

Buoni consigli da GFI

Le dieci regole per un 2011 più sicuro

1 - Limitare l'accesso alla rete alle persone che ne necessitano

Nelle piccole e medie imprese capita spesso che vengano assegnati alla quasi totalità dei dipendenti privilegi completi di accesso alla rete e ai dispositivi, anche se in realtà non ce ne sono i requisiti lavorativi.

Tali decisioni comportano però una serie di rischi per la sicurezza aziendale. Se presumibilmente l'azienda ha assunto persone affidabili, come amministratori IT e specialisti responsabili di sicurezza per proteggere la rete aziendale, offrire privilegi completi rimane comunque un rischio... e non si può mai sapere.

2 - Una strategia per prevenire la perdita dei dati

Le minacce interne possono spesso essere quelle più pericolose e da cui probabilmente ci si protegge meno, semplicemente perché i dipendenti e il management nelle piccole e medie imprese tendono ad avere elevati livelli di fiducia reciproca.

L'attività di rete dovrebbe essere monitorata e dovrebbe essere tendenzialmente vietata la connessione di dispositivi portatili, come le chiavette USB. Semplicemente, è estremamente facile per un dipendente scontento sottrarre dati confidenziali senza essere notato.

Anche i lavoratori mobili rappresentano un problema per gli amministratori, e le aziende dovrebbero attuare una strategia definita sull'utilizzo di laptop e smartphone. Ora più che mai, gli amministratori e gli specialisti di sicurezza hanno bisogno di guardare oltre il perimetro di sicurezza. La protezione contro la perdita di dati è una questione che merita di essere considerata molto bene.

3 - Limitare la navigazione su Internet ed educare gli utenti a riconoscere le minacce

Gli utenti spesso non conoscono le minacce presenti su Internet. È meglio prevenire i problemi potenziali, quali *download pericolosi* o *social engineering*, che condurre a codici malevoli.

In assenza di un motivo di business per visitare i siti Web, può essere utile limitare la capacità di navigazione attraverso *white* o *black list*.

I siti *peer-to-peer* possono essere vettori di malware o dare ai membri P2P remoti possibilità di accesso ai dati aziendali se il client non è configurato correttamente. Anche i siti di *social networking*, come ad esempio Facebook, possono portare a link malevoli.

Questi possono provenire dall'account compromesso di un amico, senza che nessuno si accorga che quel determinato link rimanda a un sito malevolo.

Il malware scaricato sulla macchina dell'utente può poi diffondersi attraverso la rete.

I professionisti di sicurezza solitamente adottano per prima cosa soluzioni tecnologiche. Tuttavia, educare gli utenti a riconoscere i pericoli di spam, phishing, truffe *codec fasulle*, falsi prodotti di sicurezza e minacce sui *social network* possono prevenire molti problemi.

4 - Eseguire regolarmente audit di rete è fondamentale

Monitorare gli event log ed effettuare regolarmente controlli fornisce dati importanti sulla rete. Si tratta di un lavoro che può risultare noioso e dispendioso in termini di tempo, ma è sicuramente un passaggio da non tralasciare per le informazioni fondamentali che fornisce.

Audit regolari consentono di ottenere informazioni sui materiali disponibili in rete. L'analisi dei log consente di comprendere come vengono utilizzate le risorse e come migliorarne la gestione. Date le richieste di conformità che oggi incidono sulle aziende, mantenere gli audit di rete aggiornati è "un must" e rappresentano una risorsa critica se qualcosa dovesse andare storto. La gestione delle vulnerabilità e delle patch è inoltre essenziale per qualsiasi strategia di sicurezza della rete. Le macchine su cui mancano alcune patch o gli ultimi aggiornamenti di sicurezza rappresentano un bersaglio facile per i creatori di malware e gli hacker, è quindi importante che gli amministratori dispongano della tecnologia in grado di identificare, valutare e riparare qualsiasi buco riscontrato in rete.

