



WatchGuard annuncia le 10 minacce principali per la sicurezza delle reti delle piccole e medie aziende

SEATTLE, 25 Settembre 2008

Novità interessanti:

- A differenza delle grandi imprese, le PMI (Piccole e Medie Imprese) si trovano ad affrontare numerose minacce per la sicurezza delle informazioni aziendali contando solo sul supporto di risorse spesso limitate per la protezione di beni, dati ed informazioni sui clienti.
- Una ricerca di WatchGuard Technologies ha identificato le 10 minacce principali per la sicurezza delle PMI:

10) *Personale interno* – In molte PMI, le informazioni sui clienti e gli archivi aziendali vengono spesso affidati ad una sola persona. In assenza di misure appropriate, come report automatizzati e registri di sistema della rete, le perdite di dati dall'interno possono estendersi a lunghi periodi di tempo.

9) *Mancanza di piani di emergenza* – Una delle minacce principali per le PMI riguarda l'impatto sull'azienda delle conseguenze di una violazione, intrusione o infezione di virus. Molte PMI non hanno un piano di *disaster recovery* né dispongono di linee di condotta in caso di perdita di dati; ciò rende più lenti il ripristino e la ripresa dell'attività.

8) *Mancata modifica dei valori predefiniti dal produttore* – Gli hacker compilano e pubblicano delle liste complete dei parametri di login predefiniti (nome utente e password) per quasi tutti i dispositivi collegati in rete; di conseguenza, possono assumere con facilità il controllo delle risorse della rete se le impostazioni di configurazione predefinite non sono state modificate.

7) *Ambienti domestici privi di sicurezza* – In molte piccole aziende, i dipendenti spesso portano a casa il computer portatile per lavorare. In un ambiente di rete domestico privo di sicurezza, il computer portatile aziendale può restare pericolosamente esposto a virus, attacchi e malware.

6) *Uso imprudente delle reti pubbliche* – Un espediente comune usato dagli attaccanti consiste nel rendere disponibile un punto di accesso wireless etichettato "WiFi pubblico gratuito" ed attendere semplicemente il collegamento di qualche utente mobile alla disperata ricerca di una connessione. Dopo avere attivato uno sniffer di pacchetti, l'attaccante può osservare clandestinamente tutto ciò che viene digitato dal dipendente e sfruttare queste informazioni per ottenere un guadagno personale.

5) Perdita dei dispositivi portatili – Ogni anno, molti dati delle PMI vengono compromessi a causa della perdita dei computer portatili e lo smarrimento dei dispositivi mobili o chiavette USB. Anche se la codifica dei dati presenti nel dispositivo portatile e l'uso di password sicure possono ridurre i rischi correlati a molte di queste perdite, parecchi utenti delle PMI trascurano semplicemente la sicurezza dei propri dati e dispositivi mobili.

4) Web server compromessi – Molte PMI non introducono una protezione adeguata nell'hosting dei propri siti Web, lasciando le reti aziendali esposte ad attacchi di botnet e iniezioni di SQL.

3) Navigazione imprudente sul Web – Oggi più che mai, malware, spyware, keylogger e spambot si possono incontrare in siti Web dall'aspetto inoffensivo. I dipendenti che si avventurano in siti apparentemente sicuri potrebbero esporre inconsapevolmente le reti aziendali a minacce estremamente gravi.

2) E-mail HTML ostili – Ormai, gli attaccanti non inviano più e-mail con allegati ostili. Oggi, le minacce sono nascoste nei messaggi e-mail HTML che includono dei link a siti-trappola ostili. Un clic sbagliato può portare con facilità a un download inaspettato.

1) Vulnerabilità prive di patch, che restano aperte a violazioni note – Più del 90 per cento degli attacchi automatizzati cerca di sfruttare delle vulnerabilità note. Anche se le patch vengono rese disponibili con frequenza, una PMI con poco personale potrebbe non riuscire a installare nei propri sistemi le patch e gli ultimi aggiornamenti delle applicazioni, lasciandole vulnerabili nei confronti di attacchi che altrimenti si potrebbero bloccare con facilità.

Parole chiave:

PMI, perdita di dati, reti, configurazioni, reti degli hotel, rischi del Wi-Fi, dispositivi portatili, server Web, navigazione sul Web, HTML, e-mail, patch, vulnerabilità, rischi, sicurezza, gestione delle minacce, WatchGuard

Citazioni:

- *“Le minacce alla sicurezza delle PMI sono reali, esattamente come nel caso delle grandi organizzazioni”, ha dichiarato Eric Aarrestad, Vice Presidente Marketing di WatchGuard Technologies. “La tragedia è che molte PMI semplicemente non conoscono le appliance UTM (Unified Threat Management - gestione unificata delle minacce) che possono combattere queste minacce”.*
- *“La disponibilità di reti sicure lascia alle aziende la libertà di restare produttive e operare con efficienza”, ha dichiarato Carl Mazzanti, Direttore Generale di eMazzanti Technologies, un fornitore di servizi di sicurezza gestiti a livello regionale. “Le PMI che restano vigili e mantengono un alto profilo di sicurezza tendono a diventare il leader del proprio settore”.*

Maggiori informazioni su WatchGuard Technologies, Inc.

Dal 1996, WatchGuard® Technologies, Inc. è il leader nelle tecnologie avanzate per le soluzioni di sicurezza delle reti e offre un livello di sicurezza mission-critical a centinaia di migliaia di aziende in ogni parte del mondo. La famiglia di appliance UTM (Unified Threat Management) WatchGuard cablate e wireless e le soluzioni di accesso remoto WatchGuard SSL VPN offrono una sicurezza espandibile della rete, accompagnata da un livello senza precedenti di controllo, gestione e visibilità della rete. I prodotti WatchGuard sono supportati dal servizio WatchGuard LiveSecurity®: un innovativo programma di assistenza, manutenzione e formazione. WatchGuard ha sede centrale a Seattle, con filiali in Nord America, Europa, Asia-Pacifico e America Latina. Per ulteriori informazioni, visitare <http://www.watchguard.com/>.

Contatto Stampa

Francesca Bertolotti

Open2Europe

Tel. +33 1 55 02 14 71

E-Mail: f.bertolotti@open2europe.com