

I cinque errori più comuni in materia di sicurezza

Siete Il pensiero che la vostra rete possa non essere protetta in maniera adeguata può causarvi notti insonni. Che cosa può esservi sfuggito nella frenesia della tipica giornata lavorativa? Dormite sonni tranquilli evitando questi comuni errori:

1. Essere troppo indulgenti nell'autorizzare l'accesso wireless alla rete

“Gli ospiti si aspettano che venga loro fornito l'accesso wireless, e questo può essere reso sicuro impostando una policy appropriata”, ha dichiarato Philip Stone, Presidente di Boardwalk Communications, Premier Partner di Cisco, in possesso della certificazione Advanced Wireless.



- Installate un access point wireless che supporti le VLAN, ad esempio gli access point Cisco Aironet, e impostate una VLAN ospite con accesso limitato.
- Assegnate agli ospiti password generate in modo random e impostatele in modo tale che scadano dopo uno specifico periodo di tempo. I Wireless LAN Controller Serie 2100 di Cisco

permettono anche alla receptionist all'ingresso di effettuare questa operazione.

- Non trasmettete le SSID aziendali, ma solo le SSID degli ospiti.
- Adattate la potenza. *“Siate certi di modificare le impostazioni in modo tale da non servire le aziende vicine”,* ha dichiarato Jerry Divino, Security Consultant presso Boice Enterprises, Certified Silver Partner di Cisco, in possesso delle certificazioni Advanced Security e Advanced Wireless.



2. Aspettarsi prestazioni superlative dalla solita coppia firewall – antivirus

Non è realistico pensare che un firewall di rete e un software antivirus siano sufficienti per garantire una protezione completa. *“In realtà, occorre un approccio di protezione in profondità, affinché una minaccia, qualora riesca a superare un livello, possa essere bloccata al successivo”,* ha aggiunto Divino.

- Utilizzate un'appliance di sicurezza integrata, anziché prodotti distinti.

Otterrete una protezione più efficace e non sarà necessario che impariate a utilizzare molteplici interfacce. Cisco Adaptive Security Appliance (ASA) Serie 5500, ad esempio, assicura una protezione completa dei contenuti tramite un'interfaccia comune con funzioni di filtraggio degli URL, antiphishing, antispam, antivirus e antispyware.

3. Concedere ai dipendenti un'eccessiva libertà di connessione da casa o in viaggio

Quando il personale si connette da casa o da hotspot pubblici, può accadere che i dati trasmessi vengano intercettati o che trapelino informazioni utilizzabili per violare la rete aziendale.

- Proteggete le sessioni su PC non di proprietà dell'azienda impostando VPN Secure Sockets Layer (SSL), criptando così i dati della sessione senza richiedere software client preinstallati. Cisco IOS SSL VPN scarica temporaneamente nel PC anche Cisco Secure Desktop per eliminare cookie, file temporanei, cronologia del browser e altri contenuti della cache dopo la chiusura della sessione.

4. Usare collegamenti non sicuri per connettere altri siti e partner

È facile usare Internet per collegare uffici remoti alla rete centrale, ma in che modo si possono rendere sicure le connessioni

- Risparmiate il tempo necessario per impostare manualmente le connessioni VPN tra un nuovo ufficio e tutti gli altri. La funzione EZVPN presente in Cisco Integrated Services Routers consente di configurare facilmente i router Cisco per inizializzare le VPN tra siti e client. Quando il dipendente di una filiale collega

il router, questo rileva automaticamente le informazioni necessarie dal router della sede centrale. La funzione EZVPN è disponibile anche per Cisco ASA.

- Vigilate su eventuali attività sospette in atto sulla rete tramite un sistema di prevenzione delle intrusioni (IPS). L'elaborazione IPS accelerata è disponibile come modulo software IOS per Cisco Integrated Services Router e come modulo hardware integrato per Cisco ASA. Pertanto non è necessario acquistare e gestire un dispositivo IPS distinto.



5. Lasciarsi ammaliare dal canto delle sirene

Molti hanno un'opinione propria sulla sicurezza informatica pur non essendo professionisti del settore. Per ricevere consulenza ad hoc, illustrate le vostre esigenze a un partner tecnologico certificato che sia competente in materia di sicurezza, conosca il settore pertinente la vostra attività e abbia già operato con aziende di dimensioni simili alla vostra. Vi fornirà soluzioni idonee al vostro ambiente, idee per ridurre i costi, assistenza nella configurazione delle policy di sicurezza e ulteriore supporto e servizi tecnici eventualmente necessari.