In caso di eDiscovery, dimostrare di aver fatto tutto il possibile per proteggersi da qualsiasi problema di sicurezza può fare davvero la differenza, anche nel caso in cui l'azienda abbia realmente subito un attacco.

5 - Verificare la sicurezza dei sistemi prima di connetterli alla rete

Se un qualsiasi nuovo computer può essere preso dalla confezione e connesso direttamente a Internet, farlo rappresenta un errore madornale per la sicurezza.

Prima di connettere qualsiasi computer a un cavo Ethernet o alla linea telefonica, deve essere installato un software anti-malware. Una volta messe in atto queste misure di sicurezza e che la macchina è connessa a Internet, è fondamentale che queste funzionalità di sicurezza siano costantemente aggiornate per assicurare la protezione da malware e virus. I sistemi operativi, i browser e le altre applicazioni sono esposte a buchi di sicurezza.

Una volta scoperta la falla, viene solitamente sfruttata nell'arco di poco tempo. Un responsabile degli acquisti IT dovrebbe essere responsabile anche del monitoraggio dei siti web del produttore o dei feed dei social media per le notifiche sul rilascio degli aggiornamenti.

6 - Rafforzare le policy di sicurezza

Le policy di sicurezza sono praticamente inutili se non vengono supportate e promosse da parte del management. Allo stesso tempo, bisogna trovare un equilibrio per consentire ai dipendenti di portare avanti il loro lavoro.

Se le policy sono troppo restrittive, i dipendenti troveranno un modo per evitarle.

Bisognerebbe fornire inoltre una spiegazione ai dipendenti sul perché vengono attuate determinate policy.

Se i dipendenti sono consapevoli del perché non possono fare una determinata cosa, sono più propensi a rispettare tali policy. Un approccio dittatoriale porterà solitamente a un senso di risentimento da parte dei dipendenti.

7 - Autenticare sempre chi effettua chiamate

Autenticare le chiamate telefoniche potrebbe sembrare un processo ridondante per gli amministratori quando riconoscono direttamente la voce di chi chiama.

Tuttavia, dare nuove password e informazioni confidenziali al telefono senza seguire una procedura di autenticazione idonea potrebbe causare problemi di sicurezza che spesso non possono essere tracciati a ritroso fino al punto di origine - risultando poi molto più difficili da rilevare e da gestire.

Lo spear-phishing, che consiste in attacchi di social engineering mirati, è sempre più diffuso e gli utenti dovrebbero essere informati su come distinguere una richiesta legittima di informazioni da un tentativo di phishing, che avvenga via email o telefonicamente.

8 - Eseguire i backup ... ma anche verificarli

Non si è praticamente mai sentito che un back-up di sistema sia fallito, ma testare i backup e confermare che il piano di disaster recovery funziona realmente è tutta un'altra questione. Per prima cosa, i backup per essere efficaci devono essere creati su base regolare e tenuti off-site in un luogo sicuro.

Se questo già avviene, il passaggio successivo è quello di garantire realmente che i backup funzionino in caso di emergenza. Spesso, vi sono richieste di conformità per la crittografia dei backup. È bene controllare due volte che la crittografia sia realmente abilitata per i backup e che i dati possano essere recuperati.

9 - Cosa fare se il programma di disaster recovery non funziona

In teoria, il piano aziendale di disaster recovery è probabilmente un capolavoro. Può sembrare perfetto sulla carta, archiviato nella cartella "disaster recovery" sul PC aziendale. Ma come funziona in pratica?

Si è provato a simulare una situazione di disaster recovery in cui i backup devono essere utilizzati in modo da ripristinare i sistemi e renderli nuovamente attivi in modo da poter continuare il lavoro e ridurre al minimo la perdita di profitto? Pianificare una simulazione di questo tipo per garantire che l'azienda possa effettivamente andare a ritroso nei backup rappresenta un elemento fondamentale per la sicurezza.

