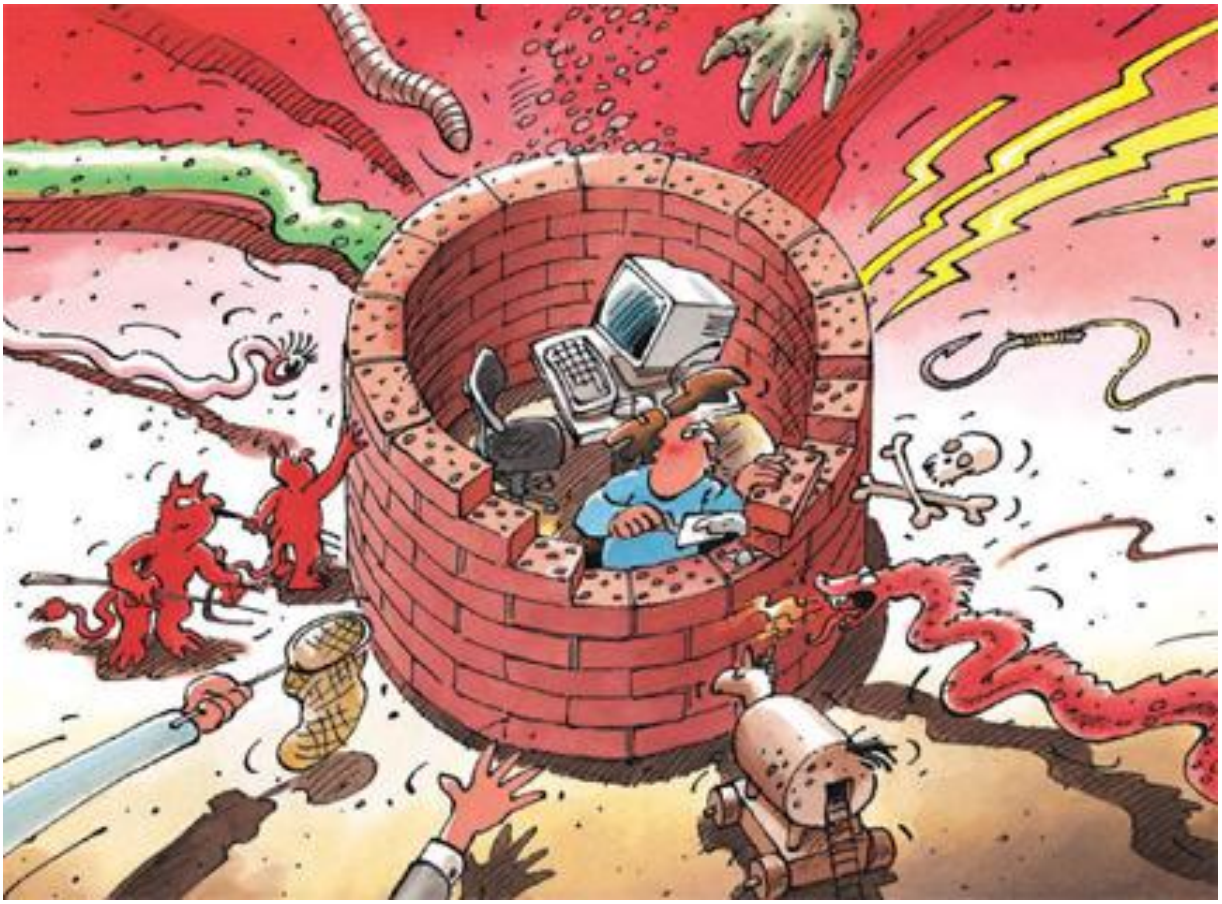
Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

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

Sicurezza dell'informazione

La situazione in Svizzera e a livello internazionale

Rapporto semestrale 2012/I (gennaio – giugno)



Indice

1 Cardini dell’edizione 2012/I

- **Hackeraggio in massa di password e di dati di carte di credito**
  Il primo semestre del 2012 è stato nuovamente caratterizzato da diversi importanti attacchi a ditte rinomate presso le quali sono stati derubati dati dei clienti, prevalentemente dati di login e password, ma anche dati di carte di credito. A questi casi in parte eclatanti fanno raffronto numerosi attacchi a ditte di minori dimensioni e ai loro dati, attacchi che si succedono quotidianamente senza peraltro essere tematizzati dai media. Secondo uno studio condotto da Verizon, oltre il 75 per cento degli attacchi è diretto contro PMI con meno di 1000 di collaboratori.

► Situazione attuale a livello internazionale: capitolo 4.5

► Tendenze / Prospettive: capitolo 5.3

- **Phishing in diverse varianti**
  In Svizzera si osservano quotidianamente casi di phishing. Nella maggior parte dei casi tali attacchi inducono tramite e-mail il cliente a fornire i dati della carta di credito. Come evidenziato da un caso di attualità i truffatori spulciano automaticamente gli albi svizzeri degli ospiti per accedere a indirizzi validi di posta elettronica verso i quali inviano gli email di phishing. Da un anno a questa parte, in Svizzera si osservano anche casi di voice phishing consistenti nell’effettuare false chiamate di supporto TIC in cui i truffatori chiedono di poter accedere al computer. Se riescono ad ottenere i dati di accesso dell’account di posta elettronica i criminali li utilizzeranno per inviare false richieste di aiuto a tutti i contatti della rubrica dell’account violato.

  Tutti questi eventi rendono necessaria una grande sensibilità da parte delle società nella comunicazione con la clientela. Se non si osservano alcune regole di base, la clientela catalogherà rapidamente le newsletter come presunte e-mail di phishing.

► Situazione attuale in Svizzera: capitolo 3.2, capitolo 3.4, capitolo 3.5, capitolo 3.6

► Tendenze / Prospettive: capitolo 5.4

- **Conflitto informatico nel Vicino Oriente**

  A fine maggio è stato scoperto il complesso programma nocivo «Flame», utilizzato per attaccare e spiare le organizzazioni in diversi Paesi del Vicino Oriente. L’analisi tecnica da parte delle imprese del settore della sicurezza ha evidenziato diverse affinità tra «Flame», «Stuxnet» e «Duqu».

  La diffusione aperta dei conflitti dall’inizio della primavera araba va di pari passo con un aumento dell’uso di mezzi TIC aggressivi e offensivi e di Internet. Si ha regolarmente notizia di siti Web oscurati, sottrazione di documenti di Stato e privati o uso di software nocivi a fini di sabotaggio.

► Situazione attuale a livello internazionale: capitolo 4.1, capitolo 4.2

► Tendenze / Prospettive: capitolo 5.2

- **Eventi nell'ambito del voto elettronico**
  È ovvio che nell’era di Internet i cittadini esigano dallo Stato la possibilità di votare per via elettronica. Esistono nondimeno alcune differenze fondamentali tra il voto elettronico e altri servizi, come l’e-banking.

► Situazione attuale in Svizzera: capitolo 3.7

► Tendenze / Prospettive: capitolo 5.5

- **Strategia nazionale di protezione contro i rischi informatici**
  Il 27 giugno 2012 il Consiglio federale ha approvato la strategia nazionale di protezione della Svizzera contro i rischi informatici.

► Situazione attuale in Svizzera: capitolo 3.9

2 Introduzione

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

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

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

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

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Avarie TIC nell'economia e nell'amministrazione

Le avarie provocate da manipolazioni errate o da disfunzioni tecniche sono una delle principali cause di disfunzione delle infrastrutture di informazione. I sistemi critici sono generalmente predisposti in maniera ridondante, in modo da impedirne la disfunzione. Come evidenziato da alcuni avvenimenti del passato, la ridondanza interviene generalmente bene in caso di guasti dell'hardware, ma solo limitatamente quando si tratta di software perché sui sistemi ridondanti girano pressoché il medesimo software e la medesima configurazione, ragione per la quale è possibile che all'atto della commutazione sul sistema di backup si verifichino i medesimi problemi apparsi sul sistema principale e che ne hanno parimenti provocato il crash[1]. Nel corso del primo semestre del 2012 alcune panne hanno destato l'attenzione in Svizzera:

Avaria informatica presso il Cantone di Berna

L'8 maggio 2012 una componente centrale della rete dell'Amministrazione del Cantone di Berna ha subito un'avaria che ha paralizzato per oltre 24 ore alcuni importanti sistemi, provocando l'indisponibilità di diverse prestazioni di servizi. In questo senso ad esempio il Servizio della circolazione stradale ha dovuto sospendere tutte le prestazioni di servizi. È stato colpito anche il portale online (TaxMe), sul quale è possibile accedere e compilare elettronicamente la dichiarazione di imposta, come pure il sistema di informazione sui dati immobiliari (GRUDIS), il *Geoportale*, i dati sui livelli delle acque dei fiumi e dei laghi, nonché la raccolta ufficiale delle leggi. È stato comunque possibile impedire una perdita di dati.

L'avaria è stata causata da un errore nel software del sistema operativo (Microcode) presso un sistema centrale di stoccaggio. Questo errore ha tra l'altro messo fuori uso le ridondanze della memoria dei dati, come ad esempio le doppie componenti di sistema e il mirroring dei dati su un centro di calcolo fuori sede[2].

Filiali Coop senza sistemi di cassa

Il 4 aprile 2012 tutte le filiali Coop della Svizzera tedesca hanno dovuto affrontare problemi con i sistemi di cassa, che per due ore non hanno potuto essere utilizzati. Ciò ha provocato la chiusura dei negozi o, in alcuni casi, ai clienti in attesa è stato distribuito un coissant. Motivo dell'avaria è stato un errore nell'aggiornamento del software, effettuato nottetempo e non apparso nel corso dei collaudi successivi.

Inizio ritardato del trading della Borsa svizzera

Venerdì 13 gennaio 2012 la borsa svizzera non ha potuto avviare le transazioni all'ora usuale. Mentre l'errore ha potuto essere rimosso prima dell'inizio usuale delle contrattazioni, il processo di riavvio di tutti i partner commerciali ha richiesto più tempo del

[1] Rapporto semestrale MELANI 2009/1, capitolo 4.6: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (stato: 31 agosto 2012).

[2] http://www.be.ch/portal/de/index/mediencenter/medienmitteilungen.meldungNeu.html/portal/de/meldungen/mm/2012/05/20120509_1347_alle_dienstleistungensindwiederverfuegbar (stato: 31 agosto 2012).

previsto, ciò che ha causato l'apertura delle contrattazioni alle 12. Il motivo dell'avaria ha invero potuto essere individuato, ma SIX, l'esercente della borsa svizzera, non ha voluto comunicarlo ufficialmente. Secondo le indicazioni fornite, solo una manciata di partecipanti alla borsa è stata interessata. Per ragioni di integrità del mercato e di imparzialità è però stato deciso di bloccare la totalità delle transazioni.

Non era la prima volta che il commercio aveva dovuto essere sospeso in seguito a problemi tecnici. Il 12 novembre 2009 la borsa aveva dovuto essere chiusa anzitempo alle 15 con la conseguente sospensione delle transazioni[3]. Nonostante questi eventi il crash di una borsa va considerato come un avvenimento estremamente raro.

Questi esempi illustrano chiaramente a quale punto l'economia, ma anche l'amministrazione, siano dipendenti da un esercizio senza guasti delle TIC. Già piccole disfunzioni possono provocare ingenti danni finanziari. È importante disporre di una solida infrastruttura TIC e soprattutto essere in grado di eliminare le avarie al più presto. Secondo uno studio che il PF di Zurigo ha condotto nel 2005, a livello nazionale una disfunzione di una settimana dell'intero complesso Internet ed estesa a tutto il territorio nazionale provocherebbe una perdita dell'ordine di 5,84 miliardi di franchi all'economia[4]. Dal momento che proprio per siffatte prestazioni di servizi non è mai possibile escludere disfunzioni, un'esatta pianificazione della continuità è indispensabile.

3.2 Violazione degli account di posta elettronica – I truffatori reagiscono alle misure dei provider di e-mail

Da ormai oltre tre anni si osservano casi di accesso ad account di posta elettronica per il tramite di dati di accesso rubati. I truffatori setacciano il conto di posta elettronica e trascrivono successivamente tutti i contatti o contatti mirati della rubrica. Nel caso di queste e-mail si tratta prevalentemente di false richieste di aiuto fingendo di essere bloccati all'estero e di essere stati derubati di tutto il denaro e del passaporto. Si richiede infine il trasferimento immediato di denaro:

«Spero che questo mio messaggio ti arrivi in tempo. Scusami per non averti informato del mio viaggio in Spagna. Mi trovo attualmente a Madrid e ho alcuni problemi perché ho perso il portafoglio».

Figura 1: Testo inviato a tutti i contatti di un conto di posta elettronica violato.

Il fatto che nemmeno i politici siano al riparo da simili attacchi è illustrato dal caso dell'esponente politica Verena Koshy, accaduto nel primo semestre del 2012. Sebbene il titolare dell'account di posta elettronica hackerato non subisca danni finanziari, un simile evento è sempre spiacevole e vincolato a un ingente cumulo di spese – soprattutto nel caso delle persone che dispongono di un'ampia rete di contatti. Una falsa richiesta di aiuto a nome della signora Koshy è stata inviata a tutti gli indirizzi della rubrica. In un caso come questo occorre informare i destinatari il più presto possibile per metterli in guardia e prendere immediatamente contatto con il *provider*, che adotterà le misure necessarie affinché la vittima possa nuovamente accedere al proprio conto. I provider reagiscono generalmente entro 48 ore e impediscono ai cracker di controllare l'account.

---

[3] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Technische-Probleme-legen-Boerse-lahm/story/30392767 (stato: 31 agosto 2012).

[4] http://www.ethz.ch (stato: 31 agosto 2012).

