Bescherm uw draadloze netwerk tegen onbevoegd gebruik

Vijf veelgemaakte fouten

Het twijfelen aan de toereikendheid van uw netwerkbescherming kan u slapeloze nachten bezorgen. Wat hebt u over het hoofd gezien in de hectiek van uw werkdag? Verbeter uw nachtrust door de volgende veelgemaakte fouten te vermijden.

1. **Te snel draadloze netwerktoegang verstrekken**

"Gastgebruikers verwachten draadloze toegang en met het juiste beleid kunt u de toegang veilig maken", aldus Philip Stone, president van Boardwalk Communications, een Cisco Premier Partner met onder andere de certificering Advanced Wireless.

- Installeer een draadloos toegangspunt dat VLAN's ondersteunt, zoals een Cisco Aironet-toegangspunt, en installeer een gast-VLAN dat de toegang beperkt.
- Wijs willekeurige wachtwoorden toe aan gastgebruikers en stel hiervoor een specifieke vervaltijd in. Met de Cisco 2100 Series Wireless LAN Controllers kan uw receptioniste dit doen.
- Verzend niet de SSID's van uw bedrijf, maar alleen die van het gast-VLAN.
- Verminder het bereik. "Zorg ervoor dat u de instelling voor het bereik wijzigt, zodat u niet ook omliggende bedrijven bedient", aldus Jerry Divino, beveiligingsconsultant bij Boice Enterprises, een Cisco Certified Silver Partner met onder andere de certificering Advanced Security en Advanced Wireless.

2. **Bovennatuurlijke prestaties verwachten van een vertrouwd duo**

Het is een sprookje dat u genoeg hebt aan een netwerkfirewall en antivirussoftware. "In werkelijkheid hebt u een 'defense-in-depth'-benadering nodig. Als een aanval voorbij de eerste laag weet te komen, wordt deze alsnog tegengehouden door andere lagen", aldus Divino.

- Gebruik een geïntegreerde beveiligingtoepassing in plaats van aparte producten. Op die manier krijgt u betere bescherming en hoeft u niet te leren werken met verschillende interfaces. Zo biedt de Cisco Adaptive Security Appliance (ASA) 5500 Series omvangrijke inhoudsbeveiliging met URL-filters, antiphishing, antispam, antivirus en antispyware, allemaal met een gemeenschappelijke interface.

3. **Werknemers onderweg of vanuit huis te gemakkelijk verbinding laten maken**

De verbindingen die werknemers vanuit huis of openbare hotspots maken, kunnen worden onderschept of informatie achterlaten die kan worden gebruikt om in te breken in het bedrijfsnetwerk.

- Beveilig sessies vanaf computers die niet van het bedrijf zijn door VPN's met SSL (Secure Sockets Layer) te installeren. Deze coderen sessiegegevens zonder vooraf geladen clientsoftware te vereisen. Cisco IOS SSL VPN downloadt daarnaast tijdelijk Cisco Secure Desktop naar de computer om cookies, tijdelijke bestanden, browsergeschiedenis en andere inhoud in het cachegeheugen te wissen zodra de sessie wordt beëindigd.

4. **Niet-beveiligde verbinding maken met andere locaties en partners**

Via internet kunt u externe kantoren eenvoudig aansluiten op uw centrale netwerk. Maar hoe beveiligt u de verbindingen?

- Bespaar de tijd die u kwijt bent aan het handmatig opzetten van VPN-verbindingen tussen een nieuw kantoor en alle andere. Met behulp van de EZVPN-voorziening in de Cisco Integrated Services Routers kunt u Cisco-routers eenvoudig instellen om VPN's tussen locaties en klanten te initiëren. Wanneer een werknemer van een nevenvestiging de router aansluit, krijgt hij of zij automatisch de gewenste informatie van de router van het hoofdkantoor. EZVPN is ook beschikbaar voor de Cisco ASA.
- Ontvang waarschuwingen bij verdachte netwerkactiviteit door een inbraakpreventiesysteem (intrusion prevention system, IPS) te gebruiken. Een IOS-softwaremodule voor de Cisco Integrated Services Router biedt versnelde IPS-verwerking. IPS is tevens beschikbaar als geïntegreerde hardwaremodule voor de Cisco ASA. Beide voorkomen dat u een apart IPS-apparaat moet aanschaffen.

5. **Worden verleid door mooie woorden**

Iedereen heeft wel een mening over beveiliging. Als u advies wilt dat is toegespitst op uw onderneming, bespreekt u uw behoeften met een bevoegde technologiepartner die gespecialiseerd is in beveiliging en ervaring heeft met het mkb. Een dergelijke partner kan u voorzien van voor uw omgeving geschikte oplossingen, ideeën voor het minimaliseren van de kosten, hulp bij het implementeren van veiligheidsrichtlijnen en andere technische ondersteuning en services die u mogelijk nodig hebt.