Le 10 principali minacce alla sicurezza dei dati delle PMI

Il seguente articolo è tratto da "Top 10 Threats to SME Data Security (and what to do about them)", un white paper scritto da Scott Pinzon, CISSP, del team WatchGuard® LiveSecurity®. Il riepilogo qui riproposto elenca queste dieci minacce e la relativa contromisura per ognuna di esse. Per ulteriori informazioni sulla modalità di selezione delle minacce, sul tipo di rete qui illustrato e per almeno due ulteriori contromisure per ciascuna minaccia, scaricare una copia gratuita del white paper completo all'indirizzo www.watchguard.com/whitepapers.

È difficile reperire rapporti basati su situazioni reali e accurati che illustrino che cosa oggi è davvero una minaccia alla sicurezza di rete per una comune azienda.

Dal 1999, il WatchGuard LiveSecurity Team ha monitorato ogni giorno le minacce emergenti alla sicurezza di rete, con una speciale attenzione ai problemi che riguardano le piccole e medie imprese (PMI). Quando rileviamo un problema che può impattare negativamente sulle PMI, avvisiamo i nostri abbonati tramite broadcast via email. Dal momento che i nostri abbonati sono professionisti IT sovraccarichi di lavoro per i quali il tempo è prezioso, inviamo gli avvisi solo quando sappiamo che un attacco non è semplicemente possibile bensì probabile. Questa enfasi sul contesto aziendale e sulla praticità rende il nostro servizio pressoché unico nel settore. Questo approccio viene costantemente perfezionato dalle segnalazioni delle nostre decine di migliaia di abbonati, da visite presso le sedi dei nostri clienti e da focus group e sessioni informali.

Il risultato: questo documento che elenca i 10 più comuni vettori di compromissione dei dati sulla base alla nostra esperienza di analisti della sicurezza per le PMI. Sono inoltre suggerite tecniche e difese pratiche per contrastare ogni singolo vettore.

Minaccia n. 10: attacchi interni

L'Intrusion Response Team di Verizon ha investigato 500 intrusioni nell'arco di 4 anni ed è stato in grado di attribuire il 18% delle violazioni di protezione a utenti interni. Di questo 18% di intrusioni, circa la metà veniva originato dallo staff IT stesso.[1]

> **Implementare il principio del doppio controllo.** Implementare il principio del doppio controllo significa che per ogni risorsa principale è sempre disponibile una procedura di fallback. Ad esempio, si può scegliere di avere un tecnico responsabile principalmente della configurazione dei server Web e SMTP. Ma come misura minima di precauzione, è opportuno che le credenziali di accesso a questi server siano note o disponibili per almeno un'altra persona.

Minaccia n. 9: mancanza di piani di contingenza

Le aziende che sono orgogliose di essere "agili" e "reattive" spesso raggiungono questi risultati tralasciando standardizzazione, processi maturi e pianificazione delle contingenze. Numerose PMI hanno riscontrato che una semplice compromissione o una perdita di dati può rivelarsi disastrosa quando non è previsto alcun piano di continuità dell'attività, un piano di disaster recovery o policy di risposta alle intrusioni oppure un sistema di backup aggiornato *da cui effettivamente ripristinare i dati*, oppure un sistema di storage off-site.

Come mitigare i rischi della mancanza di un piano

> Se è disponibile il budget, è certamente opportuno affidarsi a un esperto per sviluppare una robusta metodologia di protezione delle informazioni. Se il budget non consente di rivolgersi a un esperto, approfittare dell'ottimo lavoro svolto da altre organizzazioni e modificarlo per adattarlo alla propria organizzazione. Il SANS Security Policy Project mette a disposizione modelli gratuiti e altre risorse che consentono di stilare policy personalizzate. Per ulteriori informazioni, visitare http://www.sans.org/resources/policies/.

[1] Riepilogo disponibile in http://www.infosectoday.com/Articles/2008_Data_Breach_Investigations_Report.htm. Per scaricare un file .pdf del rapporto, visitare http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

Minaccia n. 8: una configurazione inadeguata significa compromissione

PMI con un budget insufficiente o prive di esperienza specifica spesso installano router, switch o altri dispositivi di rete senza coinvolgere nessuna persona consapevole delle implicazioni in termini di sicurezza di ciascun dispositivo. In questo scenario, un responsabile di rete dilettante si accontenta semplicemente di convogliare il traffico di dati in entrate e in uscita. Non pensa ad esempio che è opportuno cambiare il nome utente e la password di accesso impostati come predefiniti dal produttore dei dispositivi.

Come mitigare i rischi di scelte di configurazione inadeguate

Eseguire una scansione automatica delle vulnerabilità. Se non vi potete permettere di assumere un consulente, probabilmente potrete permettervi una scansione automatica una tantum della vostra rete. Sul mercato sono presenti numerosissimi pacchetti di "gestione delle vulnerabilità", per ogni fascia di prezzo. L'utilizzo regolare di tali prodotti deve essere parte integrante delle normali attività di manutenzione della rete.