Purtroppo i truffatori sono consapevoli del fatto che il blocco del conto e gli avvisi ai destinatari riducono le loro chance di successo. Di conseguenza, negli ultimi mesi hanno adottato contromisure e adeguato il modo di procedere: continuano a rubare i dati relativi ai contatti e modificano leggermente l'indirizzo del titolare dell'account hackerato (Meier diventa ad esempio Neier) in modo da passare inosservato. L'aggressore si serve dapprima di questo indirizzo ai fini del truffa. Diversamente dal conto violato, questo fake è accessibile anche dopo che il provider ha adottato le proprie misure e il cracker può continuare a comunicare con la vittima finché la truffa è conclusa.

Pure nuovo è il fatto che i truffatori eliminano successivamente dal conto violato tutti i contatti e i messaggi e-mail. Ciò è destinato a impedire che il vero titolare del conto possa mettere in guardia tutti i contatti dopo il ripristino dell'accesso al conto. Questa circostanza è fonte di profonda irritazione per la vittima perché nella maggior parte dei casi non è disponibile alcun *backup* dell'elenco dei contatti e dei messaggi. In alcuni casi il provider può ancora salvare i dati, ma spesso sono perduti per sempre.

Qui di seguito sono elencati alcuni suggerimenti per contenere nella misura del possibile i danni in caso di evento.

1. Effettuare un *backup* dei contatti affinché in caso di evento si possa ripiegare su un indirizzo di posta elettronica alternativo. In questo modo è possibile mettere in guardia rapidamente i contatti.
2. Scegliere accuratamente il provider di posta elettronica, soprattutto se le e-mail sono utilizzate a titolo professionale.
3. In caso di evento tentare immediatamente di riprendere il controllo del proprio account. Nella maggior parte dei casi anche l'indirizzo alternativo di posta elettronica viene modificato: se non ne è il caso si può inviare una password sostitutiva a questo indirizzo di posta elettronica. Se però anche l'indirizzo alternativo è stato modificato occorre avviare un *processo di recovery*. A tale scopo la maggior parte dei provider di e-mail mettono a disposizione un formulario di *recovery*. Qui di seguito è elencata una scelta non esaustiva dei provider di e-mail più utilizzati:

Google	https://www.google.com/accounts/recovery/
Hotmail/ Live	https://account.live.com/resetpassword.aspx
Yahoo	https://edit.europe.yahoo.com/forgotroot
GMX	http://www.gmx.com/forgotPassword.html

3.3 Avanzata dei trojan che bloccano i computer

MELANI aveva già reso conto dei *trojan che bloccano i computer* nel suo ultimo rapporto semestrale[5]. Nella fattispecie si tratta di cosiddetto *ransomware* (*software nocivo* a scopo di estorsione) che blocca il computer ed esige successivamente il pagamento di un riscatto. Questa forma è inizialmente apparsa in Germania nella primavera del 2011 ed era provvista del logo del Bundeskriminalamt germanico (BKA), circostanza che è valsa al *software nocivo*

[5] Rapporto semestrale MELANI 2011/2, capitolo 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2012).

il soprannome «Cavallo di Troia BKA»[6]. Questa denominazione piuttosto infelice non ha ovviamente niente a che vedere con la polizia criminale federale tedesca.

Le prime versioni in Svizzera di questo cavallo di Troia sono state inviate lo scorso autunno a nome del Dipartimento federale di giustizia e polizia (DFGP). All'inizio del mese di marzo 2012 è poi seguito un altro tipo di trojan che finge di provenire dalla SUISA, la cooperativa degli autori ed editori di musica che funge da società di riscossione dei diritti d'autore in Svizzera[7]. Dal mese di giugno del 2012 è in circolazione una versione a nome del «Cyber Crime Investigation Department» (inesistente). In questo caso viene attivata la Webcam e l'immagine viene riprodotta sullo schermo del computer bloccato per intimidire ulteriormente la vittima.

Si esige il pagamento di una multa, nella maggior parte dei casi tramite il servizio di pagamento online Paysafe.

Paysafecard, l'offerente del mezzo di pagamento prepaid utilizzato in questi casi dai truffatori, ha reagito a questo abuso e stampato nel frattempo un avviso sulle carte Paysafe.

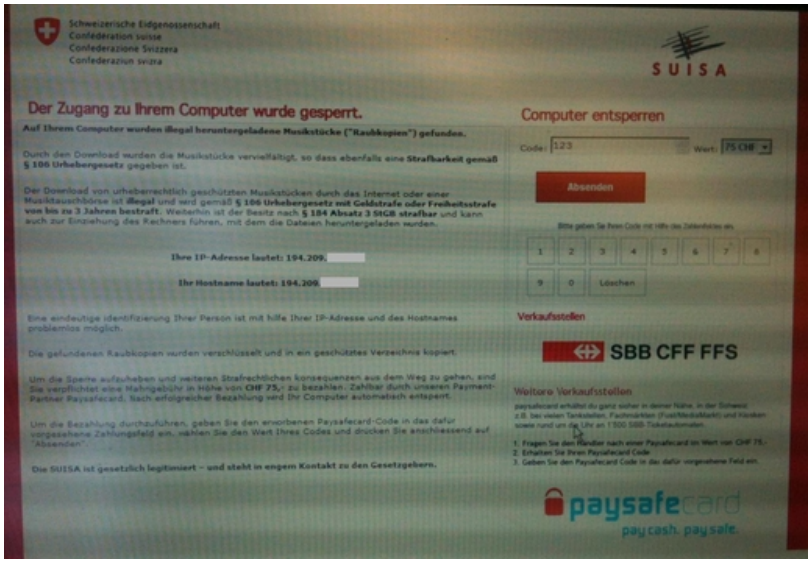


Figura 2: Trojan con il logo SUISA

Figura 3: Trojan con il logo della Confederazione Svizzera

---

6 Cfr. http://www.bka-trojaner.de – Su questo sito Web sono messe a disposizione indicazioni sulle diverse versioni (stato: 31 agosto 2012).

7 http://www.suisa.ch (stato: 31 agosto 2012).

Dall'apparizione dei primi casi in Svizzera sono stati annunciati regolarmente casi di computer bloccati alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI. L'infezione si propaga nella maggior parte dei casi via portali video oppure tramite siti che diffondono contenuti multimediali. Si presume che gli attacchi avvengano tramite file infetti o videoplayer compromessi.

Un'infezione e un blocco del computer comportano in ogni caso inconvenienti, soprattutto se si tratta dei computer di una piccola impresa che devono obbligatoriamente essere utilizzati e non possono essere sostituiti. MELANI è al corrente di casi simili.

MELANI è anche al corrente di casi in cui l'infezione può facilmente essere elusa: se il sistema viene riavviato senza connessione a Internet è possibile eludere il blocco in singoli casi.

3.4 Voice phishing (vishing)

Per molto tempo il *voice phishing* non ha interessato la Svizzera, ma dall'estate del 2011 si registra un numero crescente di casi anche nel nostro Paese. Nel suo ultimo rapporto semestrale MELANI ha abbordato in maniera dettagliata queste chiamate telefoniche[8]. Attualmente i truffatori procedono sempre nel medesimo modo: si riceve una chiamata da una presunta ditta di supporto informatico (solitamente Microsoft) che fa credere alla vittima che il suo computer invia messaggi sospetti. Per poterne «fornire la prova» le persone chiamate sono tipicamente invitate ad avviare il loro *Event-Viewer* (visualizzatore degli eventi), per il cui tramite si possono visualizzare i messaggi interni del sistema operativo. In merito occorre sapere che anche un sistema che funziona perfettamente produce occasionalmente messaggi di errore. A seconda dell'età e della configurazione del computer l'elenco dei messaggi di errore dell'Event-Viewer può essere molto lungo senza che il sistema presenti un problema di fondo. L'apertura del programma è tipicamente sfruttata dai chiamanti di «supporto» per presentare alle vittime un retroscena plausibile e spaventarle. L'obiettivo dei truffatori è convincere le persone chiamate a scaricare un programma di accesso remoto (*Remote Access Tool*) che consenta loro l'accesso al computer a distanza. Per questo tramite i truffatori hanno pieno accesso al sistema e dispongono quindi delle medesime possibilità di manipolazione dell'utente. Infine si tenta generalmente di vendere alla vittima una licenza di software oppure una prestazione di servizi («pulizia del sistema»), con la richiesta ulteriore di informazioni sulla carta di credito.

Se avete risposto a una telefonata del genere e avete dato informazioni sulla carta di credito è soprattutto importante bloccare senza indugio la carta di credito.

È di volta in volta difficile valutare cosa abbiano fatto o installato sul computer i truffatori. Se è stato concesso l'accesso tramite un *Remote Access Tool*, il truffatore dispone delle medesime possibilità di manipolazione dell'utente (copia/manipolazione/cancellazione di file, installazione di programmi, ecc. Il cracker potrebbe anche costruirsi una «*scappatoia*» per poter accedere nuovamente al sistema in secondo tempo).

Dopo un caso simile si raccomanda quindi di rivolgersi a un tecnico. Ciò non garantisce però che vengano rintracciati sul computer eventuali *software nocivi* o manipolazioni del sistema. Il metodo più sicuro consiste nel resettare completamente il disco rigido e nell'installare

[8] Rapporto semestrale MELANI 2011/2, capitolo 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2012).

nuovamente il sistema operativo. In merito va comunque osservato che prima di procedere è necessario salvare i dati personali, che altrimenti andrebbero persi.

Dopo la pulizia/nuova installazione del computer (o a partire da un altro computer) occorre inoltre modificare le password di tutti i servizi Internet che erano stati utilizzati in precedenza.

Vishing a nome di Swisscom

Nel mese di luglio 2012 è stata messa in circolazione una e-mail a nome di Swisscom. In pessimo tedesco, ma in migliore francese, le vittime erano rese attente sul fatto che qualcosa non funzionava con il loro conto, o che il loro conto era «ostacolato» (leggi: bloccato). Diversamente dalle classiche e-mail di *phishing* non si doveva indicare il nome di utente e la password, bensì chiamare un numero telefonico per ricevere ulteriori informazioni. Il numero, con il prefisso 0088, appartiene a un operatore di telefoni satellitari. In caso di chiamata sono quindi garantiti costi elevati. Non ha potuto essere accertato se durante la chiamata alla vittima sono stati chiesti il nome di utente e la password. Per quanto riguarda i conti di posta elettronica Swisscom, questi email di phishing sono stati bloccati con tempo.

Gesendet: Dienstag, 10. Juli 2012 01:19

Betreff: Sie haben 1 neue Nachricht / Vous avez 1 nouveau message

Ihr Konto ist gehemmt worden.

Für mehr Informationen erreichen Sie uns unter der Telefonnummer:
00881835211648 oder 00881835211650

Votre compte a été suspendu.

Pour de plus amples informations, vous pouvez appeler le numéro de téléphone:
00881835211648 ou 00881835211650

Figura 4: e-mail inviate nel luglio del 2012 a nome di Swisscom

3.5 Come i phisher ottengono gli indirizzi di posta elettronica

Esistono diverse possibilità attraverso le quali un indirizzo di posta elettronica può finire in una banca dati di spam. Una di queste è l'ispezione automatica di Internet a caccia di indirizzi e-mail validi (p.es. da forum o albi degli ospiti). Una volta finito in una banca dati di spam, l'indirizzo e-mail viene utilizzato ripetutamente e sovente rivenduto ad altri truffatori.

Gli esercenti di forum e di albi degli ospiti assumono una grande importanza che spesso sottovalutano o trascurano, perché nella maggior parte degli albi degli ospiti l'indirizzo di posta elettronica è tuttora pubblico e può essere molto facilmente estratto con l'ausilio di appositi tool.

Il fatto che questa fonte venga effettivamente utilizzata è illustrato da un'analisi degli indirizzi di destinatari di un'ondata attuale di e-mail di phishing. In questo caso gli indirizzi di e-mail utilizzati dai truffatori potevano essere attribuiti alle iscrizioni nell'albo degli ospiti di un sito Web svizzero. Alcuni albi degli ospiti si rivelano essere una vera miniera d'oro per i collezionisti di indirizzi. Sul sito Web di un musicista svizzero si possono ad esempio trovare oltre 2700 indirizzi di posta elettronica pubblicati. Per i truffatori ciò comporta il vantaggio

supplementare che gli indirizzi in questione appartengono con grande probabilità a cittadini svizzeri o perlomeno a persone di lingua tedesca. Grazie a queste informazioni le e-mail di phishing possono essere redatte in maniera più mirata, accrescendo la probabilità di riuscita dell'attacco.

MELANI raccomanda le seguenti misure per l'utilizzo degli indirizzi di posta elettronica sugli albi degli ospiti e nei forum:

Da parte dell'amministratore Web

- In molti casi la pubblicazione degli indirizzi di posta elettronica non è necessaria e serve unicamente da parametro di autenticazione per l'amministratore del sito Web. In questo caso è opportuno rinunciare alla pubblicazione dell'indirizzo e-mail.
- Se la pubblicazione è necessaria per la presa di contatto, si rinunci alla pubblicazione degli indirizzi di posta elettronica a chiare lettere. Esistono numerose possibilità (p.es. con l'ausilio di JavaScript) per impedire la lettura automatica degli indirizzi.
- Il metodo più sicuro è quello di non pubblicare l'indirizzo e mettere a disposizione un formulario online (ben protetto) di contatto.

Da parte dell'utente

- Indicate il vostro indirizzo di posta elettronica alle poche persone necessarie e utilizzatelo esclusivamente per la corrispondenza importante.

3.6 E-mail di phishing – Presunto rimborso d'imposta da parte dell'Amministrazione federale delle contribuzioni

Gli aggressori tentano con diversi trucchi di complicare la vita alle autorità di sicurezza che impediscono gli attacchi di *phishing*. MELANI ha reso conto in merito fin dal suo ultimo rapporto semestrale[9]. Un'ulteriore nuova variante è costituita dal modo di procedere descritto qui appresso.

Lunedì 4 giugno 2012 dei truffatori hanno inviato e-mail di *phishing* a nome dell'Amministrazione federale delle contribuzioni (AFC). Le e-mail prospettavano un rimborso d'imposta ai destinatari. Ai messaggi era allegato un formulario *HTML* nel quale si dovevano immettere i dati personali e della carta di credito. Diversamente dalle classiche e-mail di *phishing*, che invitano l'utente a cliccare su link per poi immettere i dati personali e quelli della carta di credito sulla pagina di phishing linkata, in questo caso la pagina *HTML* era acclusa all'e-mail come *allegato*. In caso di apertura la pagina *HTML* viene costruita a livello locale sul computer del destinatario. Se i campi vengono compilati e si prosegue, i dati sono trasmessi «direttamente» al cracker.

Per quest'ultimo ciò comporta il vantaggio di non dover disporre di alcun *server Web* hackerato o specialmente predisposto a tale scopo, dove altrimenti collocava la pagina di *phishing*, che poteva ovviamente essere oscurata dalle autorità di sicurezza o dall'Hosting-Provider. Tutta l'informazione della pagina Web di phishing si trova nell'allega*to*. L'unica

[9] Rapporto semestrale MELANI 2011/2, capitolo 3.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2012).

cosa ancora necessaria è un cosiddetto *PHP-Mailer*, come quelli non protetti che si trovano a migliaia in rete e tramite i quali ci si può inviare dati a qualsiasi indirizzo di posta elettronica. È chiaro che è molto più difficile bloccare e proteggersi da mailer di questo tipo.

Figura 5: E-mail di phishing con la maschera di immissione in allegato

A lungo si è pensato che le e-mail di truffa contenessero un'intestazione personale per rassicurare la vittima. Finora ciò si è sorprendentemente osservato soltanto in casi eccezionali. Un esempio di utilizzo di questo metodo è stata l'ondata di e-mail dell'estate del 2012 con la quale si è tentato di diffondere un software nocivo in *allegato*:

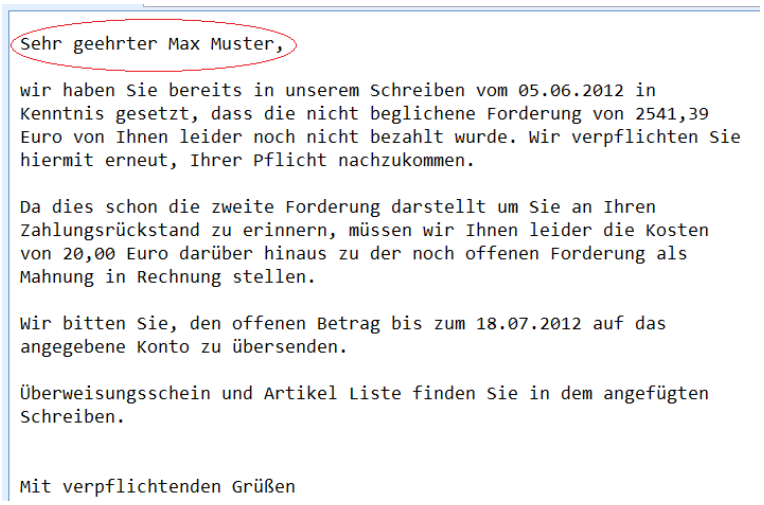


Figura 6: Esempio di e-mail con intestazione personale contenente un software nocivo

In linea di principio si può partire dal presupposto che le imprese serie non chiederanno mai tramite e-mail la password né inviteranno i loro clienti, sempre tramite e-mail, a verificare o ad aggiornare la loro carta di credito, il loro conto oppure altri dati personali. Le e-mail di questo tipo provengono generalmente da cracker. I truffatori pensano a scenari sempre nuovi per indurre i destinatari a reagire senza riflettere. Si veda in merito anche il capitolo 5.4 «Comunicazione con i clienti nell'era del *phishing*»,

Non seguite mai le indicazioni contenute in e-mail e inattese e sospette provenienti da mittenti sconosciuti, non cliccate su alcun allegato o link, ma eliminate il messaggio.

3.7 Eventi nell'ambito del voto elettronico

L'esercizio della democrazia diretta è uno dei beni più preziosi di ogni Svizzero. Ne fa parte anche l'e-voting, ovvero la possibilità di votare per via elettronica. Il vantaggio è evidente: la partecipazione ai processi di formazione dell'opinione politica, come ad esempio le votazioni popolari, non è vincolata alle ore di apertura dei locali di voto e può essere garantita ovunque in tutto il mondo.

Non sorprende quindi affatto che altri Stati oltre alla Svizzera, in particolare la Norvegia, l'Estonia e la Francia, stiano effettuando numerosi test promettenti con l'espressione elettronica del voto.

Le dicerie di manipolazione possono nondimeno porre in forse l'affidabilità dell'e-voting e pregiudicarlo durevolmente. Già semplici attacchi come gli attacchi *DDoS* possono avere ampie conseguenze e ritardare un'espressione democratica del voto o addirittura renderla impossibile. Il capitolo 5.5 esamina in maniera approfondita questa tematica.

Qui appresso sono illustrati alcuni esempi di casi che hanno riguardato l'e-voting nel primo semestre del 2012:

Voti in eccesso durante una votazione elettronica in Svizzera

Dopo la votazione popolare federale dell'11 marzo 2012 è stato reso noto che il voto espresso da un elettore domiciliato nel Cantone di Lucerna era stato conteggiato erroneamente due volte a motivo di un errore del software. L'errore sarebbe stato immediatamente individuato e gli specialisti sarebbero stati in grado di eliminare il voto in eccesso dal sistema. Come indicato nel comunicato stampa[10], non vi è alcun motivo per dubitare dell'esattezza dell'esito finale, mentre la segretezza del voto è stata tutelata in ogni momento.

Attacchi all'e-voting del New Democratic Party canadese

Per l'elezione del presidente del New Democratic Party canadese è stata effettuata la procedura di voto a più livelli tramite l'e-voting. Migliaia di membri del partito hanno votato online da casa. Nel corso della votazione i server hanno tuttavia subito un attacco *DDoS* che ha ritardato la procedura di voto. Il termine per esprimere il voto è stato prorogato a più riprese e lo scrutinio ha addirittura dovuto essere interrotto e riavviato successivamente. Questa circostanza avrebbe dissuaso numerosi elettori dalla partecipazione al voto.

[10] http://www.ge.ch/evoting/scrutin_20120311.asp (stato: 31 agosto 2012).

Hackeraggio di un progetto pilota di procedura di voto online a Washington D.C.

Nel mese di marzo 2012 alcuni ricercatori dell'Università del Michigan hanno pubblicato una notizia secondo la quale le funzioni di sicurezza di un progetto pilota di procedura di voto online per Washington, la capitale federale US, avrebbero potuto essere scardinate in pochissimo tempo. Secondo le indicazioni fornite, 48 ore dopo l'avvio del sistema i ricercatori avrebbero praticamente fruito del controllo completo del server di voto e sarebbero stati in grado di modificare ogni voto espresso e di rivelare il contenuto di quasi tutte le urne segrete. L'attacco è stato scoperto soltanto due giorni più tardi e questo unicamente perché i ricercatori avrebbero lasciato tracce univoche.

La Corte costituzionale austriaca abroga il regolamento di voto elettronico per l'elezione della Österreichische Hochschülerschaft (ÖH)

La Corte costituzionale austriaca ha abrogato il regolamento in quanto contrario alla legge l'ordinanza concernente il voto elettronico del 2009 presso la Österreichische Hochschülerschaft (ÖH), dato che non vi erano disciplinate in maniera sufficientemente precisa le modalità di verifica del funzionamento senza intoppi del sistema. Secondo il Ministero dell'Interno austriaco la decisione non ha alcuna conseguenza, in quanto il voto elettronico in ambito di elezioni federali deve comunque essere ancorato nella Costituzione. In Austria non si delinea attualmente una maggioranza costituzionale a favore di un adeguamento corrispondente[11].

3.8 Software nocivo con certificato di una presunta ditta svizzera

Tra il dicembre del 2011 e il marzo del 2012 sono apparse diverse versioni del *software nocivo* «Mediyes»[12], provviste del certificato chiave di una ditta della Svizzera interna, tale Conpavi AG. Sul suo sito Web la ditta si dice partner della Città di Lucerna e della Scuola universitaria professionale di Berna nell'allestimento di progetti di e-government.

La ditta Conpavi AG esiste effettivamente ed è iscritta nel registro di commercio, il suo scopo aziendale è però la fornitura di prestazioni di servizi e il commercio di beni nel settore farmaceutico. Ciò ha poco a che vedere con l'e-government. Si tratterebbe quindi di una ditta fantasma, inventata appositamente dai truffatori, come riportato da alcuni media?[13]

---

11 http://www.heise.de/newsticker/meldung/Oesterreichs-Verfassungsgerichtshof-hebt-E-Voting-auf-1400214.html (stato: 31 agosto 2012).

12 Nel caso del software nocivo Mediyes si tratta di un cosiddetto software di truffa mediante clic: a tale scopo il software cattura le richieste della vittima ai motori di ricerca Google, Yahoo e Bing e le dirotta sul server di una rete di annunci.

Affinché i gestori di siti Web possano collocare in maniera semplice pubblicità sul loro sito e far soldi per questo tramite, le ditte di pubblicità online mettono tra l'altro a disposizione funzioni di ricerca che possono essere facilmente integrate su tale sito. Se un visitatore cerca un concetto, oltre ai risultati del sito Web viene anche affisso un banner pubblicitario. Se il visitatore clicca sul link, il titolare del sito Web riceve denaro.

È esattamente a questo punto che intervengono i truffatori: utilizzano le richieste di ricerca copiate per forzare la pubblicazione di questi banner pubblicitari (sul sito Web appositamente creato a tale scopo) e per cliccarli automaticamente sullo sfondo e conseguire un guadagno.

13 http://www.nzz.ch/aktuell/startseite/zuger_scheinfirmaauf_krummer_tour_im_internet-1.16001018 (stato: 31 agosto 2012).

La cosa non sembra affatto così semplice. Da uno sguardo alla *macchina di archiviazione Internet* archive.org risulta che il sito conpavi.ch è apparso per la prima volta nel 2002.

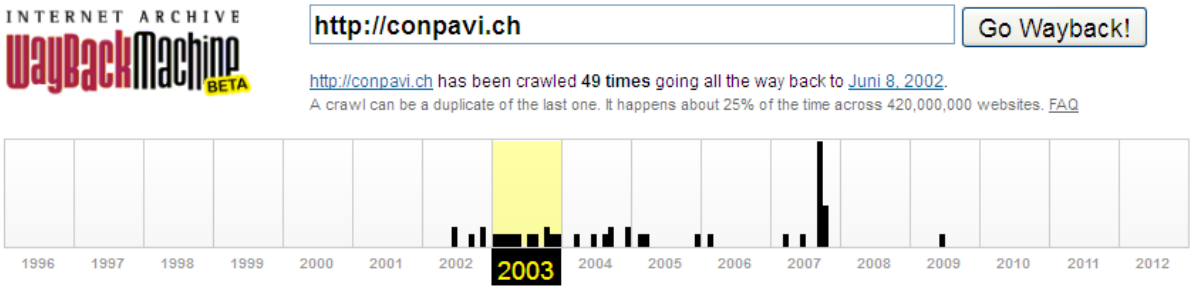


Figura 7: Registrazione nell'archivio archive.org concernente la ditta Conpavi

Da un attento esame del registro di commercio emerge che la ditta è stata fondata nel marzo 2000 con il nome netauc e che l'11 dicembre 2001 ha modificato il suo nome in conpavi. Scopo della ditta era la fornitura di prestazioni di servizi nel settore dei mezzi di comunicazione elettronica, in particolare per quanto riguarda gli interessi delle autorità in ambito di Internet[14]. Il 16 giugno 2009 la Conpavi è poi stata convertita in una ditta che fornisce prestazioni di servizi ed esercita il commercio di beni nel settore farmaceutico. Il sito Web della vecchia ditta con la descrizione delle prestazioni offerte è stato tuttavia mantenuto com'era. Ciò offriva ai criminali una piattaforma pressoché perfetta per effettuare le loro truffe e per giungere ai *certificati*. Chi non ha fatto ricerche dettagliate ha effettivamente potuto supporre che la società esiste ancora e si occupa di *e-government*. Pertanto era probabilmente possibile emettere certificati che convincessero i servizi preposti a emettere un *certificato* corrispondente.

I truffatori sondano tutte le possibilità affinché le loro azioni siano credibili agli occhi delle vittime. In merito capita sempre che il nome di una ditta o del sito Web di una ditta venga utilizzato abusivamente dai truffatori allo scioglimento della ditta. I siti Web rimangono sempre ben collegati e anche una ricerca in Google non indica alcuna attività sospetta. I truffatori riprendono sovente anche i *nomi di domini* dopo che la ditta li ha cancellati o non ne ha prorogato la registrazione. Essi possono così sfruttare la reputazione che la ditta si era costruita fino alla sua liquidazione o fino alla modifica dello scopo o del nome.

3.9 Il Consiglio federale approva la strategia nazionale di protezione contro i rischi informatici

Il 27 giugno 2012 il Consiglio federale ha approvato la stratega nazionale di protezione della Svizzera contro i rischi informatici[15]. Il Consiglio federale si è tra l'altro espresso a favore di un rafforzamento del personale di MELANI presso il DFF e il DDPS a contare dal 2013. La strategia tiene anche conto di numerosi interventi parlamentari che postulavano un rafforzamento delle misure contro i rischi informatici.

Il Consiglio federale persegue in merito i seguenti obiettivi strategici:

- l'identificazione precoce di minacce e pericoli nel settore informatico;
- l'aumento della capacità di resistenza delle infrastrutture critiche;

[14] http://www.zefix.admin.ch (stato: 31 agosto 2012).

[15] http://www.news.admin.ch/message/index.html?lang=de&msg-id=45138 (stato: 31 agosto 2012).

- la riduzione efficace dei rischi informatici, in particolare della criminalità informatica, dello spionaggio informatico e del sabotaggio informatico.

La strategia designa i servizi federali responsabili, che devono attuare entro il 2017 e nell'ambito del loro mandato di base 16 delle misure menzionate nella strategia. In questo processo di attuazione devono essere coinvolti partner provenienti dalle autorità, dall'economia e dalla società. Un servizio di coordinamento del DFF verifica l'attuazione delle misure e la necessità di nuovi interventi per diminuire i rischi.

La collaborazione nazionale tra economia e autorità, così come la collaborazione con l'estero, permangono una condizione della possibilità di riduzione dei rischi. Il costante scambio reciproco di informazioni è destinato a creare trasparenza e infondere fiducia. Lo Stato deve intervenire unicamente laddove sono in gioco interessi pubblici oppure opera nel senso della sussidiarietà.

Secondo la strategia l'approccio con i rischi informatici va inteso come parte di un processo aziendale, produttivo o amministrativo integrale nel cui contesto vanno coinvolti tutti gli attori – dal livello tecnico a quello di condotta. Ogni unità organizzativa della politica, dell'economia e della società assume la responsabilità di individuare il marchio informatico dei suoi compiti e delle sue responsabilità e quindi di indirizzare e ridurre il più possibile i rischi che ne conseguono nei loro rispettivi processi. Le strutture decentrate dell'amministrazione e dell'economia devono essere rafforzate in vista di questi compiti, mentre le risorse e i processi già esistenti devono essere utilizzati in maniera conseguente. La riunione continua di informazioni tecniche e non è necessaria per analizzare e valutare in maniera dettagliata i rischi informatici. Queste conoscenze vanno approntate in modo possibilmente centrale e essere ritrasmesse agli attori in funzione delle necessità per sostenerli nei loro processi di gestione dei rischi.

La strategia identifica anzitutto i rischi informatici come marchio dei processi e delle responsabilità esistenti. Di conseguenza tali rischi informatici devono essere integrati nei processi di gestione dei rischi. Occorre preliminarmente affinare la base di informazione sui rischi informatici presso i responsabili e acuirne la percezione. A tale scopo il Consiglio federale affida ai dipartimenti l'incarico di porre mano all'attuazione delle misure al loro livello in unione e in dialogo con le autorità cantonali e con l'economia. Le misure spaziano dall'analisi dei rischi per le infrastrutture TIC critiche a un più forte posizionamento degli interessi svizzeri in questo settore a livello internazionale.

Il Consiglio federale riconosce in questo senso che in Svizzera la collaborazione tra autorità ed economia è generalmente affermata e ben funzionante. Per il tramite della strategia nazionale di protezione della Svizzera contro i rischi informatici il Consiglio federale intende approfondire questa collaborazione e rafforzarne le fondamenta già esistenti, per abbordare in maniera mirata la riduzione a un minimo dei rischi informatici. Esso si fonda in merito sulle strutture esistenti e rinuncia a un organo centrale di condotta e di coordinamento come quello che viene attualmente istituito in altri Paesi, dove la collaborazione tra gli attori rilevanti è molto meno marcata. Occorre invece intensificare e diffondere in funzione delle necessità il flusso di informazioni e la valutazione complessiva delle informazioni esistenti sui rischi e sulle minacce a livello informatico per sostenere le autorità, l'economia e i gestori di infrastrutture critiche. A tale scopo va potenziata la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI.

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 L'Iran nel mirino? Flame e Wiper

Il 28 maggio 2012 Kaspersky Lab ha annunciato la scoperta di un programma nocivo molto complesso, utilizzato per attaccare e spiare organizzazioni in più Paesi. Le sue funzioni comprendono la raccolta di informazioni di qualsiasi genere. Il programma può ad esempio sorvegliare il traffico in rete, sorvegliare le digitazioni sulla tastiera, copiare il contenuto delle schermate, effettuare intercettazioni audio e addirittura leggere via *Bluetooth* le rubriche dei telefoni mobili situati nelle vicinanze se tale funzione è attivata sul telefono mobile. Questo programma nocivo, denominato «Flame», è stato particolarmente attivo in Medio Oriente. Circa la metà delle infezioni accertate si situa in Iran. Le prime versioni risalgono al 2006 – ragione per la quale la rete di spionaggio ha potuto operare in sordina per oltre cinque anni. Ciò non da ultimo perché gli aggressori continuano a infettare simultaneamente soltanto una dozzina di sistemi e perché «Flame» viene nuovamente disattivato dopo essersi procurato i dati sui sistemi colpiti. Pertanto, dopo che fu resa pubblica la scoperta del programma nocivo da parte di Kaspersky Lab, i cracker hanno disattivato il sistema di controllo della rete di spionaggio per fare sparire le loro tracce.

Per l'infrastruttura di controllo sono stati utilizzati per la durata dell'attacco oltre 80 *nomi di dominio* registrati e server situati in tutto il mondo, fra l'altro a Hong Kong, in Vietnam, in Turchia, ma anche in Germania, Inghilterra e Svizzera.

«Flame» si diffonde per il tramite di chiavette USB e reti locali. Nel caso delle infezioni tramite la chiavetta USB si sfrutta la medesima lacuna di sicurezza utilizzata da Stuxnet. L'analisi tecnica da parte delle ditte di sicurezza ha inoltre evidenziato diverse altre affinità tra «Flame», «Stuxnet» e «Duqu»[16].

Un programma nocivo denominato «Wiper» che nell'aprile del 2012 ha distrutto la rete di comunicazione del ministero del petrolio iraniano, ne ha letto i dati e ha infine cancellato completamente i dischi rigidi dei sistemi infettati. In Iran, per arginare «Wiper» e a titolo di misura di sicurezza, sono stati nel frattempo staccati da Internet i sistemi di computer del ministero del petrolio e di diversi terminali di trasbordo del petrolio.

Questi fatti evidenziano ancora una volta che non si tratta più di attacchi di spionaggio sporadici, bensì di un interesse persistente di accesso ai sistemi, ai dati e alle informazioni e che la pressione esercitata sui dati e sui sistemi sensibili aumenta ogni giorno. In merito è possibile che una rete di spionaggio possa operare per più anni senza essere scoperta. Occorre pertanto presumere che già fin d'ora siano stati piazzati altri software di spionaggio utilizzati in parallelo oppure approntati a titolo sostitutivo nell'ipotesi della scoperta di un attacco, per poter continuare a spiare e sabotare i sistemi e le reti già infiltrati. Cfr. in merito anche il capitolo 5.2.

[16] Cfr.: Rapporto semestrale MELANI 2010/2, capitolo 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de e Rapporto semestrale MELANI 2011/2, capitolo 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2012)

4.2 Hacktivismo in Vicino Oriente

Nel corso del mese di gennaio hacker pro e anti-israeliani si sono stati protagonisti di alcune scaramucce. Un hacker autodichiarato saudita, denominato «0xOmar», ha pubblicato i dati relativi alle carte di credito di migliaia di israeliani che ha potuto predare mediante attacchi alle banche dati di fornitori di servizi Internet. In risposta a questa azione un hacker israeliano denominato «0xOmer» ha pubblicato dati concernenti cittadini sauditi. Il giorno successivo all'appello di un portavoce dello Hamas che chiedeva di protestare contro l'occupazione della Palestina mediante attacchi ai siti Web israeliani, il sito della compagnia aerea israeliana e quello della borsa israeliana sono stati oscurati, attacchi poi vendicati con aggressioni di hacktivisti ai siti Web della borsa degli Emirati Arabi Uniti e dell'Arabia Saudita. Ciò ha nuovamente motivato un predicatore televisivo in Kuwait a invocare via Twitter una jihad informatica contro Israele. Pochi giorni dopo un hacker pro-israeliano ha pubblicato i dati di accesso a Facebook di migliaia di arabi, obbligando Facebook a resettare le password degli account violati. Dopo alcune altre operazioni di hackeraggio e la pubblicazione dei dati derubati, come pure attacchi alla disponibilità dei siti Web, le ostilità sono nuovamente scemate verso la metà del mese di febbraio.

Questi avvenimenti illustrano in maniera esemplare come conflitti politici possano essere fomentati anche da attori non statali, qualunque. Se alla pubblicazione di dati rubati da un hacker è allegata una dichiarazione politica, ciò provoca reazioni nel campo avverso. In questo modo gli hacker possono istigarsi a vicenda. Se nella fattispecie una parte è chiaramente nota, nella scelta del bersaglio l'altra parte si fonda anzitutto sull'autodichiarazione non garantita del primo aggressore. Nel corso degli avvenimenti sono però insorti dubbi sulla provenienza dell'iniziatore «0xOmar», ragione per la quale anche altri Paesi e l'Iran sono finiti nel mirino degli hacker pro-israeliani. Come per gli attacchi sferrati dagli Stati, nel caso di un hacktivismo di questo tipo si pone il problema dell'attribuzione. Finché l'aggressore non è stato identificato inequivocabilmente vi è il rischio che la vendetta sia rivolta all'indirizzo sbagliato, coinvolgendo un grande numero di persone estranee ai fatti.

4.3 Anonymous ha annunciato un attacco a Internet – Nessun danno quantificabile

Il 12 febbraio 2012 Anonymous ha annunciato che il 31 marzo avrebbe paralizzato i 13 *server root* di Internet come atto di protesta contro il progetto di legge statunitense «SOPA - Stop Online Piracy Act», Wallstreet, i politici irresponsabili, i banchieri e contro gli abusi in genere. L'appello ha suscitato grande interesse da parte dei media ma, come previsto, non ha provocato danni maggiori.

Con l'ausilio del Domain Name System (DNS) è possibile utilizzare in maniera conviviale Internet e i suoi servizi, poiché al posto degli *indirizzi IP* possono essere utilizzati gli indirizzi Web (*URL*). Internet funziona anche senza server *DNS*, ma al posto degli *URL* devono essere digitati gli *indirizzi IP*. Al massimo livello della gerarchia si situa il *root server*, cui competono come istanza superiore le informazioni riguardanti i *Top-Level-Domains* (p. es. .com, .net, .ch).

Dato che è essenziale per il funzionamento di Internet, nel *Root-Server DNS* sono implementati diversi meccanismi di sicurezza. Nel caso dei 13 Root-Server DNS non si tratta soltanto di 13 singoli server, bensì di un totale di 259 server presso differenti provider in diversi Paesi.

Nell'ipotesi del metodo di attacco «*DNS-Amplification Attack*» descritto da Anonymous si sfrutta il fatto che in determinate circostanze i server dei nomi rispondono a piccoli pacchetti

di richieste con grandi pacchetti di risposte. In teoria una richiesta lunga 60 byte può provocare una risposta di lunghezza superiore a 3000 byte. Queste grandi risposte devono successivamente essere dirette sui *Root-Server DNS* in modo da sovraccaricarli e paralizzarli. Questi server sono tuttavia dotati di enormi capacità per poter affrontare punte di carico. Così facendo si garantisce che il *DNS* funzioni anche se due terzi dei Root-Server dovessero subire un crash. A ciò si aggiunge il fatto che il crash di un *Server-Root DNS* ha ripercussioni soltanto se è paralizzato per un tempo relativamente lungo, dato che numerosi provider effettuano un salvataggio locale temporaneo delle richieste per ridurre il traffico sulla rete. I *Root-Server DNS* sono tuttavia sorvegliati in permanenza. Qualora fosse individuata un'anomalia il traffico nocivo verrebbe immediatamente bloccato. L'ultimo attacco è stato quello registrato nel 2007 ai danni di 2 dei 13 *Root-Server DNS*. Dato che gli altri server hanno continuato a funzionare perfettamente non vi furono tracce percettibili.

Un attacco a Internet non rientra nel modo di procedere di Anonymous che ha ad esempio dichiarato ripetutamente di non voler attaccare alcun media. Un attacco che coinvolgerebbe tutti gli utenti di Internet sarebbe indubbiamente controproducente e Anonymous perderebbe molti simpatizzanti. Per scatenare un simile attacco sarebbero inoltre necessari test preliminari del presunto tool e un grande numero di volontari. Diversi attivisti di Anonymous hanno preso le distanze da questo appello già nel caso dell'attacco preannunciato nel 2011 a Facebook.

La flessibilità del vincolo ad Anonymous sfocia in una serie di annunci e di attacchi non coordinati e più o meno spettacolari. Data l'assenza della qualità di membro nella struttura di Anonymous e che non esistono né un portavoce ufficiale né persone responsabili dell'intero movimento, chiunque può in linea di massima pubblicare comunicati a nome di Anonymous e suscitare in tal modo l'interesse dei media.

Anonymous intercetta una conferenza telefonica tra Scotland Yard e l'FBI

Gli attivisti di Anonymous sono riusciti a intercettare una conferenza telefonica confidenziale tra la polizia londinese Scotland Yard e l'FBI, la polizia federale statunitense. I contenuti sono stati peraltro pubblicati dagli attivisti su YouTube.

La conferenza telefonica trattava – oltre che di numerosi oggetti di scarsa importanza – anche di dettagli sulle indagini in corso concernenti Anonymous e «LulzSec», come la pianificazione delle date di arresto. Oltre al file audio della teleconferenza Anonymous ha parimenti pubblicato le e-mail con i dati di accesso alla teleconferenza. Una procedura penale è stata avviata[17].

4.4 Proteste contro ACTA – anche in Internet

All'inizio del 2012 in diversi Paesi vi sono state proteste contro il disegno di ratifica dell'accordo ACTA («Anti-Counterfeiting Trade Agreement»), un disegno di accordo commerciale multilaterale a livello di diritto internazionale. Con questo accordo le Nazioni contraenti intendono stabilire standard internazionali di lotta contro i prodotti della pirateria informatica e le violazioni del diritto di autore.