Un piano di disaster recovery che fallisce, una volta messo in pratica, non è altro che un ulteriore disastro!

10 - Chiedere aiuto se serve!

Non bisogna temere di chiedere aiuto per i compiti più importanti. Eseguire da soli le impostazioni di rete è un compito estremamente impegnativo.

È consigliabile cercare aiuto all'esterno se non si possiedono ancora l'esperienza e gli skill sufficienti.

Se da un lato ricorrere a un aiuto esterno può risultare costoso, dall'altro, professionisti assicureranno che il lavoro sia eseguito correttamente.

Tom Kelchner, Communications e Research Analyst di GFI Software

CINQUE CONSIGLI DA WEBSense

Per aumentare la sicurezza dell'e-mail

La posta elettronica è oggi lo strumento più utilizzato dai cyber-criminali per diffondere virus, spam e altri tipi di malware.

Già a partire dal 2009 i Security Labs di Websense hanno registrato un forte incremento delle e-mail utilizzate per diffondere file e Trojan malevoli come allegati.

Quest'anno, gli attacchi via e-mail sono diventati più sofisticati e complessi: gli hacker sfruttano sempre più spesso topic considerati opportuni per convincere gli utenti ad aprire le e-mail o cliccare link malevoli. Questi messaggi riescono però a superare indenni la maggior parte dei sistemi di difesa, esponendo gli utenti a un grande rischio.

Per aumentare la sicurezza della posta elettronica, Websense consiglia di seguire cinque semplici regole.

Chiudere la finestra di esposizione

Il panorama delle minacce cambia molto velocemente e ogni minuto nascono nuovi pericoli. È importante cercare una soluzione di sicurezza che classifichi in tempo reale le minacce per bloccarle subito.

No alla trappola social engineering

Le trappole di social engineering utilizzano e-mail phishing personalizzate e, mentre in precedenza gli spammer sfruttavano i nomi delle grandi aziende per convincere gli utenti a cliccare gli URL, negli ultimi mesi sono stati sfruttati come esche soprattutto Facebook, Twitter, iTunes, Amazon, Adobe e siti con offerte di lavoro.

Attenzione agli allegati

Nel 2010 le e-mail, spesso contenenti topic popolari, sono ritornate ad essere lo strumento principale per diffondere come alle-

gati file malevoli e Trojan. Inoltre, i ricercatori hanno rilevato un incremento di attacchi misti, allegati e URL malevoli per il furto dei dati.

Unificare la sicurezza per fermare le minacce convergenti

Oggi i cyber-criminali sfruttano la combinazione di e-mail, Web e furto dati: per questo, è fondamentale avere una soluzione di sicurezza unificata, che protegga le tre aree, offrendo i più alti livelli di protezione della posta elettronica contro i rischi legati sia alle minacce interne che esterne.

Mantenere aggiornate le soluzioni per la sicurezza

A causa della natura dinamica delle minacce, gli aggiornamenti in tempo reale sono fondamentali.

La modalità più semplice per gestirli è sce-

gliere una soluzione Security-as-a-Service (SaaS) per garantire la sicurezza dei servizi Web ed e-mail senza i costi e la complessità dell'implementazione on-premise.

Grazie all'implementazione SaaS i processi di analisi e gestione sono trasferiti dall'azienda ai datacenter disponibili nelle diverse sedi in modalità cloud.

Websense, offre protezione contro le moderne minacce al minor costo a migliaia di multinazionali e piccole-medie imprese nel mondo. Distribuite attraverso una rete globale di partner di canale, le soluzioni software, appliance e software-as-a-service (SaaS) aiutano le aziende a utilizzare nuove forme di comunicazione, collaborazione e strumenti Web 2.0 che permettono di bloccare eventuali minacce ed evitare la perdita di dati essenziali, rinforzando le policy di sicurezza.