CONOSCERE LE MINACCE PER LE PMI

Cyberwar, hacktivism e attacchi DDoS fanno sempre notizia. Tuttavia, si tratta di fenomeni limitati esclusivamente a multinazionali ed enti governativi?

Esa Tornikoski di F-Secure illustra il panorama delle minacce per le pmi.

Il mondo della protezione dei dati è complesso e in rapido cambiamento. Gran parte delle aziende è troppo impegnata e diversificata per occuparsi della manutenzione di competenze in materia di protezione. Tuttavia, a causa della continua presenza di Stuxnet e Flame nei notiziari quotidiani, abbiamo ricevuto molte domande da diversi tipi di organizzazioni su come le loro attività ed i loro dati sono a rischio.

Non esiste un solo "tipo" di minaccia, ma un intero panorama

Uno degli aspetti più astratti per le aziende consiste nell'individuare i casi che costituiscono solo notizie interessanti e quelli che costituiscono un reale pericolo per le PMI. In che modo è possibile individuare con maggiore probabilità gli attacchi che potrebbero colpire la vostra?

GLI ASPETTI PIÙ RISCHIOSI PER LE PMI NON RIGUARDANO OGNI SINGOLO "TIPO" DI MINACCIA, MA L'INCUBO COSTANTE E MUTEVOLE DEL CYBERCRIME.

Un aspetto impossibile da analizzare a livello di singoli elementi come "virus" o "spam" e spesso descritto sommariamente dai mezzi di comunicazione. Il business del cybercrime è

F-Secure

variegato e complesso come molti altri tipi di attività: ciascuna "minaccia" viene creata da un soggetto diverso per poi essere acquistata, venduta e mescolata con molti altri elementi, producendo un sistema complesso, variegato e con un unico obiettivo: rubare denaro e dati.

Computer zombie, inganni e vulnerabilità invisibili

Alla radice dell'attività dei cyber-criminali esiste uno schema molto preciso. Grazie tecnologie di sicurezza sempre più efficaci, come ad esempio antivirus, filtri per lo spam e protezione della navigazione, i cyber-criminali cercano metodi sempre diversi e innovativi per accedere ai dati. Le PMI sono molto soggetti a determinati tipi di attacchi: botnet (computer zombie), ingegneria sociale (l'arte di raggirare le persone) e gli exploit delle vulnerabilità (attacchi condotti attraverso sconosciute vulnerabilità di sicurezza).

Botnet: risorse aziendali a servizio di altre "aziende"

Le **botnet** sono fra i problemi più diffusi che affliggono le PMI. Un "bot" è un computer infetto che è possibile controllare in remoto, mentre una botnet è una rete di macchine infette di questo tipo, che ricorda un esercito di zombie controllati da una sola persona che eseguono quello che a loro viene detto di fare. In questi casi, le risorse di un'azienda possono essere acquisite e controllate in modo da essere utilizzate per attività illegali come l'invio di spam, il furto di dati o persino l'attacco verso altri siti web. Per individuare questa situazion, può essere necessario molto tempo.

Spesso, la persona che crea la botnet non è la stessa che ne trae profitto. È molto redditizio vendere il bot al miglior offerente, oppure arrivare a noleggiarlo con tariffa oraria o settimanale.

Le PMI sono un ambiente ideale per l'utilizzo delle botnet, poiché utilizzano un gran numero di dispositivi collegati in rete che non sono spenti neppure di notte.

“UNA RETE AZIENDALE COMPROMESSA CREA UN INSIEME DI RISORSE VIRTUALMENTE INFINITE PER I CYBER-CRIMINALI”, SPIEGA SEAN SULLIVAN, SECURITY ADVISOR DI F-SECURE LABS.

“Si tratta di una situazione in cui le risorse di un’azienda vengono utilizzate per le attività reali dei cyber-criminali”.

Ingegneria sociale: i cyber-criminali conoscono bene la nostra natura umana.

I perfezionamenti delle tecniche di protezione hanno spinto i cyber-criminali a cercare altri metodi per accedere a un sistema, quale modo migliore se non attraverso gli utenti del sistema?. Per "**ingegneria sociale**" si indica la manipolazione delle persone al fine di eseguire determinate azioni o a fornire informazioni, come ad esempio installare un file o comunicare

le informazioni della propria password o della carta di credito. Anche se alcuni attacchi sono piuttosto infantili (ricorderete il principe nigeriano che continua a chiedere il vostro numero di conto bancario), i malintenzionati stanno diventando creativi ed eleganti, risultando a volte quasi indistinguibile dalle persone attendibili.

Il ransomware è un attacco che sta diventando molto comune. Un criminale riesce a bloccare il computer di un utente, chiedendo denaro per renderlo di nuovo utilizzabile. Avviene di solito attraverso un messaggio apparentemente proveniente dalle forze di pubblica sicurezza, secondo il quale all'utente è stata prescritta una multa, dovuta al possesso di contenuti illegali e compromettenti. "L'utente dovrebbe contattare l'helpdesk", spiega Sullivan, "ma spesso ciò non avviene poiché il malware crea una situazione imbarazzante".