Queste proteste, volte a fare naufragare l'ACTA, si sono soprattutto svolte in forma di dimostrazioni tradizionali che hanno raggiunto il loro culmine l'11 febbraio 2012, la giornata

[17] http://www.spiegel.de/netzwelt/web/anonymous-attacke-hacker-veroeffentlichen-fbi-gespraech-mit-scotland-yard-a-813224.html (stato: 31 agosto 2012).

di azione paneuropea. Si sono però anche osservate numerose proteste in rete; ne menzioniamo alcune qui appresso:

Repubblica Ceca

Nella Repubblica Ceca sono stati derubati e pubblicati 27 000 record di dati concernenti i membri del partito di Governo ODS. Oltre all'indirizzo privato i record di dati comprendevano anche il numero di telefono dei membri del partito. Il 6 febbraio 2012 la ratifica dell'ACTA è stata sospesa sine die.

Polonia

Diversi siti Web del Governo polacco sono stati paralizzati temporaneamente da attacchi *DDoS*. Sembra che dietro a questi attacchi si celino la cellula polacca di Anonymous e il gruppo di hacker «Polish Underground». Alcuni attivisti hanno inoltre infiltrato il sito Web del Comune di Kraszewniki[18], lasciando un comunicato. Anche in questo caso il Governo ha deciso di sospendere la ratifica dell'ACTA.

USA

Nel contesto delle proteste contro l'ACTA, Anonmyous avrebbe hackerato numerosi siti Web della FTC, la commissione US per il commercio. Sarebbero stati colpiti sette siti Web, ma non la pagina principale.

Grecia

Venerdì 3 febbraio 2012 alcuni hacker del movimento Anonymous hanno attaccato il sito Web del ministero della giustizia greco. In questo contesto si è protestato contro le misure di risparmio, ma anche contro la partecipazione della Grecia all'accordo l'ACTA. Per quattro ore di seguito sul sito Web del ministero sono stati proiettati messaggi di protesta. Gli hacker hanno impartito al Governo due settimane di tempo per recedere dall'accordo ACTA. Se l'ultimatum non fosse stato rispettato sarebbero seguiti altri attacchi.

Slovenia

Nel quadro delle proteste contro l'ACTA la cellula slovena di Anonymous ha paralizzato temporaneamente numerosi siti Web, fra i quali quello del partito di Governo SDS e di altri partiti. Lo stop alla ratifica è giunto il 7 febbraio 2012.

In Svizzera le proteste sono state molto meno marcate. Questo anche perché in Svizzera il cittadino può ricorrere al referendum e all'iniziativa, oltre che ad altri strumenti a livello politico. Vi sono state piccole dimostrazioni, soprattutto a Zurigo, mentre non sono state osservate dimostrazioni di maggiore entità né attacchi alla rete, come in altri Paesi europei. Sebbene la Svizzera abbia partecipato all'elaborazione e ai negoziati dell'ACTA, il Consiglio federale ha comunicato il 9 maggio 2012 di non volere per il momento firmare l'accordo.

Le proteste contro l'accordo ACTA costituiscono un ulteriore esempio del fatto che le proteste si spostano sempre più verso lo spazio virtuale. Esse evidenziano altresì una grande sensibilità dei cittadini nei confronti delle tematiche riguardanti Internet. Ogni limitazione e regolamentazione è considerata con particolare scetticismo perché a Internet viene associato uno spazio ancor sempre libero e talvolta privo di coercizioni legali.

[18] http://www.kraszewniki.pl/ (stato: 31 agosto 2012).

4.5 Furto in massa di password e di dati di carte di credito

Il primo semestre del 2012 è stato nuovamente caratterizzato da diversi attacchi a ditte rinomate presso le quali sono stati derubati dati di clienti, prevalentemente dati di login e dati di carte di credito.

In questo senso nella settimana del 4 giugno 2012 sono stati ad esempio pubblicati sui pertinenti forum oltre 6 milioni di valori di password *SHA*-1-*Hash* della rete professionale online «LinkedIn». *SHA*-1 è una funzione crittografica hash molto diffusa, che genera a partire da qualsiasi messaggio un valore hash di 160 bit (checksum). Da questo valore hash può sovente essere ricostruita la password. Numerose password sono già state pubblicate. Nei documenti pubblicati mancavano invero gli indirizzi e-mail corrispondenti (che fungono da nome di utente), ma occorre nondimeno presumere che anche questi dati siano stati rubati e siano in mano agli aggressori.

Poche ore dopo che l'evento è stato reso pubblico sono comparse le prime pagine Web di *phishing* che sollecitavano gli utenti a «verificare» le loro password LinkedIn.

Accesso alla banca dati della filiale di Amazon «Zappos»

Degli sconosciuti hanno avuto accesso ai dati personali e rubato la password hash di circa 24 milioni di clienti US registrati presso la filiale di Amazon «Zappos». Fortunatamente nella banca dati erano registrate di volta in volta soltanto le ultime quattro cifre della carta di credito. Gli autori non hanno potuto accedere ai server sui quali sono memorizzate altre informazioni e il numero completo della carta di credito[19].

Attacco ai dati delle carte di credito presso Global Payments

Non ha invece fruito della medesima fortuna l'elaboratore di carte di credito «Global Payments». Nel suo caso sarebbero stati sottratti 1,5 milioni di record di dati di numeri di carte di credito. Sembra che alla base del furto dei dati ci sia stato l'attacco a una società di taxi di New York[20]. Nel corso di questo attacco gli aggressori sono riusciti ad procurarsi l'accesso a un conto di amministratore dell'impresa di taxi e ad accedere, per alcuni mesi, ai dati delle carte di credito. Tali dati non stati utilizzati immediatamente, ma i truffatori li hanno raccolti per poterli usare tutti a un determinato momento. Essi hanno evitato che il furto fosse notato e che eventuali contromisure potessero diminuirne il rendimento.

Furto di 450 000 nomi di utente e di password dalla «Content Börse Yahoo! Contributor Networks»

Nel primo semestre del 2012 Yahoo ha subito un attacco. Il gruppo di hacker «D33Ds Company» ha sottratto e pubblicato in rete circa 450 000 nomi di utente e password della «Content Börse Yahoo! Contributor Networks»[21]. Secondo quanto riferisce Yahoo è stata sfruttata abusivamente una lacuna di sicurezza del sistema di computer, che è poi stata immediatamente colmata. Secondo il gruppo di hacker «D33Ds Company» la banca dati non sarebbe stata sufficientemente protetta e le password non sarebbero state memorizzate in forma codificata. L'attacco doveva essere inteso come segnale di sveglia per gli amministratori responsabili della banca dati.

---

19 http://online.wsj.com/article/BT-CO-20120116-706917.html (stato: 31 agosto 2012).

20 http://blogs.gartner.com/avivah-litan/2012/03/30/new-credit-card-data-breach-revealed/ (stato: 31 agosto 2012).

21 http://www.focus.de/digital/internet/datenbank-muehelos-geknackt-hacker-veroeffentlichen-zugangsdaten-von-450-000-yahoo-nutzern_aid_781269.html (stato: 31 agosto 2012).

Comparsa su Twitter di 50 000 nomi di utente e password

Il 9 maggio 2012 hanno fatto la loro comparsa anche su Twitter oltre 50 000 nomi di utente e password. Twitter ha successivamente promesso di resettare i conti interessati. Restano ignoti l'origine dei dati e gli autori dell'attacco. È probabile che la qualità dei dati non sia stata abbastanza elevata, perché vi figuravano numerosi doppioni, conti già bloccati o contenenti false indicazioni (fake accounts)[22].

Hackeraggio di conti GMX

Il provider di posta elettronica GMX ha constatato almeno 3000 casi di account violati. Inizialmente si era ritenuto che gli attacchi fossero stati perpetrati mediante un attacco *Brute Force*. Questo modo di procedere è però limitatamente adatto nel caso di prestazioni di servizi online, perché un attacco di questa portata sarebbe rapidamente identificato. È molto più probabile che gli aggressori siano stati in possesso dei dati di login e delle password. In questo senso GMX ha confermato che i nomi di utente e le password erano stati immessi in maniera molto mirata. Non è noto come siano state sottratte le password. Si potrebbe però trattare di password rubate in un altro contesto – in altre parole presso altri fornitori di servizi – e successivamente «testate» sui conti GMX[23]. Un simile approccio non è fuorviante dato che per tutti i servizi di Internet numerose persone utilizzano sempre una sola ed unica password.

Secondo «Firehost» gli attacchi alle pagine Internet per il tramite di *SQL-Injections* sono aumentati del 69 per cento tra aprile e giugno del 2012[24]. Nel caso delle *SQL-Injection* si tenta di inviare comandi manipolati alla banca dati. Nella maggior parte dei casi ciò è effettuato mediante un'interfaccia mal programmata, che non verifica o verifica insufficientemente i comandi inviati, oppure attraverso una lacuna di sicurezza. È così che si possono spiare i dati dei clienti, manipolare gli shop online e anche semplicemente distruggere intere collezioni di dati. Un attacco riuscito, la perdita dei dati dei clienti e di reputazione che ne risulta possono costare rapidamente molto denaro e addirittura rovinare una società. Anche in questo caso è utile tenere sempre aggiornato il software dei siti Web e proteggere bene questi ultimi dagli attacchi esterni.

Oggigiorno è indispensabile utilizzare password diverse per le diverse prestazioni di servizi online. Ciò comporta un miglioramento in termini di sicurezza, anche che se per ricordarsi queste password occorre segnarle da qualche parte (su carta).

4.6 SCADA – Aggiornamento

Un gruppo di fornitori di servizi di sicurezza ha pubblicato nel mese di gennaio del 2012 le lacune di sicurezza delle componenti degli impianti industriali di comando. Questa pubblicazione ha suscitato inquietudini sia presso i produttori, sia presso gli esercenti. Infatti coloro che hanno scoperto le lacune di sicurezza non ne hanno informato preliminarmente i produttori, affinché tali lacune potessero essere colmate entro la vigilia della pubblicazione. Le lacune sono pervenute direttamente a conoscenza dell'opinione pubblica, suscitando numerose critiche.

---

22 http://www.spiegel.de/netzwelt/web/twitter-passwoerter-im-netz-a-832171.html (stato: 31 agosto 2012).

23 http://www.zeit.de/digital/datenschutz/2012-07/gmx-passwort-account (stato: 31 agosto 2012).

24 http://www.heise.de/newsticker/meldung/Deutlicher-Anstieg-der-SQL-Injection-Angriffe-1651041.html (stato: 31 agosto 2012).

Chi ha individuato le lacune di sicurezza voleva da un canto mostrare come fosse semplice compromettere i sistemi *SCADA*. D'altro canto l'azione era stata pensata come promemoria per i produttori. Sembra che il gruppo abbia già cumulato esperienze dalle quali risulterebbe che i produttori conoscono da diversi anni alcune lacune di sicurezza e che invece di sopprimerle tempestivamente ne abbiano ritardato il più a lungo possibile la loro pubblicazione e il loro aggiornamento[25]. Occorre aggiungere che un aggiornamento dei sistemi *SCADA* non è paragonabile all'aggiornamento di un PC, poiché ogni aggiornamento dei sistemi di controllo comporta il rischio di errori di funzionamento che a seconda delle circostanze possono avere gravi ripercussioni.

La grande differenza rispetto al software usuale dei computer risiede nel fatto che da un canto i produttori mancano finora di esperienza nella rimozione delle lacune di sicurezza e che, d'altro canto, lo svolgimento in continuo dei processi ne consente un aggiornamento soltanto durante determinate finestre di manutenzione. Anche le ripercussioni di *patch* sull'intero processo possono essere testate in anticipo solo in parte. Il principio «don't touch a running system» si applica nella misura in cui le avarie e i crash possono provocare rapidamente ingenti costi.

In origine i sistemi *SCADA* avevano poche affinità con le TIC usuali: essi erano isolati dalle reti di computer, possedevano hardware e software proprietari e utilizzavano protocolli propri per comunicare con il calcolatore centrale. Questa situazione è cambiata radicalmente nel corso degli ultimi anni, da quando sono disponibili apparecchiature a prezzi accessibili con interfaccia integrata sul protocollo Internet. Nella maggior pare dei casi queste componenti non dispongono (ancora) di un collegamento a Internet, ma è comunque possibile che un *software nocivo* infiltri questi sistemi separati attraverso un laptop infetto oppure una *chiavetta USB*. Dato che le componenti *SCADA* non sono predisposte per supportare elementi di sicurezza come *firewall* e *software di protezione antivirus*, poche barriere si oppongono agli aggressori che sono ormai già penetrati nella rete.

Possibile attacco agli impianti di binari ferroviari US

Secondo un rapporto della «Transportation Security Administration TSA» statunitense, il 1° dicembre 2011 si è verificato un guasto a un impianto ferroviario nel nordovest degli Stati Uniti, apparentemente provocata da due accessi ignoti con indirizzi IP non americani. Ne sono risultati ritardi di 15 minuti. Il giorno successivo si sarebbe verificato un secondo accesso, che non ha però provocato alcuna perturbazione. Non è stato reso noto chi esattamente si celasse dietro questi accessi. Il Dipartimento della sicurezza interna ha comunque indicato che poteva essere escluso un attacco mirato. I dati relativi ai tre indirizzi IP all'origine dell'accesso erano stati messi a disposizione di altre imprese di trasporto negli Stati Uniti e in Canada[26].

Protesi che presentano vulnerabilità

Il fatto che non ci si debbano attendere solo attacchi con gravi ripercussioni a grandi sistemi, ma che anche piccoli sistemi possano subire danni vitali è evidenziato dal seguente esempio: in uno studio alcuni esperti di sicurezza hanno verificato le protesi mediche dal profilo dei loro rischi. Ne è risultato senza grande sorpresa che gli stimolatori cardiaci presentano un notevole rischio per la sicurezza. Sono noti a tutti i segnali di avvertimento ai

---

25 http://www.heise.de/security/meldung/Sicherheitsexperten-setzen-Hersteller-von-Industriesteuerungen-unter-Druck-1418292.html (stato: 31 agosto 2012).

