Principi fondamentali sulla sicurezza di rete per le PMI

Che cos'è la sicurezza di rete?

La sicurezza di rete comprende ogni attività pensata per proteggere l'usabilità e l'integrità della rete e dei dati. Include sia tecnologie hardware che software. Una sicurezza di rete efficace gestisce l'accesso alla rete. Mira a varie minacce e impedisce che penetrino o si diffondano nella rete.

Come funziona la sicurezza di rete?

La sicurezza di rete combina più livelli di difesa alla periferia e all'interno della rete stessa. Ogni livello di sicurezza della rete implementa policy e controlli. Gli utenti autorizzati ottengono l'accesso alle risorse di rete, ma viene impedito agli hacker di eseguire exploit e minacce.

Come traggo vantaggio dalla sicurezza di rete?

La digitalizzazione ha trasformato il nostro mondo. Il modo in cui viviamo, lavoriamo, giochiamo e impariamo è cambiato completamente. Tutte le aziende che vogliono offrire i servizi richiesti da clienti e dipendenti devono proteggere la propria rete. La sicurezza di rete consente anche di proteggere le informazioni proprietarie dagli attacchi. Di fatto è questa che protegge la reputazione dell'azienda.

6 azioni che puoi adottare per proteggere la rete

1. Monitora il traffico in entrata e in uscita dal firewall e leggi attentamente i report. Non affidarti agli avvisi per contrassegnare le attività pericolose. Assicurati che qualcuno del team comprenda i dati e sia in grado di adottare le misure necessarie.
2. Tieni d'occhio le nuove minacce che vengono scoperte e rese pubbliche online. Ad esempio, il sito TrendWatch di Trend Micro monitora l'attività corrente delle minacce.
3. Abilita aggiornamenti regolari per il software antivirus e firewall.
4. Forma i dipendenti in modo continuativo così che possano comprendere tutte le modifiche alla policy dell'uso consentito. Inoltre, incoraggia un approccio alla sicurezza simile alle "ronde di quartiere". Se un dipendente nota qualcosa di sospetto, ad esempio non riesce ad accedere subito a un account e-mail, dovrebbe farlo immediatamente presente alla persona responsabile.
5. Installa una soluzione per la protezione dei dati. Questo tipo di dispositivo può proteggere la tua azienda dalla perdita di dati se viene violata la sicurezza della rete.
6. Valuta soluzioni di sicurezza aggiuntive che proteggano ulteriormente la rete e aumentino le capacità della tua azienda.

© 2018 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati.

Opzione - B

Principi fondamentali sulla sicurezza di rete per le PMI

Tipi di sicurezza di rete

Controllo degli accessi

Non tutti gli utenti devono avere accesso alla rete. Per tener fuori potenziali hacker, devi riconoscere ogni utente e ogni dispositivo. A quel punto puoi applicare le policy di sicurezza. Puoi bloccare i dispositivi endpoint non conformi o consentirne solo un accesso limitato. Questo processo si definisce controllo dell'accesso alla rete (NAC).

Software antimalware e antivirus

" Malware" , abbreviazione di " malicious software" (software dannoso), include virus, worm, Trojan, ransomware e spyware. A volte il malware infetta una rete ma poi rimane latente per giorni o addirittura settimane. I migliori programmi antimalware non solo cercano il malware in ingresso, ma continuano a monitorare i file anche in seguito per individuare le anomalie, rimuovere il malware e porre rimedio ai danni.

Sicurezza delle applicazioni

Qualsiasi software utilizzato per gestire l'azienda deve essere protetto, sia che venga creato dal personale IT o che venga acquistato. Purtroppo, qualsiasi applicazione può presentare lacune o vulnerabilità che gli hacker possono sfruttare per infiltrarsi nella rete. La sicurezza delle applicazioni comprende l'hardware, il software e i processi che usi per colmare tali lacune.

Analisi comportamentale

Per rilevare comportamenti anomali della rete bisogna conoscere il comportamento normale. Gli strumenti di analisi comportamentale distinguono automaticamente le attività che si scostano dalla norma. Il team di sicurezza può quindi identificare meglio gli indicatori di compromissione che costituiscono un potenziale problema e correggere rapidamente le minacce.

