



MARCELLO PISTILLI
Business
Development
Manager
Information
Security
Eustema S.p.A.

HOMELAND SECURITY

L'Homeland Security è la difesa da attacchi dolosi mediante un'approfondita conoscenza delle condizioni di esercizio delle grandi infrastrutture e della loro vulnerabilità. Una vulnerabilità che, pur essendo quasi organica nel caso degli apparati informatici, può essere ridimensionata ricorrendo alle armi dell'attenzione e della consapevolezza.

■ L'accesso alle risorse

È fondamentale che l'accesso all'apparato informatico sia identificato univocamente, subordinandolo all'immissione di specifiche credenziali (user-Id e password). Attualmente l'attivazione di numerosi dispositivi avviene mediante sensori e algoritmi biometrici, una soluzione che prevede la misurazione di determinate caratteristiche fisiche e il confronto con quelle precedentemente acquisite.

Se l'apparato è utilizzato da più persone è bene creare più ambienti, uno per ciascun soggetto, ai quali accedere con credenziali diversificate. È inoltre opportuno lasciare sempre attiva la funzionalità di salva schermo (screensaver), che si avvierà in caso di no-

stra assenza e richiederà l'inserimento di una password per ripristinare l'operatività dell'apparato.

Per essere efficaci le password dovrebbero avere una lunghezza minima di 8 caratteri e soddisfare requisiti minimi di complessità quali: presenza di lettere maiuscole e minuscole; caratteri speciali (. ; \$! @ - > <); numeri; stringhe non riconducibili alle informazioni personali dell'utente. Le parole d'accesso dovrebbero essere cambiate frequentemente, almeno ogni 90 giorni, e non dovrebbero essere riutilizzate successivamente. Naturalmente ne è sconsigliata la trascrizione su fogli volanti o la comunicazione verbale.

■ Cura e aggiornamento contro le minacce del Web

Poiché il funzionamento dell'apparato informatico si basa sul Sistema Operativo, è importante che quest'ultimo, al pari di tutte le altre applicazioni, sia sempre originale, ben configurato e aggiornato. Se non curati, OS e SW possono esporre l'intero sistema a grandi rischi. Gli aggiornamenti rilasciati periodicamente dai produttori, infatti, non si limitano a risolvere errori preesistenti ma mirano a fronteggiare

nuove minacce provenienti dalla Rete, come i malware. La "cura" di tali aspetti rappresenta un tassello fondamentale nella difesa dalle principali minacce presenti sul Web.

Un malware è un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Può essere del tipo Virus, Worm, Trojan e Spyware.

■ Il backup

L'integrità del proprio apparato informatico e delle informazioni in esso contenute passa anche dal backup periodico del sistema operativo. Si tratta di un salvataggio-copia dell'intero stato del sistema: il nuovo "ambiente" ospiterà tutte le informazioni necessarie a ripristinare la configurazione di computer, driver e altri dispositivi in caso di guasto o attacco informatico.

Naturalmente la perdita di documenti e informazioni è un evento che non può essere scongiurato completamente, il più delle volte a causa del "fattore umano". Sovra-scritture o cancellazioni accidentali rappresentano probabilmente la causa principale della perdita di informazioni. All'imperizia o disattenzione bisogna poi aggiungere i malware, oltre ad eventuali guasti o malfunzionamenti dei dispositivi di archiviazione. Per cercare di ridurre al minimo tali eventualità sarà opportuno effettuare periodicamente delle copie di riserva su supporti esterni come hard disk, DVD o supporti remoti messi a disposizione dai fornitori di connettività.

■ La crittografia

Per accrescere il livello di riservatezza e di sicurezza dei dati memorizzati all'interno degli apparati informatici è possibile ricorrere a soluzioni di crittografia per i singoli documenti o, in modo ancora più efficace, per le stesse directory che li contengono.

La crittografia è il sistema che, mediante uno specifico algoritmo e una chiave di cifratura, permette di variare i messaggi testuali (messaggio in chiaro) in simboli non comprensibili senza una specifica e corrispondente chiave di lettura. Quest'ultima, naturalmente, andrà conservata in un posto sicuro.

■ Wi-Fi domestico e Soho

Negli ultimi anni si è assistito a un vero e proprio boom della tecnologia di accesso a Internet senza fili, sia per la sua capacità di soddisfare qualsiasi esigenza di mobilità, sia per l'indiscutibile comodità e flessibilità che la contraddistingue. Al tempo stesso, però, la tecnologia wireless presenta numerose vulnerabilità e insidie. Gli access point assicurano la possibilità di collegarsi alla Rete tramite onde radio e l'area di copertura sferica generata da questi dispositivi travalica ostacoli fisici quali mura e soffitti. In assenza di una corretta configurazione della stazione access point e della stessa postazione utente, il rischio che estranei possano carpire i nostri dati o sfruttare per altri scopi la nostra connessione è elevatissimo.