26 http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/ (stato: 31 agosto 2012).

portatori di stimolatori cardiaci in prossimità di apparecchiature a forte radiazione magnetica. Nel corso di un test i ricercatori hanno irradiato un impianto defibrillatore con onde radio, con il risultato che l'impianto ha smesso di funzionare. Sono inoltre state individuate altre terrificanti vulnerabilità. In questo senso ad esempio i link WiFi utilizzati per la funzione di aggiornamento comportano lacune che possono essere sfruttate. Nella peggiore delle ipotesi ciò provoca la disattivazione del singolo apparecchio (ad esempio nel caso delle pompe per l'insulina) con tutte le relative conseguenze a livello di salute[27].

4.7 Creazione di un Centro europeo sulla criminalità informatica

Il 28 marzo 2012 la Commissione europea ha proposto la creazione di nuovo Centro europeo sulla criminalità informatica presso Europol, l'autorità europea di polizia con sede all'Aia. Europol coordina già attualmente le attività delle autorità nazionali europee di polizia nel settore della criminalità organizzata transfrontaliera e promuove lo scambio di informazioni tra le autorità nazionali di polizia.

Il centro che deve focalizzare la propria attività sulla lotta contro il ciberterrorismo in Europa sarà operativo dal 1° gennaio 2013. In questo ambito dovranno essere riunite le informazioni e le esperienze, si dovrà offrire sostegno alle inchieste criminali e si dovranno promuovere soluzioni a livello europeo come pure la percezione della criminalità informatica. Il Centro istituirà inoltre una comunità di esperti provenienti da tutti i settori della società per combattere in maniera più efficace la criminalità informatica e la pornografia infantile[28].

Il continuo aumento della comunicazione via Internet e del suo sfruttamento commerciale va anche di pari passo con un incremento dei casi di truffa e di altri reati in Internet. Nelle indagini sono regolarmente coinvolte centinaia di vittime in diverse parti del mondo. Nella maggior parte dei casi le tracce degli autori portano in più Paesi e interessano pertanto numerose giurisdizioni. Indagini di questa portata e complessità non possono più essere il fatto esclusivo di singole forze nazionali di polizia, mentre le procedure tradizionali e prolisse di assistenza giudiziaria raggiungono i loro limiti di efficienza. Nessun reato è internazionale come la criminalità informatica. Per poterla perseguire con efficacia è necessario un approccio coordinato, comune e transfrontaliero. È esattamente su questo punto che il Centro europeo sulla criminalità informatica deve intervenire e fornire un complemento di ausilio.

4.8 Disattivazione di una rete bot Zeus

Unitamente ai fornitori di servizi finanziari, all'Information Sharing and Analysis Center (FS-ISAC) della Electronic Payments Association (NACHA) e allo specialista di sicurezza IT Kyrus, Microsoft ha adito il tribunale distrettuale di New York. Il 23 marzo 2012 il tribunale ha disposto una perquisizione domiciliare, eseguita dagli sceriffi federali, in due edifici di uffici negli Stati della Pennsylvania e dell'Illinois. Sono stati sequestrati diversi *server Web*,

---

27 http://www.pcwelt.de/news/Sicherheitsrisiko-Medizinische-Implantate-als-Zielscheibe-fuer-Hacker-5708296.html (stato: 31 agosto 2012).

28 https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417 (stato: 31 agosto 2012).

sospettati di essere utilizzati nell'ambito di una rete bot Zeus. Affinché la perquisizione fosse effettivamente possibile Microsoft ha percorso nuove vie giudiziarie: in collaborazione con organizzazioni del settore finanziario è stata promossa contro i gestori della rete bot Zeus una causa civile e non una causa penale. Le prime azioni di Microsoft sono state dirette contro ignoti. Nel mese di luglio Microsoft ha successivamente pubblicato due nomi in connessione con la rete bot Zeus. Yevhen K. E Yuriy K sono già agli arresti in Gran Bretagna[29].

Nel caso di questo modo di procedere non ci si è focalizzati sulla distruzione della rete bot. Una rete bot della complessità di Zeus non può essere semplicemente disattivata. Si trattava piuttosto di ripartire il lavoro e i costi sugli esercenti di queste reti nella speranza che alla lunga l'esercizio non ne fosse più stato redditizio.

Ad avvenuta perquisizione non si sono però elevate soltanto voci positive. In questo senso «FoxIT», un fornitore di servizi di sicurezza dei Paesi Bassi, a pubblicato alcune osservazioni critiche a proposito dell'operazione di Microsoft. [30]

4.9 Infezioni drive-by – Diffusione tramite le insegne pubblicitarie

Nel mese di maggio 2012 è stato propagato *software nocivo* sul sito Web www.wetter.com per il tramite di una lacuna di sicurezza del software per insegne pubblicitarie *OpenX*. Non si sa per quanto tempo questa infezione sia stata attiva sul sito di wetter.com. A seconda delle circostanze è stato installato *software nocivo* all'insaputa dei visitatori del sito. Al CERT.at è noto che esistono diverse varianti di *software nocivo* diffuso per questo tramite, fa le quali una era un *cavallo di Troia* (*ransomware*)[31]. In merito ai trojan che bloccano i computer si vedano anche il capitolo 3.5, nonché il rapporto semestrale MELANI 2011/2, capitolo 3.5[32].

Le infezioni di siti Web costituiscono attualmente il vettore più utilizzato di diffusione di *software nocivo*. Nell'ambito di tale diffusione svolgono un ruolo primordiale i server centrali che mettono a disposizione diversi contenuti di siti Web. La compromissione può avere conseguenze estremamente vaste soprattutto nel caso della pubblicità online, ma anche nel caso dei servizi di statistica.

Le modalità di manipolazione del software utilizzato assumono grande importanza in ambito di offerenti di pubblicità su Internet, ma anche di offerenti di altri contenuti. In tale contesto tutti i programmi devono sempre essere mantenuti aggiornatissimi. Proprio nel caso di questi servizi vale in definitiva il principio secondo il quale un sito Web può essere altrettanto sicuro del suo punto più debole. Si tratta sovente di offerte di terzi iniettate sul sito Web e quindi incontrollabili da parte del gestore del sito Web.

---

29 http://www.golem.de/news/botnet-microsoft-nennt-zwei-mutmassliche-betreiber-von-zeus-1207-92930.html (stato: 31 agosto 2012).

30 http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/ (stato: 31 agosto 2012).

31 http://www.cert.at/warnings/all/20120516.html (stato: 31 agosto 2012).

32 Cfr.: Rapporto semestrale MELANI 2011/2, capitolo 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2012).

5 Tendenze / Prospettive

5.1 Fusione di imprese e di TIC privata – un rischio per la sicurezza?

Se in precedenza si osservava una stretta separazione tra vita privata e vita professionale, tale frontiera è attualmente divenuta flessibile: da un canto le imprese si aspettano che i collaboratori siano raggiungibili anche all'infuori delle ore d'ufficio e lavorino anche di sera (e al proprio domicilio) sotto la pressione delle scadenze e, d'altro canto, in ufficio i collaboratori utilizzano le TIC anche a scopi privati. Essi fanno ad esempio capo al loro indirizzo privato di posta elettronica o curano le loro reti sociali. A ciò si aggiunge che la richiesta degli strumenti più moderni è onnipresente anche nel mondo del lavoro. Come è possibile che il collaboratore che utilizza uno *smartphone* ultramoderno a titolo privato possa accontentarsi di un telefono mobile aziendale senza funzioni supplementari? Se la ditta non reagisce il collaboratore utilizzerà presto o tardi lo *smartphone* privato per porre in sintonia gli iter di lavoro con i propri desideri e le proprie necessità. È ovvio che ciò comporti una sfida ulteriore per i responsabili TIC delle imprese. Il fatto che vengano utilizzati computer che non situati nella rete aziendale (controllata), ma all'infuori del posto di lavoro, è infatti fonte di nuovi pericoli.

Comporta pericoli supplementari lo scambio di dati tra computer aziendali e computer privati mediante *chiavette USB* oppure CD. Come insegna l'esperienza le chiavette USB sono volentieri sfruttate come veicolo di trasmissione di attacchi mirati per accedere alle reti aziendali. A tale scopo l'aggressore infetta il computer privato (mal protetto) di un collaboratore e si introduce in maniera completamente inosservata nella rete aziendale tramite un media di memorizzazione esterno. A ciò si aggiunge l'aggravante che – come nel caso di un evento che colpisce un computer privato – le indagini sono molto difficili perché manca tipicamente una registrazione secondo le norme dell'attività del computer e dell'attività di rete. Nel caso ad esempio di un attacco mirato con *software nocivo* via la posta elettronica aziendale esiste ancora una possibilità di verificare a posteriori se le e-mail siano effettivamente arrivate e state aperte, mentre tale possibilità è generalmente inesistente nel caso delle reti private.

Questa evoluzione illustra in maniera esemplare quale sia l'importanza di un approccio integrale della sicurezza. In questo senso non si pongono soltanto questioni classiche di sicurezza TIC, ma piuttosto questioni organizzative: Chi ha accesso a quali dati? I collaboratori sanno quali dati possono essere prelevati dalla rete aziendale? Quali apparecchi si possono introdurre nell'azienda ed essere collegati alla rete aziendale? Nelle zone di sicurezza basta bloccare le porte USB o devono essere vietate anche le videocamere handy? Si pone in genere la questione se le apparecchiature di lavoro non debbano essere consegnate in maniera relativamente ampia e anche essere dotate di ampi diritti di uso privato. Anche se ciò dovesse comportare maggiori spese amministrative all'azienda, sarebbe perlomeno garantito il controllo degli apparecchi e delle applicazioni che girano su di essi, perché essi appartengono pur sempre al datore di lavoro e sottostanno al suo controllo.

I meccanismi tecnici di sicurezza sono irrinunciabili, ma non offrono una sicurezza al 100%. Occorre prescindere dalla protezione esclusiva dei computer e delle reti sulle quali sono conservate le informazioni e concentrarsi sulla protezione dell'informazione. Ciò comporta una gestione rafforzata dell'informazione e dei dati, la classificazione delle informazioni e simili. Si presuppone peraltro una chiara ponderazione dei rischi che deve sfociare nell'adeguamento del valore effettivo di un'informazione alla sicurezza dei canali di distribuzione, dei diritti di accesso e dei luoghi di memorizzazione. Non ogni canale o luogo

di memorizzazione è ugualmente sicuro e non tutti i documenti di un'azienda sono ugualmente sensibili. In molti casi le TIC sono generalmente considerate come un fattore di costi e corrispondono, nella visione della direzione, a una mera funzione logistica e di supporto. Le TIC come parte del processo di tutela dell'informazione devono essere obbligatoriamente integrate nel processo di gestione aziendale e strategica dei rischi a motivo dei loro fattori critici. Anche la tutela dell'informazione costituisce pertanto parte integrante della gestione strategica dei rischi e del concetto di sicurezza e si situa quindi al medesimo livello strategico della protezione degli edifici e delle persone, del controlling finanziario ecc.

5.2 Conflitto informatico in Vicino Oriente

Con l'inizio della primavera araba e la caduta dei primi regimi sono anche venuti alla conoscenza del pubblico documenti e informazioni che comprovavano il fatto che singoli Stati arabi utilizzavano tecnologie sofisticate proveniente dall'Occidente per la sorveglianza su Internet dei critici del regime. Anche gli Stati nei quali non si sono verificati disordini oppure si è assistito a disordini meno violenti hanno apparentemente utilizzato programmi e infrastrutture per una sorveglianza possibilmente capillare delle comunicazioni. Gli affari realizzati con simili soluzioni TIC hanno conosciuto un boom e, come già descritto nel rapporto semestrale MELANI 2011/2[33], si tratta di una problematica complessa che non consente una semplice visione in bianco e nero. Differenti avvenimenti in diversi focolai di crisi e di conflitto in Vicino Oriente evidenziano nondimeno che nel settore dei mezzi TIC sussiste una vasta gamma di attori e di mezzi che va ben oltre la sorveglianza delle comunicazioni: in questo senso il programma nocivo «Stuxnet» e i suoi moduli accessori dimostrano chiaramente l'efficienza dei mezzi basati sulle TIC quando vengono sviluppati con sufficienti risorse e con la copertura dello Stato e utilizzati a scopo di sabotaggio o di spionaggio. Come illustrato nel capitolo 4.2 anche gruppi non statali partecipano virtualmente ai conflitti in Vicino Oriente. In merito è difficile valutare chi esattamente si celi dietro questi movimenti di protesta, in quale misura essi siano sostenuti più che ideologicamente dallo Stato e come essi si incitino vicendevolmente all'azione. A tale scopo essi utilizzano una vasta gamma di *phishing* di dati, che spaziano da attacchi alla disponibilità dei siti Web a deturpazioni virtuali che riscuotono favore unanime, i cosiddetti defacement. Anche dal profilo organizzativo e propagandistico si fa capo ai vantaggi offerti da Internet. In questo senso gli attivisti di qualsiasi provenienza si organizzano tramite Facebook, Twitter e simili, oppure postano foto e video ripresi con gli handy per consolidare le loro dichiarazioni e rivendicazioni in rete, fermo restando che il contesto reale può difficilmente essere ricostruito integralmente in maniera probante.

Pertanto non sorprende affatto che si tenti di infiltrare nelle forme più diverse non soltanto i conti di posta elettronica degli avversari, ma anche i gruppi sulle reti sociali per carpirne indicazioni sulle azioni in progetto e per procurarsi l'identità dei partecipanti, come pure ulteriori informazioni utili: già prima della primavera araba si è ad esempio avuto conoscenza di azioni per il tramite delle quale critici del regime viventi all'estero sono stati sommersi da attacchi mirati. Ma anche i membri di regimi autoritari e i loro familiari possono essere disturbati dai servizi di intelligence esteri, come evidenziato dall'esempio della pubblicazione degli acquisti via iTunes di Bashar al-Assad[34].

---

[33] Cfr.: Rapporto semestrale MELANI 2011/2, capitolo 5.3: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2012).

[34] http://www.guardian.co.uk/world/2012/mar/14/assad-itunes-emails-chris-brown (stato: 31 agosto 2012).

Il fabbisogno in aumento di tecnologie (centrali) di sorveglianza, i sabotaggi TIC, l'uso di immagini come materiale di propaganda fino al discredito di singole persone sulla base di e-mail personali derubate sono un'emanazione dell'impiego di tutti i mezzi TIC disponibili da parte dell'uno o dell'altro partito in una regione da sempre instabile e sotto tensione.

Il Vicino Oriente è attraversato da disordini, crisi e dai più diversi potenziali di conflitto non soltanto dall'epoca della primavera araba.Con lo scoppio delle dimostrazioni e dei disordini alcuni di questi conflitti subcoscienti sono entrati in un nuovo stadio, oppure le vecchie difficoltà finora celate sotto un coperchio sono affiorate in pubblico. Anche in Vicino Oriente l'impiego delle TIC non risale soltanto a questi eventi ed esplosioni, che si tratti di comunicazione, di sorveglianza (centrale) della comunicazione o anche in ambito di sistemi *SCADA* oppure ancora di supporto a processi aziendali o di produzione. La diffusione aperta dei conflitti dall'inizio della primavera araba va di pari passo con un aumento dell'uso di mezzi TIC aggressivi e offensivi e di Internet.

Si ha regolarmente notizia di casi di disattivazione di siti Web, di sottrazione di documenti di Stato e privati o di uso di *malware* in un intento di sabotaggio. A prescindere da questa inondazione dei servizi Web 2.0 con messaggi, video e spezzoni di informazione sulla presunta situazione sul posto – e fermo restando che tutte le parti in causa si avvalgono di questa tecnica e che una verifica o una ricostruzione sono sovente impossibili – ad acuire il tutto si aggiunge il fatto che i mezzi basati sulle TIC sono spesso relativamente a buon mercato, dispongono di un vasto raggio di azione, il che li rende attraenti per tutti i partecipanti.

In questa misura il conflitto informatico in Vicino Oriente che viene diffuso su più livelli è anzitutto una manifestazione collaterale dei conflitti reali e delle realtà sul posto. In questo senso anche gli eventi in questo ambito e il loro contesto non vanno intesi e compresi come singoli avvenimenti – come presentato volentieri nei media – bensì integrati in un complesso generale che consenta di effettuare una valutazione approfondita di quanto mostrato, accaduto e annunciato.

5.3 Furto di dati: attacchi a numerose piccole e a poche grandi imprese

Continuano a fare titolo nei media attacchi ai dati dei clienti di grandi ditte e in particolare di dati delle carte di credito. Oltre agli eventi di attualità descritti nel capitolo 4.5 vanno ricordati i numerosi attacchi del passato: a titolo di esempio la perdita dei dati dei clienti presso Sony lo scorso anno, l'incidente avvenuto presso la catena di vendita anglo-americana TJX nel 2005, incidente nel corso del quale sono stati derubati sistematicamente sull'arco di un anno e mezzo oltre 45 milioni di record di carte di credito, oppure l'incidente occorso nel 2009 all'elaboratore di carte di credito Heartland.

Uno studio effettuato dall'impresa dell'impresa statunitense di sicurezza Verizon[35] con dati del 2011 provenienti dall'US Secret Service e dalle polizie australiana, dei Paesi Bassi e irlandese mostra tuttavia che gli attacchi alle grandi imprese costituiscono soltanto una piccola parte degli attacchi. Sul totale di 855 incidenti annunciati e concernenti complessivamente 174 milioni di record di dati compromessi, soltanto una piccola parte riguardava gli incidenti occorsi alle grandi imprese. Ai casi in parte molto spettacolari ammessi fanno raffronto numerosi attacchi a ditte di minori dimensioni e ai loro dati, che si

[35] http://securityblog.verizonbusiness.com/category/ask-the-data/ (stato: 31 agosto 2012).

verificano quotidianamente sotto i radar dei media. In oltre il 75% dei casi si tratta di attacchi a PMI con meno di 1'000 collaboratori.

Le grandi imprese si preparano bene ai rischi informatici e dispongono nella maggior parte dei casi di un team di sicurezza TIC e anche di un CSO, mentre questa sensibilità fa ancora difetto presso numerose imprese di minori dimensioni. Molte ditte continuano a praticare un approccio molto insensibile ai dati dei clienti e delle carte di credito. A cosa serve ad esempio la trasmissione sicura di un'ordinazione se poi i dati sono memorizzati senza codificazione sul computer?

Una parte dei criminali sfrutta spietatamente questa circostanza perché essi operano all'insegna del principio della minore resistenza possibile e ricercano gli obiettivi «più semplici». A tale proposito ci si avvale sovente di metodi automatizzati di attacco e si ricercano sistematicamente note lacune di sicurezza e configurazioni nei siti Web e nelle banche dati per poi derubarne i dati. Per i criminali può rivelarsi estremamente proficuo attaccare al posto di una grande impresa numerose piccole ditte, questo con un minore dispendio ma anche con un utile minore – ovvero con meno record di dati.

Le grandi imprese non devono però credersi al sicuro. Per alcuni criminali che dispongono di un grande know-how tecnico e di buone capacità può rivelarsi proficuo un maggiore dispendio sull'arco di un tempo più lungo. In ambito di spionaggio si è pertanto affermato il concetto di *Advanced Persistent Threat* (APT), utilizzato prevalentemente per gli attori statali senza vantaggio finanziario diretto. Se l'utile corrisponde in definiva a quanto ci si aspettava può rivelarsi proficuo da parte dei criminali un attacco mirato, estremamente professionale e preparato per lunghi mesi. Diversamente dallo spionaggio statale al centro figura l'intento finanziario.

5.4 Comunicazione con i clienti nell'era del *phishing*

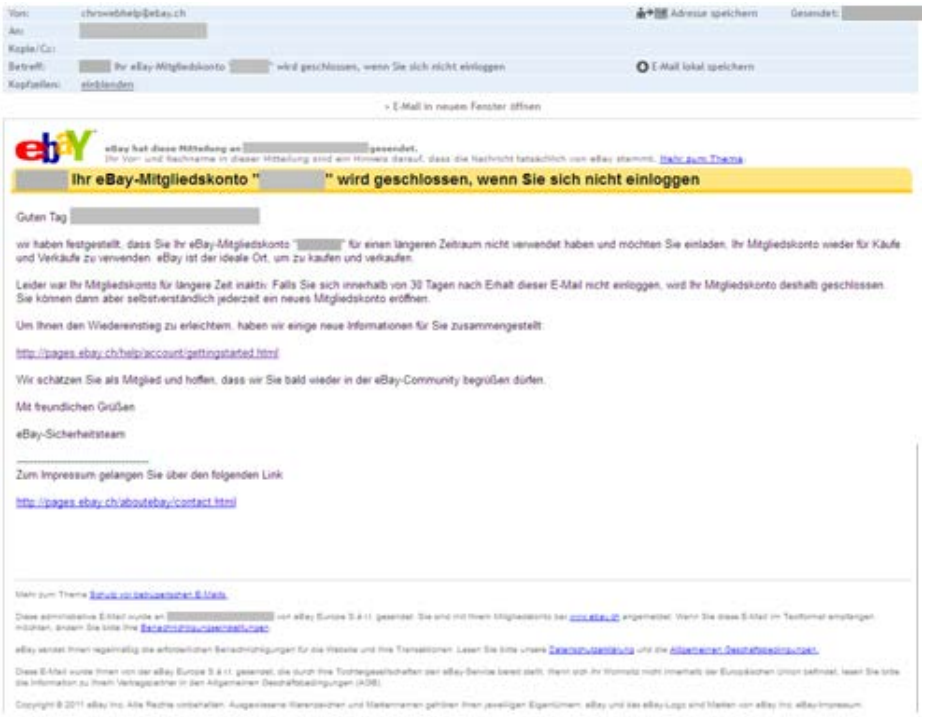
«Nessuna ditta seria vi chiederebbe mai i vostri dati di login e la vostra password via e-mail». Questa è la risposta standard che MELANI fornisce sempre alle persone che annunciano una e-mail della quale non sono sicure se pervenga effettivamente o no dalla ditta in questione. Nell'era della comunicazione elettronica con i clienti questa affermazione, inizialmente semplice, pone talvolta le ditte dinanzi a determinate sfide. Quali sono le modalità di comunicazione di una ditta con i suoi clienti affinché essi non considerino fraudolente le loro e-mail? Più importante ancora: una comunicazione troppo spensierata da parte di una ditta ai propri clienti può influenzare negativamente il comportamento della clientela per quanto riguarda le e-mail fraudolente?

Verifica dei clienti in eBay

Diamo qui di seguito un esempio che illustra in maniera esemplare il dilemma che devono fronteggiare le imprese:

eBay invia sporadicamente e-mail di verifica dei membri quando essi non hanno effettuato il login sul loro conto per un certo periodo di tempo. È ovvio che si tratta di una procedura necessaria perché altrimenti i conti non utilizzati da più anni su eBay potrebbero accumularsi.

Sebbene non venga richiesta direttamente l'immissione del none di utente e della password , l'e-mail suscita immediatamente presso alcuni destinatari sensibili un certo scetticismo, in particolare se il conto del cliente è appena stato utilizzato di recente per partecipare a un'asta.



Ihr eBay-Mitgliedskonto " " wird geschlossen, wenn Sie sich nicht einloggen

Guten Tag

wir haben festgestellt, dass Sie Ihr eBay-Mitgliedskonto " " für einen längeren Zeitraum nicht verwendet haben und möchten Sie einladen, Ihr Mitgliedskonto wieder für Käufe und Verkäufe zu verwenden. eBay ist der ideale Ort, um zu kaufen und verkaufen.

Leider war Ihr Mitgliedskonto für längere Zeit inaktiv. Falls Sie sich innerhalb von 30 Tagen nach Erhalt dieser E-Mail nicht einloggen, wird Ihr Mitgliedskonto deshalb geschlossen. Sie können dann aber selbstverständlich jederzeit ein neues Mitgliedskonto eröffnen.

Um Ihnen den Wiedereinstieg zu erleichtern, haben wir einige neue Informationen für Sie zusammengestellt:

http://pages.ebay.ch/help/account/gettingstarted.html

Wir schätzen Sie als Mitglied und hoffen, dass wir Sie bald wieder in der eBay-Community begrüßen dürfen.

Mit freundlichen Grüßen

eBay-Sicherheitsteam

Zum Impressum gelangen Sie über den folgenden Link:

http://pages.ebay.ch/aboutebay/contact.html

Figura 8: E-mail di eBay per la verifica dei clienti

Modifica delle CGA presso PayPal

Un altro caso che ha provocato annunci a MELANI è quello della modifica delle CGA che PayPal ha invito a mezzo e-mail a fine giugno. Nonostante il fatto che l'e-mail non contenesse alcun link alla pagina di login, la sola circostanza che gli utenti ricevessero inaspettatamente una e-mail da parte di PayPal ha suscitato una forte insicurezza.

Newsletter di Svizzera Turismo

MELANI ha parimenti ricevuto richieste consecutive all'invio di una e-mail da parte di Svizzera Turismo lo scorso 31 maggio 2012. I link che essa conteneva non rinviavano ai domini di Svizzera Turismo, bensì a un altro server svizzero denominato «crm.stnet.ch». I link erano inoltre molto complicati e lunghi, circostanza che ha indotto i destinatari a chiedere a MELANI di verificare l'esattezza di questa e-mail.

Betreff: Mit allen Wassern gewaschen

Falls der Newsletter nicht korrekt dargestellt wird, klicken Sie hier <http://crm.stnet.ch/crm/service/nlweb?bpid= language=de&chk=iSXRD6ASZf> .

<http://crm.stnet.ch/content/campaign_data/content_804302666/Headerde.jpg>
<http://crm.stnet.ch/content/campaign_data/content_980099386/Mainimage.jpg>
<http://crm.stnet.ch/content/campaign_data/content_804302666/juerg-foto-Sommer.jpg>

Grüezi

Freuen Sie sich auf Ferien, die prickeln. Unser Reiseland steht diesen Sommer ganz im Zeichen des Wassers. Spri
<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Fempfehlungen%2Fstaedtereisen
3D47010&b -1&chk=3fJxLXXDLW&ganame=Newsletter+05%2F2012_CHdefr> oder geheimnisvo
<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Ferlebnisse%2Fwandern.html%3F
3D25527& &chk=6VAZSFLJaD&ganame=Newsletter+05%2F2012_CHdefr> in einer atember
haben für Sie das Beste herausgepickt.

Finden Sie uns im Netz

<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.facebook.com%2FMySwitzerland&bpid=
<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%
2Ftwitter& &lid=4&chk=D6xD9RVRAR&ganame=Newsletter+05%2F2012_CHdefr> <http://crm.
2Fwww.youtube.com%2Fmyswitzerland&b &lid=5&chk=2DeDD32Te2> <http://crm.stnet.ch/cr
2Fwww.flickr.com%2Fphotos%2Fswitzerland_tourism%2F&b lid=6&chk=XXWJhOFADF>
Viel Genussreiches wartet auf Sie. Lassen Sie sich erfrischen von unseren Ideen rund ums Element Wasser!

<http://crm.stnet.ch/content/campaign_data/content_804302666/Juerg.gif>

Jürg Schmid, Direktor Schweiz Tourismus

Figura 9: E-mail pubblicitaria di Svizzera Turismo con link al dominio stnet.ch

Nuova iscrizione alla newsletter di MELANI

Anche MELANI non è immune da simili problemi. Dato che dal mese di giugno 2012 la newsletter di MELANI è stata trasferita sul portale di informazione della Confederazione e che per motivi tecnici non è stato possibile trasferire la banca dati con tutti gli indirizzi di posta elettronica registrati, tutti gli abbonati alla newsletter di MELANI hanno dovuto essere informati della necessità di una nuova iscrizione qualora avessero manifestato ulteriormente il loro interesse per la newsletter di MELANI.

