Bezdrôtové pripojenia a bezpečnosť III

Riziká, ktoré hrozia bezdrôtovej sieti

WAR DRIVING

Je to metóda zisťovania existencie sietí Wi-Fi a možností vstúpiť do nich. Na jej realizáciu stačia aj jednoduché metódy a jednoduché zariadenia (ako napr. PDA s kartou Wi-Fi). Uskutočňovateľ hrozby a prieniku jednoducho chodí alebo sa pohybuje v dopravnom prostriedku po uliciach a napr. zariadenie PDA vybavené citlivou anténou Wi-Fi signalizuje prítomnosť konektivity Wi-Fi. Po vyhodnotení zabezpečenia sa bod možného vstupu zaznačí do mapy, prípadne dohodnutými značkami na chodník alebo plot pre ďalších používateľov.

NEAUTORIZOVANÉ POUŽÍVANIE ŠÍRKY PÁSMA

Všetky stanice komunikujúce s AP ukrajujú zo zdieľanej šírky pásma. Pri kalkulácii napr. s 802.11b, kde prenášaný kanál má 11 Mb/s, jeho réžia zníži kapacitu približne na 6 Mb/s. Pri slabom signáli sa táto prenosová rýchlosť ešte zníži približne na 1 Mb/s. A každé zariadenie, ktoré sa len hlási na AP, z tejto kapacity ešte ukrajuje.

NEAUTORIZOVANÝ PRÍSTUP DO INTRANETOVÝCH APLIKÁCIÍ

Bez vhodnej kontroly prístupu treba AP umiestňovať vždy do nedôveryhodnej časti siete, t. j. väčšinou pred perimeter chrániaci intranetové servery. Ak to neurobíte, otvárate dvierka neautorizovaným prístupom, útokom a kopírovaniu dát z intranetových serverov.

NEAUTORIZOVANÝ PRÍSTUP DO INTERNETU

Mnohí si možno povedia: „No a čo?" Neautorizovaná stanica vám však bude ukrajovať z WAN šírky pásma, čo sa nebude využívať na firemné prístupy. Kontrola adries MAC alebo kontrola na úrovni používateľov väčšinou postačuje ako účinné opatrenie proti tejto hrozbe.

PRIENIK DO BEZDRÔTOVÉHO ZARIADENIA

Urobiť vstup do cudzej siete je výzva sama osebe, ale čo tak vykonať prienik do koncovej stanice? Pokiaľ nie je aplikovaná bezpečnosť aj na koncové zariadenie, neautorizované bezdrôtové zariadenia môžu počúvať prevádzku z takejto stanice, vykonať prístup na zdieľané súbory a tlačiarne alebo uskutočniť útok DoS proti takto pripojenej stanici.

PRIENIK DO ACCESS POINTU

Najkritickejší bod na bezdrôtovej sieti je sám access point (AP). AP nesmie byť inštalovaný s default nastaveniami, ľahko uhádnuteľnými heslami na správu, SNMP comutity stringy a http/Telnet prístupnými portmi na vzdialenú správu. Dobrý tip je použitie rovnakých metód a predpisov nastavení ako pre prístupový smerovač WAN.

AUTENTIFIKAČNÉ RIZIKÁ

Pri strate alebo ukradnutí karty alebo zariadenia PDA treba zakázať MAC ACL a updatovať konfigurácie vrátane *shared keys*. Toto riziko možno znížiť použitím dvojfaktorovej autentifikácie.

Pri MAC spoofingu môže zachytávateľ frameov extrahovať platné adresy MAC a použiť ich na legitímne prístupy. Kombinácia MAC ACL s inými typmi autentifikácie môže sieť WLAN urobiť menej zraniteľnou na spoofing adries MAC.

Neautorizované AP sú veľkou hrozbou pre podnikové siete. Ceny mnohých neznačkových zariadení sú veľmi nízke a nie je to prekážka, aby si zamestnanec alebo náhodný návštevník nepripojil tajne do podnikovej siete svoj súkromný AP. Zo strany správy podnikovej siete to vyžaduje dôsledné využívanie monitorovacích metód a pravidelné vyhodnocovanie udalostí.

HĽADISKO SÚKROMIA

Prevádzka WLAN bez šifrovania umožňuje prípadným ďalším (neželaným) záujemcom pomocou analýzy prevádzky zistiť hodnoty, ako je SSID, adresa MAC a adresa IP. Získanie cieľovej adresy, požiadavky DHCP, dopytu DNS alebo NetBIOS broadcastu môže uľahčiť prístup do intranetu alebo k zdieľaným súborom.

