Che cosa è il “Penetration Test” a cosa serve, come si svolge

© Copyright 2014 Claudio Ballicu, Tutti i diritti riservati

I rischi informatici

Non sempre i server aziendali o, comunque, i collegamenti tramite internet, sono privi di rischi imprevisti. A volte, infatti, la scarsa competenza tecnica di chi usa la “rete” costituisce l’anello debole della catena, aprendo così la porta all’ingresso di software maligni, i cosiddetti “malware”.

Si tratta di codici di programmazione in grado di spiare quanto viene digitato sulla tastiera del computer, per poi inviare questi dati, via internet, a server esterni o a caselle di posta elettronica anonime dalle quali è impossibile, o estremamente difficile, risalire all’utente reale.

Anche le vulnerabilità interne al sistema, possono consentire a un dipendente infedele di accedere a zone riservate o a files contenenti dati classificati il cui accesso deve essere riservato esclusivamente agli aventi diritto. Si pensi, solo per fare un esempio, ai dati riguardanti offerte commerciali o alla partecipazione a gare d’appalto, la cui conoscenza potrebbe portare consistenti vantaggi alla concorrenza e altrettanto pesanti conseguenze economiche per la vittima.

Secondo uno studio della Price Waterhouse Coopers, un network internazionale che fornisce servizi di revisione di bilancio, advisory e consulenza legale e fiscale, a causa dello spionaggio industriale, le prime mille aziende del mondo perdono ogni anno, mediamente, la bellezza di cinquantatré miliardi di dollari!

Non si creda però che la sicurezza informatica riguardi solamente le grandi aziende o i maggiori imprenditori; gli accessi al proprio conto corrente bancario, via internet, per leggere il saldo disponibile o eseguire un normale bonifico o i numeri della propria carta di credito, digitati per effettuare un acquisto a distanza, sono operazioni che riguardano oramai anche il singolo cittadino e che, nel prossimo futuro, vedranno un sempre maggiore numero di utenti.

Il web sta cambiando, rapidamente, e con esso stanno cambiando, rapidamente, le minacce, che diventano sempre più sottili, elaborate e intrusive.

Se, fino a tempi abbastanza recenti, l’intrusione abusiva nei computer altrui mediante l’iniezione di pericolosi “malware” era un’azione portata a termine da singoli pirati del web, spesso giovanissimi “smanettoni” dotati di notevoli conoscenze informatiche, oggi esistono delle vere e proprie organizzazioni criminali, fornite di elevati mezzi economici e ramificazioni internazionali, dedite esclusivamente alla ricerca sistematica delle falle dei vari sistemi operativi o delle ingenuità dei singoli utenti.

Nel mondo globalizzato e interconnesso nel quale viviamo, le transazioni bancarie, anche

relative a somme importanti, viaggiano alla velocità della luce e comunque molto più rapide del tempo necessario a prendere contatto con il centro antifrode della propria carta di credito, nel tentativo di bloccare l'emorragia di denaro dal conto corrente: quando riusciremo, il danno sarà già fatto.

Sperare di riavere indietro i soldi illecitamente sottratti è poco più che un'utopia: le somme transitano spesso in conti correnti dislocati nei più noti paradisi fiscali, dove conoscere l'identità di un correntista, a prescindere dalla limpidezza di suoi movimenti bancari, è semplicemente impensabile. "Pecunia non olet" dicevano i latini; "il denaro non ha odore" e, in certi luoghi, non lascia neppure tracce della sua provenienza, aggiungo io.

Altrettanto difficile è sperare di veder puniti questi moderni bucanieri degli oceani informatici, anche quando fossero individuati, a causa delle problematiche connesse con le rogatorie internazionali necessarie per avviare le indagini. I paesi dove originano questo genere di frodi informatiche sono scelti con oculatezza e con una profonda conoscenza delle leggi locali.

Le difese possibili

In breve, le difese che è necessario mettere in atto per difendersi da simili evenienze si possono riassumere in una sola parola: prevenzione!

La prevenzione, almeno ai livelli più basilari, passa attraverso l'uso accorto dei migliori software antivirus, dei migliori firewall e attraverso la conoscenza, almeno approssimativa, del pericolo.

Spesso però, tutto ciò non è sufficiente; i moderni telefoni cellulari "smart phone" e i tablet, ad esempio, sono frequentemente usati per le transazioni bancarie o per acquisti telematici. In questi dispositivi è raro trovare la presenza di un valido antivirus, con le conseguenze che è facile immaginare. Il fattore umano, soprattutto, costituisce spesso l'anello debole della catena: la scelta di password troppo deboli, quando non addirittura ingenue, equivale alla chiave della porta nascosta sotto il classico zerbino.

La prevenzione, dunque, costituisce la prima essenziale barriera difensiva ma, di fronte a organizzazioni criminali che hanno fatto della frode informatica, della sottrazione di dati sensibili e del furto d'identità il cardine della propria attività fuorilegge, le difese basilari possono non bastare.