Minaccia n. 7: uso disinvolto dell'accesso di rete di hotel e chioschi

Le reti degli hotel sono notoriamente ricettacolo di virus, worm, spyware e malware e sono spesso gestite con criteri di sicurezza complessivamente scadenti. Per i malintenzionati i chioschi pubblici rappresentano un luogo comodo per posizionare un keylogger e attendere che un malcapitato finisca nella trappola. I laptop privi di software firewall, antivirus e antispyware aggiornati possono quindi venire compromessi. Le tradizionali difese possono venire neutralizzate quando l'utente aggira il firewall del gateway e si connette dall'interno dell'area trusted.

Come mitigare i rischi dell'utilizzo disinvolto di reti di hotel

Configurare e applicare una policy che impedisca ai dipendenti di disattivare le difese. Secondo uno studio commissionato da Fiberlink, 1 su 4 "utenti di strada" ha ammesso di alterare o disattivare le impostazioni di sicurezza dei propri laptop. La policy deve impedire che i dipendenti siano in grado di disattivare le difese se non espressamente consentito dall'azienda. Molte delle soluzioni antivirus più diffuse sono configurabili in maniera tale da non potere venire disattivate, anche da parte di utenti con privilegi locali di amministratore. È quindi opportuno verificare se la soluzione utilizzata fornisce questo tipo di funzionalità.

Minaccia n. 6: uso disinvolto di hot spot Wi-Fi

Gli hot spot wireless pubblici pongono gli stessi rischi delle reti degli hotel e forse anche qualcuno in più. Gli attaccanti in genere impostano un punto di accesso wireless non protetto che pubblicizzato come "Wi_fi pubblico gratuito" per poi attendere che un "utente di strada" affamato di connettività si colleghi. Con un packet sniffer attivato, l'attaccante può vedere tutto quello che il dipendente digita, inclusi i login di accesso. Questo attacco risulta particolarmente nocivo perché l'attaccante acquisisce i dati *senza lasciare alcuna traccia* di compromissione del computer della vittima.

Come mitigare i rischi dell'uso disinvolto del Wi-Fi

Insegnare agli utenti come scegliere sempre connessioni criptate. Istruire gli utenti a collegarsi attraverso una rete VPN (Virtual Private Network). La rete VPN crittografa i flussi di dati in maniera tale che se anche un intruso si inserisce in wireless riceverà dati non utilizzabili.

Minaccia n. 5: perdita di dati su dispositivo portatile

Una notevole quantità di dati sensibili viene compromessa ogni anno quando i dipendenti dimenticano lo smart phone in un taxi, la scheda USB in una camera d'albergo o il laptop su un treno pendolare. Quando i dati sono memorizzati su dispositivi di piccole dimensioni, per gli amministratori è più saggio non pensare a che cosa fare "*se* si perde il dispositivo" bensì pensare che cosa fare "*quando* il dispositivo viene perduto".

Come mitigare il rischio di dati perduti su dispositivi portatili

Gestione centrale dei dispositivi mobili. Considerare l'investimento in server e software in grado di gestire centralmente i dispositivi mobili. Blackberry Enterprise Server di RIM può aiutare ad assicurarsi che le trasmissioni siano crittografate e se un dipendente segnala di avere perso un telefono, è possibile cancellare i dati dal dispositivo Blackberry perduto. Queste precauzioni consentono di ridurre al minimo le conseguenze negative determinate dalla perdita di questo tipo di dispositivi.

Minaccia n. 4: compromissione del server Web

I siti Web sono attualmente il bersaglio più comune di attacchi di botnet e la vulnerabilità che si rivela fatale per la maggior parte dei siti Web è un codice applicativo scritto in maniera inadeguata. Gli attaccanti hanno compromesso centinaia di migliaia di server in un colpo solo grazie ad attacchi che sfruttano iniezioni SQL automatizzate. I siti legittimi sono indotti quindi a trasmettere malware, allargando inconsapevolmente l'area di influenza dell'attaccante.

Come mitigare i rischi di compromissione del server Web

Controllare il codice applicativo Web. Se (ad esempio) un modulo Web include un campo in cui un visitatore deve specificare un numero di telefono, l'applicazione Web deve eliminare i caratteri in eccesso. Se l'applicazione Web non sa che cosa fare dei dati o di un comando, deve rifiutarli e non elaborarli. Ricercare la migliore soluzione

di revisione del software alla propria portata del proprio budget (un team di esperti oppure un tool automatizzato), in grado di rilevare se il proprio codice convalida correttamente l'input dei dati.