Exploit di vulnerabilità: anche le origini più affidabili possono procurare danni

Il metodo dai cyber-criminali per accedere a un computer consiste nello sfruttare gli **exploit di vulnerabilità**. Si tratta dell'arte di individuare le vulnerabilità di protezione nel software e di utilizzarle per infettarlo.

Il principale responsabile di questo tipo di situazioni è il software non aggiornato e privo delle necessarie patch.

"IL VOSTRO SOFTWARE È COME LA PORTA DI INGRESSO PER IL VOSTRO PC", DICHIARA SULLIVAN

"Il software obsoleto è una porta spalancata per tutti i tipi di attacchi, soprattutto provenienti da luoghi apparentemente innocui". Un esempio di questo problema sono i banner pubblicitari presenti su siti attendibili come i giornali online, studiati per sfruttare plug-in come Java e Flash al fine di individuare un sistema per infettare il computer dell'utente e installare malware capace di rubare dati, trasformarlo in un bot o semplicemente bloccarlo così da poter chiedere un riscatto.

In futuro, gli exploit avranno un'evoluzione ancora più rapida

Secondo Sean Sullivan, gli exploit diventeranno sempre più rapidi e frequenti, arrivando a essere del tipo "zero-day", ovvero un fenomeno per motivi cronologici impossibile da contrastare con patch o correzioni.

"Le vulnerabilità verranno scoperte con una velocità tale da impedire ai produttori di software di restare al passo", spiega. "Inoltre, il fenomeno del 'zero-day' è soltanto all'inizio". Lo scorso agosto, un exploit Java zero-day ha scatenato un'onda d'urto nell'intero settore. La banda responsabile dell'attacco è riuscita a individuare una grossa falla di sicurezza di Internet Explorer, che viene attivata visitando un sito web compromesso anche con le versioni più recenti del programma (IE7, 8 e 9). Così facendo il controllo del computer veniva completamente ceduto ai criminali.

Si tratta di un esempio di minaccia che non viene messa in risalto dai mezzi d'informazione, ma solo da alcuni blog tecnologici, restando così nell'ambito dell'utenza più avanzata. In

casi come questi, la prima linea di difesa consiste nell'interrompere l'utilizzo del prodotto coinvolto fino al rilascio di un'adeguata correzione.

La guerra informatica porterà a danni collaterali?

Come illustrato in precedenza, attacchi come Flame ricevono una notevole attenzione da parte dei mezzi di comunicazione. In poche parole, Flame sembra essere un elemento di una guerra cibernetica fra governi nazionali che, sebbene non ancora in grado di colpire gli utenti normali, potrebbe favorire lo sviluppo di tecniche in grado di rappresentare una minaccia a breve termine. Flame è stato sviluppato usando metodi avanzati per l'individuazione dei computer da infettare, ingannando il sistema operativo in modo da presentarsi come aggiornamento creato dalla stessa Microsoft.

Al momento, gran parte dei cyber-criminali non ha bisogno di una tale tecnica raffinata. Tuttavia, quando sarà possibile ottenere un migliore ritorno sull'investimento o superare la concorrenza, i criminali informatici potrebbero iniziare ad adoperare questo tipo di competenze.

Secondo Sean, "la ricerca e lo sviluppo di oggi si trasformeranno in un'applicazione domani". La parte più complessa è stata già completata: i metodi utilizzati per Flame potranno essere utilizzati dalle organizzazioni criminali. Pertanto, dobbiamo essere pronti.

Siate vigili. Niente panico.

Quali sono i principali elementi da tener d'occhio in un panorama sottoposto a cambiamenti così rapidi?

Innanzitutto, verificare che la propria impresa disponga di un'efficace e funzionante protezione antivirus, antispam e della navigazione all'interno dell'ambiente operativo, a partire dal computer portatili fino ai desktop, ai server fino ai device mobili.

L'aspetto più importante per le PMI consiste nell'utilizzo delle versioni più aggiornate del software in uso (sistemi operativi, plug-in come Flash e Java, Microsoft Office e browser per Internet) e non solo del software di protezione.

Infine, contattare un esperto in grado di gestire i problemi di protezione e aggiornato sui pericoli in agguato.

In poche parole, utilizzando software continuamente aggiornato all'ultima versione e prodotti di protezione in grado di occuparsi di tutti i livelli di un'organizzazione, sarà possibile dedicare tempo e risorse alle principali priorità aziendali.

Informazioni sull'autore

Esa Tornikoski, Product Manager di F-Secure, è specializzato nella costruzione di offerte adatte alle esigenze di protezione IT per le PMI.

Informazioni su F-Secure

F-Secure è un'azienda globale con sede centrale a Helsinki, in Finlandia. Fondata nel 1988, F-Secure è un pioniere del settore della protezione, è attiva in oltre 100 Paesi, dispone di 18 filiali e vanta oltre metà dei dipendenti al di fuori del territorio nazionale finlandese. Siamo un attendibile fornitore di servizi per oltre 200 operatori e un'azienda di protezione scelta da realtà produttive di tutto il mondo attraverso un'ampia rete di rivenditori partner