Ecco emergere la figura del consulente informatico, gergalmente definito "ethical hacker" in grado di condurre una profonda analisi del sistema, il "penetration test" appunto, ponendosi dal punto di vista di un potenziale attaccante malintenzionato e tentando di individuare e sfruttare le vulnerabilità rilevate al fine di aggredire il sistema e ottenere il maggior numero di informazioni possibili.

Il "Penetration Test"

Ovviamente, i processi di analisi che sono condotti in un "penetration test", vengono svolti a seguito di un incarico tecnico/professionale ben preciso, preventivamente concordato con il committente e si compongono di più fasi, alcune automatiche, altre manuali, allo scopo di fornire una stima accurata sulle capacità di difesa e le eventuali debolezze del sistema esaminato e del livello di penetrazione raggiunto nei confronti delle vulnerabilità interne, esterne e della sicurezza fisica.

Inizialmente vengono acquisite le informazioni principali sull'architettura della piattaforma e sui servizi offerti. Subito dopo è effettuata la scelta su come condurre il passo successivo, consistente in un dettagliato esame dei principali errori e problemi.

Le metodologie adottate, nell'ottica del raggiungimento del miglior livello di sicurezza nel sistema informatico preso in esame, consentono di verificare che non sia possibile ottenere accessi a informazioni per le quali non si ha l'autorizzazione necessaria. Consentono, altresì, di

valutare se, per un utente con privilegi minimi, sia possibile accedere a informazioni che superano le mansioni ricoperte.

Sarà quindi l'esperienza dell'analista a evidenziare tutte le possibili vulnerabilità, incluse quelle più recenti e sofisticate e alcune non ancora di pubblico dominio.

Infine, il "penetration test" tende a verificare se un determinato software permette di ottenere accessi a un malintenzionato che sappia sfruttarne le debolezze.

Al termine dell'esame, gli eventuali problemi di sicurezza evidenziati, sono presentati al committente, unitamente alla valutazione del loro impatto nello scenario del business aziendale, tramite un dettagliato rapporto scritto, fornendo inoltre le soluzioni tecniche o le proposte di migrazione e/o mitigazione del sistema.

Gli attacchi informatici in ambito domestico

La diffusione capillare di telefoni cellulari sempre più "smart" e con funzioni internet, i tablet, i computer, oramai presenti anche in ambiente domestico, ha fornito a chiunque i mezzi per eseguire transazioni bancarie, il cosiddetto "home banking" senza spostarsi dal divano di casa e senza disturbare il gatto che dorme sul cuscino.

Effettuare acquisti a distanza, tramite internet, con la carta di credito, con la PostePay o con il sistema Pay-Pal, è oramai un gesto comunissimo e, nell'immediato futuro, destinato a incrementarsi ulteriormente.

Tutto ciò ha spinto il mondo sotterraneo del "cybercrime" alla creazione di "malware" in grado di iniettare virus informatici o "trojan horse" in maniera del tutto invisibile all'utente, allo scopo di carpire le password di accesso ai servizi finanziari.

In alternativa, sofisticate tecniche di "ingegneria sociale" cercano di spingere gli utenti della rete a rivelare spontaneamente le proprie password clonando ad arte la home-page degli istituti bancari, dei servizi postali ecc. sostituendosi fraudolentemente a queste.

Nulla di più facile, per questi criminali del web, acquistare oggetti di valore, (in genere, telefoni cellulari di ultima generazione, computer portatili, televisori ecc.) usando i dati delle carte di credito di ignari cittadini, illecitamente sottratti dai loro computer dopo averli infettati con programmi-spia.

Ovviamente, l'indirizzo fisico cui spedire i beni in questione, sarà predisposto in maniera opportuna. In genere, il cybercriminale attenderà il corriere sul portone d'ingresso e lo intercetterà, qualificandosi come il legittimo destinatario e munendosi, se necessario, anche di un documento contraffatto. I sistemi di tracciamento delle spedizioni, offerti da tutti i corrieri, faciliteranno il "lavoro" del truffatore indicandogli persino il giorno e l'ora approssimata della consegna.

Tutto questo deve farci considerare che anche un computer, usato in ambito domestico, è soggetto a tentativi di accesso illeciti e alla possibilità, tutt'altro che remota, del furto di dati sensibili.

Anche se le transazioni finanziarie non sono certo dello stesso ordine di grandezza di quelle usuali in ambiti professionali/industriali, tuttavia sono sufficienti a suscitare gli appetiti di pirati informatici di "piccolo cabotaggio" che navigano sottocosta, senza avventurarsi nel "mare magnum" del cybercrime internazionale.

Anche in quest'ambito, quindi, la parola d'ordine è: prevenire! O meglio, affidarsi all'esperienza e alla professionalità di un consulente informatico qualificato.

In alternativa si può seguire il consiglio di Kevin Mitnick, uno fra i più famosi hacker: *"Un computer sicuro è un computer spento"*. Anche se ciò equivale a una torta al cioccolato… senza il cioccolato.

© Copyright 2013 Claudio Ballicu, Tutti i diritti riservati

Torna alla Home Page: http://www.perizieforensi.com/