Abbandonando il protocollo WEP (Wired Equivalent Privacy), dimostratosi insicuro, si può far fronte alle insidie delle reti WiFi domestiche ricorrendo a meccanismi di protezione più efficaci quali WPA-PSK (Wireless Protected Access - Pre-Shared Key) o WPA2-PSK (anche detti WPA/WPA2 Personal). Entrambi i protocolli prevedono l'utilizzo di una password condivisa (i.e.: pre-shared) tra l'access point e le stazioni e impiegano meccanismi di crittografia delle informazioni più robusti rispetto al WEP.

■ E-mail

Per la sua semplicità, immediatezza, diffusione, l'e-mail è probabilmente considerata il più "utile" ed efficace strumento di comunicazione globale. Ma le stesse ragioni sono anche alla base del successo di cui essa gode presso nutrite schiere di delinquenti hi tech, impegnati prevalentemente nelle frodi informatiche. A prescindere da eventuali declinazioni particolari, una frode informatica punta a intercettare dati sensibili che verranno utilizzati successivamente per scopi malevoli. Questo tipo di reato è cresciuto parallelamente allo sviluppo in Rete dell'e-commerce e delle banche on line e si è progressivamente affinato con l'evoluzione dell'ingegneria sociale, lo studio

dei comportamenti individuali per estorcere informazioni. Le frodi vengono messe in atto ricorrendo a tecniche di spamming e phishing.

Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, fino a discutibili progetti finanziari o a veri e propri tentativi di truffa. Spesso il testo del messaggio è proposto in un italiano approssimativo, frutto dell'attività di un traduttore automatico. Lo spammer, cioè l'individuo autore dei messaggi spam, invia messaggi identici a migliaia di indirizzi e-mail, raccolti in maniera automatica dalla rete oppure ottenuti dalla commercializzazione dei database. A differenza di quanto avviene con la posta tradizionale, la spedizione e la consegna di queste e-mail hanno un costo che non è sostenuto dal mittente, ma dal ricevente. Per difendersi, oltre ai filtri anti spam presenti nelle offerte di qualsiasi provider, può giovare una buona dose di diffidenza.

Attraverso le e-mail possiamo essere raggiunti anche da messaggi ben più insidiosi e pericolosi: quelli di phishing o pishing. Il phishing è una tecnica illegale per raccogliere dati sensibili come





le informazioni sulla carta di credito o gli accessi ad account bancari. Per ottenere tali informazioni gli autori della frode inviano false e-mail con grafica e logo ufficiale di siti privati o istituzionali come ebay, paypal, ma anche di servizi bancari e di società che emettono carte di credito. Solitamente questi messaggi richiedono la compilazione di un modulo su una pagina web con indirizzo internet presente nella stessa e-mail. Per arginare ogni forma di rischio è opportuno verificare sempre tutte le mail con spirito critico, coscienti che difficilmente le nostre coordinate bancarie saranno richieste via mail dalla nostra banca. Prima di "cliccare" controllare l'effettivo link della pagina web cui il messaggio ci rimanda... molte volte esso riporta nomi di fantasia difficilmente identificabili con siti ufficiali.

■ Navigare sicuri

Per ridurre la portata dei rischi presenti in Rete si può comunque ricorrere ad una delle numerose soluzioni offerte dalla tecnologia, sia proprietarie che open source, come la barra del browser che cambia il proprio colore, virando al rosso se il sito sul quale si sta navigando non è attendibile o etico, gli antivirus, i personal firewall, i cleaner.

L'antivirus è un applicazione che ricerca nella memoria del computer o all'interno dei file la presenza dello schema tipico dei malware, una stringa di byte cui corrisponde un preciso numero di istruzioni. Il successo di questa tecnica di ricerca si basa sul costante aggiornamento degli schemi che l'antivirus è in grado di riconoscere. Solitamente il processo di aggiornamento che rende efficace la soluzione viene eseguito in automatico dalla stessa applicazione.

Il personal firewall è un programma che controlla le comunicazioni in entrata e in uscita dal PC, permettendole o vietandole in base a regole di sicurezza preimpostate o impostate dall'utente. Il suo compito principale è quello di analizzare il traffico e monitorare, eventualmente bloccandoli, i tentativi che provano a stabilire una connessione con il nostro apparato da parte di applicazioni esterne. Analogamente il personal firewall è anche in grado di controllare i programmi del nostro computer che possono trasmettere informazioni, bloccando l'invio di dati non autorizzati verso l'esterno.