Z uvedeného dôvodu odporúčam používať šifrovanie, ak nie je iná možnosť, pomocou WEP, ale radšej WPA alebo WPA2. Niektorí výrobcovia okrem štandardov ponúkajú aj neštandardné riešenia na bezdrôtovú autentifikáciu a súkromie, napr. použitím šifrovania DES, 3DES, Twofish alebo AES s výpočtom session key pomocou Diffieho-Hellmanovej metódy.

Výhodné pri podnikových aplikáciách môže byť použitie protokolu TKIP, ktorý spravidla predpokladá použitie 802.1X na autentifikáciu a poskytovanie kľúčov.

WEP a TKIP šifrujú framy len na bezdrôtových spojeniach. PPTP, IPSec alebo L2TP over IPSec šifrujú dáta na celom spojení zo vzdialeného zariadenia až do bezpečnostného gateway. Pre používateľov, ktorí už používajú prístupy VPN cez internet, je vhodné rozšíriť uvedenú službu aj pre zariadenia Wi-Fi. Pri tomto spôsobe môže byť s výhodou použitá vlastnosť niektorých AP, ktoré môžu fungovať aj ako VPN gateway.

Metódy, ktoré sa používajú na šifrovaný prenos z internetu, sú takisto využiteľné aj pri bezdrôtových prenosoch. Napríklad e-mailové správy sa môžu prenášať pomocou PGP alebo S/MIME, na vzdialenú administráciu môže byť použitý SSH a napr. remote desktop možno ovládať pomocou napr. GoToMyPC.

Na jednej webovej stránke venovanej bezpečnosti som našiel krátke a vcelku jednoduché pravidlá:

1. Nehovorte nie novým technológiám.
2. Nepredstierajte vysokú bezpečnosť a nízke riziko. Vyvážte zisk a risk.
3. Nereagujte bez rozmýšľania.
4. Nezanedbávajte cenu informácií.
5. Nezameriavajte sa na strom, pričom ignorujete celý les.

Prehodnoťte si aj vy, čo z toho dodržiavate.

Ako sa vlastne správať a ako postupovať, keď chceme zriadiť a prevádzkovať bezdrôtové pripojenia?

Väčšinou pri prevádzke bezdrôtových sietí ide o integráciu s drôtovými sieťami LAN. Výsledok tvorby bezdrôtových pripojení musí mať jednotnú štruktúru v celom rozsahu siete. To znamená, že existujú rozdiely v prístupoch, ktoré zvolíme pre malú, strednú alebo veľkú firmu. Použitie zariadení od jedného výrobcu pre drôtovú a bezdrôtovú časť poskytuje výhodu, hlavne pri správe siete, ale nie je to podmienka. V prvom rade je dobré poriadne si rozmyslieť, čo potrebujeme prepojiť, čo má s čím komunikovať a ktorej komunikácii chceme zabrániť. Investícia do poriadnej analýzy, aj keď stojí čas a peniaze, môže priniesť do prevádzky úspory, ktorých hodnota presiahne niekoľkonásobne vložené prostriedky. Treba pamätať na skutočnosť, že dobre a hlboko vykonaná analýza zabráni vzniku dodatočných požiadaviek na prevádzku a tým aj vzniku rôznych konfiguračných nedostatkov a nedôsledností, napr. aj z dôvodu nedostatku času, lebo prevádzka musí fungovať do stanoveného termínu. Analýza musí obsahovať štandardy, ktoré treba dodržať, zoznam aplikácií, ktoré sa prevádzkujú, a ich požiadavky na sieťové prostredie, úroveň služieb, ktoré je potrebné poskytnúť v sieti, požiadavky na rozširovanie do budúcnosti, použitú technológiu a cenu riešenia.

Pri malých kancelárskych riešeniach, kde väčšinou požiadavky nepresahujú niekoľko pristupujúcich používateľov, je pravdepodobne najvhodnejší access point pripojený priamo k lokálnemu prepínaču alebo priamo k pripojeniu WAN. Požiadavkám bezpečnosti možno vyhovieť pomocou WPA, pričom verejné a nechránené oblasti sa odporúča prekonať šifrovanými pripojeniami VPN. Na správu zariadení postačuje spravidla jeden monitorovací nástroj.