Data Loss Prevention

Le aziende devono essere certe che il proprio personale non invii informazioni sensibili all'esterno della rete. Le tecnologie di Data Loss Prevention, o DLP, possono impedire alle persone di caricare, inoltrare o perfino stampare informazioni critiche in modo non sicuro.

Sicurezza dei sistemi e-mail

I gateway e-mail sono il principale vettore di minaccia per una violazione della sicurezza. Gli hacker utilizzano informazioni personali e tattiche di social engineering per creare campagne di phishing sofisticate in modo da ingannare i destinatari e indirizzarli su siti che distribuiscono il malware. Un'applicazione di sicurezza dei sistemi e-mail blocca gli attacchi in arrivo e controlla i messaggi in uscita per prevenire la perdita di dati sensibili.

Firewall

I firewall creano una barriera tra la rete interna affidabile e le reti esterne non affidabili, come Internet. Utilizzano una serie di regole definite per consentire o bloccare il traffico. Un firewall può essere costituito da un componente hardware, software o entrambi. Cisco offre dispositivi Unified Threat Management (UTM) e Next-Generation Firewall incentrati sulle minacce.

Intrusion Prevention System

Un Intrusion Prevention System (IPS) analizza il traffico di rete per bloccare attivamente gli attacchi. A tale scopo, le appliance Next-Generation IPS (NGIPS) di Cisco correlano moltissima intelligence globale sulle minacce non solo per bloccare attività dannose, ma anche per monitorare lo sviluppo di malware e file sospetti in tutta la rete e prevenire così la diffusione degli attacchi e la reinfezione.

© 2018 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati.

Principi fondamentali sulla sicurezza di rete per le PMI

Sicurezza dei dispositivi mobili

I criminali informatici prendono sempre più di mira i dispositivi mobili e le app. Entro i prossimi 3 anni, il 90 per cento delle aziende IT potrebbe supportare le applicazioni aziendali sui dispositivi mobili personali. Naturalmente, devi avere il controllo dei dispositivi che possono accedere alla rete. Inoltre, dovrai anche configurare le connessioni per mantenere il traffico di rete privato.

Segmentazione della rete

La segmentazione software-defined suddivide il traffico di rete in diverse classificazioni e semplifica l'applicazione delle policy di sicurezza. Idealmente, le classificazioni sono basate sull'identità degli endpoint, non sui meri indirizzi IP. Puoi assegnare i diritti di accesso in base al ruolo, alla posizione e ad altro ancora, in modo che il livello di accesso adeguato venga attribuito alle persone giuste e i dispositivi sospetti siano contenuti e corretti.

VPN

Una Virtual Private Network cripta la connessione da un endpoint a una rete, spesso su Internet. In genere, una VPN ad accesso remoto utilizza IPsec o Secure Sockets Layer per autenticare la comunicazione tra il dispositivo e la rete.

Sicurezza Web

Una soluzione di sicurezza Web controllerà l'uso che il personale fa del Web, bloccherà le minacce basate sul Web e negherà l'accesso ai siti dannosi. Proteggerà il gateway Web in sede o nel cloud. " Sicurezza Web" si riferisce anche alle azioni che intraprendi per proteggere il sito Web della tua azienda.

Sicurezza wireless

Le reti wireless non sono sicure come quelle cablate. Senza misure di sicurezza rigorose, l'installazione di una LAN wireless può avere le stesse conseguenze di mettere porte Ethernet ovunque, incluso nel parcheggio. Per evitare che un exploit prenda piede, hai bisogno di prodotti elaborati appositamente per proteggere una rete wireless.

Sede centrale Americhe
Cisco Systems, Inc.
San Jose, California (USA)

Sede centrale Asia Pacifica
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono e di fax delle sedi italiane sono disponibili nel sito Web Cisco all'indirizzo **www.cisco.com/web/IT/local_offices/contatti_sedi/contatti_sedi_home.html**. Per ottenere maggiori informazioni da Cisco Italia, contattare il numero verde 800 787 854.

Cisco e il logo Cisco sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi. Per vedere l'elenco dei marchi Cisco, visita il sito Web all'indirizzo: www.cisco.com/go/trademarks. I marchi commerciali di terze parti citati sono proprietà dei rispettivi titolari. L'utilizzo del termine partner non implica una relazione di partnership tra Cisco e altre aziende. (1110R)

© 2018 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati.