Bezdrôtové pripojenia a bezpečnosť II.

V prvej časti článku (IW č. 12/2006) boli rozobrané základné princípy fungovania bezdrôtových sietí a vplyv ich prevádzky na bezpečnosť.

V 2. časti článku by sa mal záujemca o bezpečnosť bezdrôtových sietí oboznámiť so základnými bezpečnostnými princípmi týchto sietí, aby vedel nastaviť parametre prevádzky aktívnych prvkov a aby mu tieto nastavenia zabezpečili základný stupeň bezpečnosti.

Zvýšenie bezpečnosti

Nástroje, techniky a metódy bezdrôtových spojení, ktoré existujú, majú nedostatky. Ak sa však nepoužijú bezpečnostné nástroje, nie je zaistená bezpečnosť. Múdri robia prevenciu, nie takí múdri hasia, keď sa už niečo stane. Neodhalené útoky sa ťažko kvantifikujú, oveľa ťažšie, ako sa im predchádza. Je to niečo podobné ako s poistením: keď ho treba platiť, väčšina hundre, že sa aj tak nič nestane, a keď sa stane, každý je rád, že sa poistil.

Bezpečnosť WLAN závisí od dátovej vrstvy (2. vrstva OSI) a fyzickej vrstvy (1. vrstva OSI). Autentifikácia používateľov vo WLAN môže byť porovnávaná s fyzickou kabelážou, portmi a spojením, len s tým rozdielom, že predrôtované zariadenia sú nemobilné.

Podpora protokolov na druhej vrstve je podobná v oboch prípadoch. Ak sa šifruje na druhej vrstve, musia mať všetky zariadenia rovnaký šifrovací kľúč, keď chcú pristupovať na sieť. Preto sa neodporúča šifrovať eternetový protokol. Rovnaký kľúč len kompromituje bezpečnosť celej siete. Všetko, čo predlžuje čas na prelomenie prístupu do WLAN, zvyšuje bezpečnosť.

SSID (SERVICE SET IDENTIFIER) je od výrobcu nastavený na hodnotu dafault. Nikdy ho nenechajte v takom stave. Vyberte si nie veľmi obyčajné meno a nezverejňujte ho široko-ďaleko. Vypnite SSID broadcast na hodnotu *off*. To prinajmenšom spomalí inicializačný prienik.

802.11X – ak vaše zariadenie nepodporuje tento štandard, implementujte dodatočný hardvér a softvér, aby ste ho dosiahli. Je to štandard, ktorého frame je založený na EAP. Spoločnosti používajúce Windows XP môžu využiť server Radius, ktorý podporuje EAP-TLS, ako napr. Microsoft IAS. EAP-TLS však vyžaduje digitálne certifikáty na každej stanici a tento spôsob ešte v našich zemepisných šírkach ešte nie je veľmi používaný.

WEP, WPA A WPA2 – ak neimplementujete alebo nemôžete implementovať 802.11x, používajte WEP, WPA alebo najlepšie WPA2. WEP nie je perfektný, na internete je viac crackovacích nástrojov na jeho prelomenie. Ak vaše zariadenie nepodporuje WPA a musíte použiť aspoň WEP, vyskúšajte si pomocou internetových nástrojov, ako váš WEP obstojí oproti útoku. Ak budete pravidelne a často meniť kľúče, sťaží to kontinuálne prieniky do vašej siete. Nikdy nerozposielajte nové kľúče po sieti, nemáte nikdy istotu, že vo vašej sieti už niekto nepočúva. Nájdite si bezpečnejší spôsob na ich distribúciu.

RADIUS – implementujte tento autentifikačný protokol. Server RADIUS možno využiť na bezdrôtovú prevádzku, ale aj na „prevádzku po drôte".

IAS – ak používate Windows, použite Internet Access Server. Pozor, musí byť nainštalovaný a nakonfigurovaný pred jeho prvým spustením. Nie je súčasťou prvého setupu (prvotnej inštalácie).

Windows XP podporuje 802.1x a robí prirodzeného klienta pre IAS pre bezdrôtové, ale aj „drôtové" bezpečnostné služby.

EAP – používajte Extesible Authentication Protocol alebo jeho odrody (opísané v 1. časti článku), ktoré sú podporované IAS.

FIREWALL – ak ho umiestnite medzi WLAN a káblovú sieť, zabráni pri dobrej konfigurácii väčšine útokov a prienikov.

IDS A IPS (Intrusion Detection Systems a Intrusion Prevention Systems) – stoja za zváženie v pozitívnom zmysle, pretože dokážu identifikovať a IPS aj reagovať na prieniky a útoky, ktoré prejdú aj cez firewall. Pracujú na 4. až 7. vrstve OSI a pomocou správnej konfigurácie vedia už rozlíšiť, či ide o korektnú komunikáciu vašej používanej aplikácie alebo niekto simuluje podobnú prevádzku s cieľom preniknúť do siete.

ADRESY IP – odporúčam používať statické adresy IP pre každé bezdrôtové zariadenie; vypnite DHCP server a protokol. Budete možno hundrať, že je to menej flexibilné, ale bude to prípad aj druhej strany.

ADRESY MAC – požadujte na prístup deklarovanú adresu MAC. Hoci mnohé softvéry vedia imitovať ľubovoľné adresy MAC, ale na začiatku to sťaží prienik. Na druhej strane zabránime hneď v úvode komunikácie asociáciám s neznámymi bezdrôtovými stanicami.

VPN TUNELOVANIE – je to technika, pri ktorej je používateľský paket zabalený do chránených sieťových paketov, ktoré sú zvyčajne posielané protokolom IPsec. Pozor na distribúciu šifrovacích kľúčov, ak ich zistí útočník, je takisto zabezpečený ako vaša prevádzka. Pri použití monitorovacieho softvéru totiž vidíte len pohyb šifrovaných paketov, ale nevidíte, kto ich inicioval.

DIVERZIFIKUJTE UMIESTNENIE ANTÉN – táto technika umožňuje na jeden signál použiť dve alebo viac antén. Klient si vyhľadá anténu s najlepším signálom. Táto technika môže zabrániť útoku DOS.

Zakážte okamžite stratené zariadenie. Existuje aj novšia myšlienka, kde správca by mal schopnosť na ukradnuté zariadenie downloadovať interný kód, ktorý by ho znefunkčnil.

Identifikujte v sieti zariadenia, ktoré ste nepovolili. Niektoré zariadenia sú cenovo prístupné (až veľmi) a používatelia si ich pripájajú na pracoviskách, aby obišli firemnú politiku. Používajte nástroje na vyhľadávanie bezdrôtových zariadení a identifikujte, či sú všetky len tie, čo tam majú byť.

Keď sa zariadenie Wi-Fi asociuje s AP, bezdrôtová stanica posiela meno siete (SSID). Mnohé zariadenia akceptujú „NULL" alebo „ANY" nastavenie. Presvedčte sa, aby to nebol prípad vašej siete. Konfigurovaním ťažko hádateľného SSID, zakázaním broadcastu SSID zo strany AP a povolením módu closed system môžete odcloniť svojich susedov od náhodného pripojenia do svojej siete, ale nezastavíte *war driving*, pretože SSID sa dá vždy zistiť počúvaním frameov existujúcej prevádzky.

Väčšina produktov Wi-Fi podporuje autentifikáciu výzva/reakcia s použitím reťazca – kľúča – známeho pre AP a koncovú stanicu. *Shared Key Autentication* je jednoduchá ochrana, ktorá môže byť ochranou v prvej línii proti narušiteľom *war driver*. No SKA nevykonáva robustnú kontrolu prístupu. SKA je známa na každej stanici, ktorá potrebuje komunikovať s AP. A navyše je to statický element, používaný dlhý časový úsek. Ak je *Shared Key* prezradený alebo craknutý, zmena si vyžaduje reinštaláciu a opätovné nadviazanie spojenia. Pre malé siete WLAN to však nie je až taký veľký problém.

To boli spomenuté technické nastavenia, ktoré drvivá väčšina zariadení podporuje. Okrem toho ešte existujú aj aspekty bezpečnostnej politiky. Riadeniu bezpečnosti v spoločnostiach je venovaný iný článok.

MILOSLAV ĎURČÍK,
mdurcik@infoware.sk

Miloslav Ďurčík vyštudoval technickú kybernetiku na Technickej univerzite Ilmenau v Nemecku. V súčasnosti vedie spoločnosť RSN Systems, s. r. o.