Pre riešenia s viac ako 5 prístupovými bodmi (stredne veľké kancelárie) má už význam aj distribúcia niektorých funkcií architektúry WLAN. Sú možné dva rozdielne prístupy k riešeniu. Pri prvom sa presúva bezpečnosť na centrálny kontrolér s plnými privilégiami na autentifikáciu používateľov. Podľa druhého sa uskutočňuje autentifikácia lokálne (v skutočnosti len reautentifikácia) a vzdialene. Rozhodnutie, nakoľko riešenie distribuovať, mnohokrát závisí aj od nákladov, ktoré sa majú na riešenie vynaložiť. Centralizácia je lepší spôsob na zníženie nákladov, distribuovanosť je podporovaná lepšími výkonovými ukazovateľmi. Centralizovaný spôsob riešenia predpokladá tunelovací protokol medzi prístupovým bodom a centrálnym kontrolérom. Niektoré centralizované riešenia môžu používať protokol GRE (Generic Routing Encapsulation) so špeciálnym rozšírením na podporu roomingu. Pokiaľ sú všetky použité zariadenia od rovnakého výrobcu, spravidla nevznikajú problémy. Náročnejšie to môže byť pri použití zariadení rôznych výrobcov, hoci veľká časť z nich deklaruje dodržanie štandardov.

Pre veľké kancelárske riešenia je typické pripojenie AP k lokálnemu prepínaču a nástup napájania cez eternet. Z dlhodobého hľadiska by však asi malo význam inštalovať aj prepínače s podporou WLAN. Väčšia šírka pásma a vyššia priepustnosť sú najviac sledovanými kritériami pri riešeniach do veľkých kancelárií. S AP niektorých výrobcov možno dosiahnuť priepustnosť 108 Mb/s, ale takéto riešenia nie sú štandardné. V prípade, že priepustnosť bezdrôtových pripojení nie je postačujúca, treba pristúpiť ku kombináciám s drôtovými riešeniami a efektívne plánovať využívanie pripojení spolu s overenými praktikami správy siete.

Na správne riešenie treba správne zvoliť aj používanú fyzickú vrstvu. Rozdiely medzi IEEE 802.11a, 802.11b a 802.11g boli opísané v prvej časti článku. Pri riešeniach do veľkých kancelárií odporúčam použiť 802.11a aj z pohľadu rozširovania do budúcnosti.

Umiestnenie AP

Všetky spôsoby návrhov vyžadujú úvodnú rekognoskáciu a spoznávanie podmienok v oblasti inštalácie. Tieto praktiky sa môžu pohybovať od prechádzky s handheldom s pripojením Wi-Fi až po sofistikované návrhové automatizované programové prostriedky. Všetky prístupové body by mali byť umiestnené na všeobecne dostupných miestach, aby nebol sťažený ich prípadný servis. 2,4 GHz a 5 GHz technológie odporúčam umiestňovať tiež spolu s ohľadom na prístupnosť. Aby bolo dosiahnuté nerušené pokrytie, je dobré body umiestňovať pod plafóny alebo vyššie budovy v závislosti od produktu, ale aj návrhu aplikácie. Umiestnenie AP možno dodatočne upravovať na základe pokrytia a potreby prenosových kapacít.

Na zabezpečenie prevádzky WLAN možno implementovať ďalšie doplňujúce spôsoby k už spomenutým šifrovacím metódam WEP, WPA a WPA2. Sem patrí napr. oddelenie bezdrôtovej prevádzky do osobitných VLAN (virtuálnych LAN), z ktorých možno kontrolovať prevádzku prostredníctvom ACL (Access Control List), prechodom cez firewall alebo IDS a IPS sondami. Ponúka sa aj riešenie umiestnenia bezdrôtovej prevádzky do DMZ (demilitarizovanej zóny) alebo úplne mimo LAN a firewallu. Zvýšenie autentifikačnej istoty poskytujú možnosti dvoj-, prípadne trojfaktorovej autentifikácie (napr. produkty RSA, Swivel a pod.).

Možnosti a prínosy viacstupňovej autentifikácie opíšeme v niektorej z nasledujúcich častí.

S bezpečnosťou WLAN súvisí aj zabezpečenie koncových bodov, a to nielen notebookov, ale aj PDA a mobilných telefónov. Aké sú konkrétne možnosti zabezpečenia týchto zariadení, tomu sa budeme venovať v inom článku.

V niektorom z nasledujúcich čísel si tiež povieme aj o novo nastupujúcej technológii RFID, nakoľko táto technológia prevádzkovaná na frekvenciách WiFi bude zaznamenávať čoraz väčší rozmach v blízkej budúcnosti.

■ 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.