Minaccia n. 3: navigazione sul Web degli utenti

Uno studio del 2006 condotto dalla University of Washington ha rilevato che i siti che diffondono la maggiore quantità di spyware sono, nell'ordine:

1. Siti dedicati a personaggi dello spettacolo (ad esempio, i siti che pubblicano aggiornamenti sulle ultime avventure di Paris Hilton e Britney Spears);
2. Siti di giochi online (dove ad esempio si può giocare a scacchi con uno sconosciuto)
3. Siti porno (sorprendentemente classificatisi solo al terzo posto)

I siti di social networking quali MySpace e Facebook sono ora in testa alla classifica in quanto centri di raccolta e diffusione di spamming, trojan horse e spyware. I dipendenti che navigano su siti non correlati al proprio lavoro finiscono con l'invitare all'interno dell'azienda client bot di rete, trojan horse, spyware, keylogger, spambot, ovvero l'intera gamma del malware.

Come mitigare i rischi della navigazione sul Web

Implementare il filtraggio dei contenuti Web. Utilizzare software di filtraggio Web quali WebBlocker di WatchGuard. Le soluzioni di filtraggio del Web gestiscono database (aggiornati giornalmente) di URL bloccati in decine di categorie. Ulteriori categorie consentono di specificare una quantità maggiore di sfumature. Questi strumenti consentono di applicare le policy di utilizzo consentito degli strumenti tecnologici.

Minaccia n. 2: email in formato HTML

L'attacco via email più comune viene oggi veicolato da messaggi email in formato HTML che includono un link a un sito nocivo irto di trappole. Un clic sbagliato può avviare un download drive-by. I rischi sono gli stessi indicati per la Minaccia n. 3, "Navigazione sul Web" ma l'attaccante utilizza l'email per indurre la vittima a visitare il sito Web nocivo.

Come mitigare i rischi delle email in formato HTML

Implementare un proxy Web in uscita. È possibile impostare la propria LAN in maniera che tutte le richieste e le risposte HTTP reindirizzino a un server proxy Web, che fornisce un punto singolo in cui è possibile monitorare la legittimità di tutto il traffico Web. Il proxy Web non intercetterà un messaggio email in entrata nocivo, ma se un utente della vostra rete fa clic su un link contenuto nel messaggio email in formato HTML, viene generata una richiesta email che verrà intercettata dal proxy Web. Se la richiesta HTTP dell'utente non raggiunge il sito dell'attaccante, l'utente non ne diventerà vittima.

Minaccia n. 1: attacco automatico di una vulnerabilità nota

Il *2008 Data Breach Investigations Report* di Verizon include dati effettivi relativi a oltre 500 violazioni di protezione, verificatesi nel corso di 4 anni. Il RISK Team di Verizon ha rilevato che il 73% delle violazioni proveniva da fonti esterne.
Le PMI che trascurano la sicurezza diventeranno le vittime predestinate se non procedono all'installazione delle patch Windows nello stesso mese di pubblicazione delle patch. Ma la rete contiene molto di più dei prodotti Microsoft. La procedura di installazione delle patch deve essere estesa a tutte le applicazioni e ai componenti del sistema operativo presenti nella rete.

Come mitigare il rischio di attacchi automatici

Investire nella gestione delle patch. Il software di gestione delle patch consente di eseguire la scansione della rete, identificare le patch mancanti e gli aggiornamenti del software e distribuire le patch da una console centrale, aumentando in maniera significativa la probabilità di disporre di una rete aggiornata in ogni sua parte.

Realizzare una rete di prova non costosa. Anche le aziende che godono di buona reputazione possono commettere un passo falso. Pertanto, raccomandiamo di installare una patch su un sistema di prova e per verificarne il funzionamento prima di distribuire la patch in tutta la rete. Se non è al momento disponibile un ambiente di rete di prova, è possibile utilizzare computer desktop e server obsoleti per realizzare un ambiente di prova.

Conclusione

Le contromisure suggerite consentono di fare molto per mitigare i rischi e di proteggere la propria rete. Ma questi sono solo alcuni dei passi che un amministratore IT può prendere al fine di aumentare la sicurezza della propria rete. Per suggerimenti pratici su come rafforzare la propria rete nei confronti degli attacchi più comuni, scaricare una copia gratuita del white paper completo **Top Ten Security Threats for SMEs (and what to do about them)** disponibile nel sito Web di WatchGuard.

WatchGuard® fornisce appliance di protezione gateway XTM (Extensible Threat Management) che consentono di contrastare nove delle dieci minacce elencate nel presente documento. Le nostre appliance non possono purtroppo impedire che i vostri dipendenti perdano i propri dispositivi portatili. Possiamo però aiutarvi a proteggere la vostra rete wireless, controllare l'integrità dei client che richiedono l'accesso alla rete, filtrare lo spam, applicare proxy per i servizi Web, ridurre al minimo le minacce interne, creare VPN e molto altro ancora.

Per informazioni sulle soluzioni di protezione WatchGuard e sulla protezione che forniscono nei confronti di botnet e le altre minacce di rete, visitare il sito www.watchguard.com o contattare un nostro rivenditore.