Una simile impresa è difficile e deve essere pianificata minuziosamente. MELANI ha tentato di risolvere questo problema annunciando questo modo di procedere in una e-mail preliminare e fissando esattamente la data di invio dell'e-mail. L'e-mail è stata inviata in pieno formato testo e conteneva unicamente un link che dirigeva anche sui domini di MELANI, in maniera analoga alle precedenti newsletter. I nuovi abbonati non sono stati invitati in nessun momento a immettere la loro password (ma a sceglierne una nuova). La pagina iniziale di MELANI recava inoltre un chiaro rimando all'invio. Nonostante questo modo di procedere non sono mancate le reazioni – che si sono comunque mantenute entro i limiti. Un tempo rapido di reazione alle domande dei clienti durante e dopo l'invio della newsletter costituisce altresì uno strumento utile per contenere l'insicurezza. Ciononostante anche in questo caso sussiste un potenziale di miglioramento, come ad esempio l'utilizzazione nell'e-mail di un link a una pagina cifrata (https).

Nel caso dell'invio di newsletter dovrebbero essere osservati i seguenti punti:

- Inviare nella misura del possibile le e-mail sotto forma di pieno testo.
- Inviare le e-mail di news in maniera possibilmente regolare.
- Fare un uso parsimonioso di link e dirigere i link unicamente sui propri domini. Utilizzare nella misura del possibile link a pagine cifrate (https) e darne comunicazione anche ai destinatari.
- Non inserire link a siti Web che esigono l'immissione del nome di utente e della password oppure altri dati.
- Rinviare sulla pagina iniziale del sito Web alla newsletter o collegare direttamente l'informazione a un link affinché il destinatario abbia la possibilità di inserirvi manualmente l'indirizzo principale e di cliccare da lì la newsletter.
- Rivolgersi al cliente con il nome e il cognome sempreché questa informazione sia disponibile.

5.5 e-voting in Svizzera – Esperienze attuali

Nel 2000 è stato avviato in Svizzera il progetto «Vote électronique» – ovvero la possibilità di esprimere elettronicamente il proprio voto. Il primo esperimento pilota è stato effettuato nel 2003 in un piccolo Comune del Cantone di Ginevra, dove un numero percettibile di cittadini e di cittadine ha avuto la possibilità di esprimere elettronicamente il proprio voto nel quadro di una votazione comunale. Questo primo esperimento pilota ha suscitato grandi ondate a livello internazionale ed è stato menzionato in maniera corrispondente da rinomati giornali svizzeri ed esteri.

Dall'epoca di questo primo esperimento il Consiglio federale ha autorizzato più di 100 esperimenti nel quadro di votazioni popolari federali. In occasione della votazione popolare federale del 25 novembre 2012 si effettuerà il 115 esperimento di voto elettronico. Se vi si aggiungono i numerosi altri esperimenti a livello cantonale e comunale, nonché diversi esperimenti nel quadro di elezioni, il numero di esperimenti di voto elettronico in Svizzera è di molto maggiore. Nonostante questo numero elevato di esperimenti si sono verificati unicamente alcusi incidenti con conseguenze limitate (si veda ad esempio il capitolo 3.7).

L'e-voting svizzero è comunque sicuro? L'analisi succinta qui appresso intende esaminare queste questioni:

Attualmente solo un numero limitato di elettori svizzeri può esprimere elettronicamente il proprio voto. Nel frattempo l'autorizzazione al voto elettronico è stata invero estesa agli Svizzeri all'estero. Per il momento tuttavia è improbabile per diversi motivi che un esperimento di «Vote électronique» affetto da errori possa comprometterne il risultato finale:

- Le dimensioni dell'elettorato sono scelte in maniera tale che anche in caso di risultati stretti si possa presumere che l'avaria parziale o totale del sistema elettronico non abbia molto probabilmente alcun influsso sul risultato finale. Attualmente sono soprattutto gli Svizzeri all'estero a ricorrere al voto elettronico.

- Le urne elettroniche devono sempre essere chiuse prima delle urne fisiche il sabato precente la domenica di voto. Queste misure devono ad esempio consentire che in caso di avaria totale del sistema elettronico (p. es. in caso di crash a livello nazionale dei collegamenti Internet o in caso di un efficace attacco DDoS) sussista per gli elettori la possibilità di esprimere fisicamente il proprio voto nei locali di voto.

Oltre a queste misure organizzative esiste tutta una serie di misure tecniche destinate ad assicurare che i principi sanciti dalla «Legge federale sui diritti politici» e dall'«Ordinanza sui diritti politici» (unicità del voto, anonimità del voto e confidenzialità del voto) siano garantiti.

Come è però la situazione se la maggior parte della popolazione fa capo a questa prestazione di servizi? È soprattutto in caso di utilizzazione capillare dell'e-voting in tutta la Svizzera che le misure qui sopra non funzionano più o soltanto limitatamente:

- Un attacco alle urne elettroniche è sicuramente improbabile: in questo caso i voti espressi sono conservati in maniera codificata fino al momento del loro conteggio. Il tempo relativamente breve durante il quale il voto elettronico è possibile non dovrebbe bastare per decodificare e falsificare tempestivamente i voti anche in caso di attacco *Brute Force* massiccio. Anche un attacco riuscito non comporterebbe probabilmente alcun influsso sul risultato della votazione: i limiti attuali (il 10 % al massimo dell'elettorato federale può votare elettronicamente) sono predisposti in maniera tale che il risultato finale non possa essere pregiudicato neppure in caso di avaria totale del sistema o di manipolazione dei voti.

- Cionondimeno non si può ovviamente escludere che una volta o l'altra possa riuscire un attacco ai sistemi del «Vote électronique». Si potrebbe ad esempio ipotizzare un attacco *DDoS* ai sistemi elettronici tale da impedire gli Svizzeri all'estero di esprimere tempestivamente il loro voto.

- Il maggiore problema è sicuramente costituito delle insicure apparecchiature di immissione (sistemi cliente) assieme all'assenza di ricostruibilità e di capacità di prova. Numerose possibilità di attacco (vettori) che riguardano attualmente l'e-banking in Internet possono addirittura anche prendere di mira direttamente o in forma semplificata l'e-voting. Le misure di protezione previste in ambito di e-banking in Internet – procedure di autentificazione e di sorveglianza delle transazioni – non funzionano in questo caso. Per via di conseguenza la situazione di minaccia è notevole e il cliente costituisce il tallone d'Achille dell'e-voting[36]. Se viene installato un software nocivo sul computer dell'elettore, tale programma può manipolare a piacimento il risultato della votazione. Ad esempio il codice il codice nocivo introdotto

[36] https://www.e-voting-cc.ch/index.php/de/workshops/workshop09/programm09/87 (stato: 31 agosto 2012).

nel browser ha per effetto che ogni volta che viene inviato un valore parametrico «Sì» al server di e-voting tale valore parametrico è convertito in «No» prima ancora della sua codificazione. Ad avvenuta codificazione il codice nocivo può parimenti manipolare l'immagine di sicurezza restituita dal server di e-voting in maniera tale che l'elettore non si accorga di nulla. Un simile scenario di attacco è in particolare grave se viene utilizzato in maniera capillare e se una grande quantità di voti può essere manipolata[37]. Le moderne tecnologie di e-voting, come la cosiddetta «verificabilità», consentono comunque di individuare tempestivamente simili attacchi.

La verificabilità serve a individuare eventuali manipolazioni dei voti. Se un virus modifica il voto di un elettore, la manipolazione può essere rilevata con un sistema verificabile. La verificabilità può essere attuata ad esempio in una prima fase trasmettendo all'elettore un codice per ogni oggetto (o candidato, in caso di elezioni) dopo l'invio del voto. L'elettore confronta questo codice con il codice personale, ricevuto con il materiale di voto. Dato che i codici sono diversi per ogni oggetto in votazione (risp. candidato) e per elettore, il virus non può «sapere» quale codice visualizzare per fuorviare l'elettore.

La grande differenza tra l'e-voting e l'e-commerce si situa a livello di tolleranza di errore dei sistemi. Nel caso delle prestazioni elettroniche di servizi una certa percentuale di truffe è senz'altro tollerata e anche pagata dalle ditte – le ditte risparmiano infatti denaro facendo capo alle prestazioni elettroniche di servizi – mentre nel caso delle votazioni via Internet il risultato del voto deve rispecchiare la volontà dell'elettorato. Tutto il resto sminuirebbe la fiducia del cittadino nella democrazia.

Un allargamento dell'elettorato al voto elettronico deve essere subordinato all'introduzione della verificabilità.

[37] http://data.rrb.zh.ch/appl/rrbzhch.nsf/0/C12574C2002FAA1FC1257942004EB439/$file/Evaluation_E-Voting_Z%C3%BCrich.pdf (stato: 31 agosto 2012).

6 Glossario

Allegato/Attachment	Un allegato al file (inglese: «attachment») è un file inviato come allegato al testo di una e-mail.
Antivirus Software	I software antivirus proteggono i vostri dati dai virus, dai vermi informatici o dai cavalli di Troia.
Attacco brute force	Metodo di attacco nel cui ambito sono semplicemente provate tutte le potenziali soluzioni/password finché viene rintracciata quella giusta.
Attacco DDoS	Attacco Distributed-Denial-of-Service Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di acce-dere al computer eludendo le normali protezione di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.
Backup	Backup (in italiano: salvaguardia dei dati) designa la copia di dati nell?intento di poterli ricopiare in caso di perdita.
Bluetooth	Una tecnologia che consente la comunicazione senza fili tra due apparecchi finali e utilizzata soprattutto in ambito di telefonia mobile, di laptop, di PDA e di dispositivi di immissione (ad es. il mouse del computer).
Certificato digitale	Certifica l'appartenenza di una chiave pubblica (PKI) a un soggetto (persona, elaboratore).
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).
DNS Amplification Attack	Attacco di Denial of Service (DoS), che sfrutta abusivamente server DNS accessibili al pubblico e li utilizza come amplifier (amplificatore).
DNS Root-Server	I server root dei nomi, o semplicemente root server, sono server per la risoluzione dei nomi alla radice (root) del Domain Name System in Internet. La zona del root server comprende i nomi e gli indirizzi IP di tutti i server di nomi di tutti i Top-Level-Domains.

Domini	Il nome di dominio (ad es. www.example.com) può essere ri-solto dal DNS (Domain Name System) in un indirizzo IP che può poi essere utilizzato per istituire collegamenti con questo computer.
E-Commerce	Nel quadro delle attività economiche su Internet il concetto di e-commerce è ampiamente sintetizzato come commercio e-lettronico.
E-government	Per e-government si intende la semplificazione e l'esecuzione di processi con l'ausilio di tecniche digitali di informazione e di comunicazione tra le istituzioni statali, comunali e altre istituzioni delle autorità, come pure tra queste istituzioni e i cittadini, rispettivamente le imprese.
Event-Viewer	Programma cha visualizza messaggi di errore e di servizio nel sistema operativo Windows.
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere – ossia sul vostro computer.
Funzione hash MD5	Algoritmo che genera costantemente una serie di cifre di uguale lunghezza a partire da qualsiasi testo. Le funzioni hash sono utilizzate in tre settori: - nella crittografia; - nei sistemi di banche dati. Essi le utilizzano per effettuare ricerche più efficienti nelle grandi raccolte di dati delle banche dati; - nelle somme di controllo. Un valore hash può essere attribuito a qualsiasi file. Un valore hash modificato fa presagire una manipolazione.
Geoportale	Portale Web che mette a disposizione informazioni geografiche.
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.
IP-Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).

Macchina di archiviazione Internet	Servizio di Internet che archivia a intervalli determinati e poi rimette a disposizione una pagina Web di tutti/numerosi siti Web. I vecchi siti Web non più raggiungibili sono pertanto ancora sempre visibili.
Malicious Code	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Toia, nonché le Logic Bombs.
OpenX	OpenX è un software open source che mette a disposizione una gestione delle insegne pubblicitarie.
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.
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.
PHP-Mailer	Programma PHP che invia testo tramite una funzione e-mail. PHP è un linguaggio script utilizzato prevalentemente per l'allestimento di pagine Web dinamiche o di applicazioni Web.
Ransomware	Malware tramite il quale i proprietari dei computer infettati sono ricattati (ransom: termine inglese per riscatto). Nel caso tipico i dati sono cifrati e nuovamente messi a disposizione dall'aggressore dopo il pagamento del riscatto per la chiave di decodificazione necessaria al loro ripristino.
Recovery Process	Recovery (in italiano: ripristino dei dati) significa il ripristino dei dati originali dopo la loro perdita.
Remote Administration Tool	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manu-tenzione a distanza di qualsiasi computer o sistema di computer.
SHA	Secure Hash Algorithm (inglese per algoritmo hash sicuro) Il concetto di SHA designa un gruppo standardizzato di funzioni crittografiche hash. Esse servono a calcolare un valore univoco di

	veri-fica per qualsiasi dato elettronico.
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Smartphone	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
Spoofing	Nella tecnica informatica sono denominati spoofing (italiano: manipolazione, camuffamento o simulazione) diversi tentativi di inganno sulle reti di computer per mascherare la propria identità.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L'aggressore tenta di intro-durre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
Top-Level-Domains	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separate da un punto. La designazione Level-Domain si riferisce all'ultimo nome di questa successio-ne e costituisce il livello più elevato della risoluzione del nome. Se ad esempio il nome completo di dominio di un compu-ter, rispettivamente di un sito Web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome.
Trojan che bloccano i computer	Malware che provoca un blocco del computer ed esige successivamente il pagamento di un riscatto dal proprietario.
Trojan per il perseguimento penale	Software utilizzato dalla polizia nel quadro di un'inchiesta penale, per intercettare ad esempio le conversazioni VoIP.
URL	Uniform Resource Locator L'indirizzo Web di un documento composto dal protocollo, dal nome del server e dal nome del documento con il percorso (esempio: http://www.melani.admin.ch/test.html).
USB Memory Stick	Piccoli dispositivi di memoria che possono esser raccordati al computer per il tramite di un'interfaccia USB.
Voice phishing	Genere di truffa nel cui ambito la vittima è indotta

	tramite una conversazione telefonica a rivelare i propri dati di accesso.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.