I cleaner sono prodotti che permettono il mantenimento generale del sistema. Oltre ad eliminare i file inutili dalle cartelle e i parametri superflui dei registri, rimuovono i file temporanei e quelli di log più datati, cancellano la cronologia, la cache, i cookie e le chiavi di registro invalide, risolvendo i problemi riscontrati con estensioni, riferimenti e collegamenti mancanti. La pulizia e il riordino dei registri di sistema coincide con l'eliminazione di file "vulnerabili" e quindi potenzialmente attaccabili da diversi generi di malware. Secondo una recente analisi condotta da Trend Micro sarebbero oltre 1,5 milioni i computer "infetti" nel nostro Paese. Una volta infettata, la macchina viene integrata in una botnet, ossia una rete di bot (Pc comandati a distanza), una vera e propria infrastruttura dalla quale malintenzionati e organizzazioni criminali lanciano attacchi malware, compiendo un'ampia serie di attività finalizzate al furto di informazioni (credenziali, password, dati bancari...). Al momento, le tre reti bot più estese e conosciute sono: Koobface, Zeus/Zbot e Ilomo/Clam-

pi. Un attacco di tipo DoS (denial of service) cerca di portare il funzionamento di un qualsiasi sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni. Saturandone le risorse con l'invio di grandissime quantità di "pacchetti" di richiesta, compromette il sistema impedendo l'accesso ai suoi servizi da parte degli utenti abilitati. Gli attacchi di tipo DoS sfruttano solitamente computer di utenti inconsapevoli nei quali è stato precedentemente inoculato un programma ad hoc. Tale programma si attiva ad un comando proveniente dall'attaccante. Se il programma maligno è diffuso su molti computer, può succedere che migliaia di apparati informatici producano inconsapevolmente e nello stesso istante un flusso incontenibile di dati che travolgerà come una valanga il sito bersaglio.

■ Conclusioni

Nell'era di Internet è fondamentale accettare che la sicurezza informatica travalica i confini fisici del proprio edificio, coinvolge l'educazione e gli apparati dei soggetti con cui si viene direttamente o indirettamente a contatto, richiede specifiche conoscenze. Si deve acquisire la coscienza che la tecnologia, per quanto amichevole e utile, può essere impiegata anche a nostro danno, mettendo in pericolo i nostri cari e il nostro lavoro.

Si tratta quindi di un aspetto che deve entrare a far parte del bagaglio culturale di ciascuno di noi. Naturalmente la creazione della consapevolezza e l'opera di sensibilizzazione sulla sicurezza informatica non possono prescindere dall'iniziativa pubblica.

Governo e Parlamento devono mettere a disposizione le risorse necessarie, economiche e legislative, per far sì che la tutela esterna si traduca sempre più nell'autotutela di chi vive e opera su Internet. Soltanto in presenza di questa attenzione "dal basso" si potranno garantire contemporaneamente la sicurezza e una forma di autoregolamentazione, eliminando all'origine anche la semplice possibilità di "gestioni restrittive" o a carattere coercitivo della Rete. ■



*ANTONINO
LUCANTONIO,
DANILA PITOTTI*

MODELLI, SOLUZIONI E TECNOLOGIE ICT PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE PORTUALI

I porti costituiscono i nodi infrastrutturali critici della rete di comunicazione navale, pertanto necessitano di metodi e strumenti di Homeland Security per la gestione di azioni di risposta a catastrofi antropiche o naturali tanto più significative quanto più è elevato il volume e la pericolosità del relativo traffico merci e passeggeri. Tutto ciò è possibile attraverso un'adeguata comprensione del contesto organizzativo, dei metodi di analisi del rischio, del modello informativo delle soluzioni e delle tecnologie ICT a supporto della sicurezza dei porti. HP, in questo articolo, espone la propria visione e le proprie competenze frutto delle esperienze acquisite worldwide.

■ Il contesto organizzativo

La sicurezza portuale deve considerare molti aspetti, alcuni dei quali di seguito riportati:

- l'elevato traffico di beni, mezzi ed individui coin-

volti nella "filiera" marittima: ad esempio l'elevato numero di "container" che vengono quotidianamente lavorati nei porti commerciali ed industriali e l'elevato numero di passeggeri che, con i propri mezzi di trasporto, transitano durante il periodo estivo nei porti turistici;

- i porti sono le aree di sosta e di spedizione di beni quando diverse risorse devono essere mobilitate in caso di catastrofi globali, o di operazioni quotidiane nazionali, come centri di raccolta, ordinamento, classificazione e distribuzione.
- i porti sono nodi di passaggio di forniture critiche importanti come energia, alimenti e materiali pericolosi. Non solo esiste la necessità di gestire carichi pericolosi noti o dichiarati, ma è anche cruciale la necessità di individuare e gestire elementi ad alto rischio in carichi normali.

Ci sono diverse modalità di trasporto internazionale dei beni da sorgente a destinazione, su rotta, gomma, via fiume, via mare, via aereo. E'