Bezdrátová síť

jako nástroj elegantního zločinu!

Jiří Hološka

Rychlost, nenásilnost, s mizivým rizikem dopadení, to jsou hlavní výhody novodobých zlodějů firemních dat. Jak se před těmito útoky chránit? Strategie obrany může být stejně elegantní jako samotné provedení útoku. Nové trendy v bezpečnosti bezdrátových systému (WIPS) přechází od pasivních k aktivním opatřením založeným na stejných principech jako útoky samotné.

Neustále se měnící prostředí uživatelů v bezdrátovém prostředí dává prostor útočníkům rozvíjet svoje nekalé aktivity. Vzniká tak silný tlak na správce sítí řešit vzniklé hrozby nejlépe v reálném čase. Aktuální a přesné informace o provozu sítě jsou nejdůležitější komoditou pro správné vyhodnocení stavu a stanovení účinných protiopatření. Systémy schopné automaticky spravovat a vyhodnocovat informace na základě definovaných modelů jsou dnes již běžně součástí produkčních řešení. Přináší snížení zátěže na IT pracovníky a zvyšují efektivitu řešení negativních událostí.

WiFi obecně

Díky rostoucímu počtu aplikací využívajících internetových služeb v mobilních zařízeních, jako jsou chytré mobilní telefony, PDA, notebooky, tablety apod., roste i tlak na bezdrátovou konektivitu pro tato zařízení. A právě WiFi patří mezi nejsnáze dostupné technologie, ať už z důvodu široké podpory zařízení, tak nízkých nákladů na provoz a údržbu sítě.

Firemní nasazení

Při nasazení bezdrátových zařízení ve firemním prostředí je nutné počítat s určitým kutilstvím ze strany zaměstnanců. Ti totiž dříve nebo později zjistí, že ačkoliv firemní síť neumožňuje přístup k oblíbeným službám, jakými jsou bezplatné e-mailové a komunikační služby nebo sociální sítě, lze snadno najít způsob, jak omezení firemních politik obejít.

Přístup k blokovaným službám lze získat například prostřednictvím veřejné WiFi sítě, kterou provozuje kafetérie přes ulici. Veřejná síť obvykle žádné restrikce nemá, tudíž se zaměstnanci mohou jednoduše připojit a získat nefiltrovaný přistup do internetu. Zaměstnanci se také mohou pokoušet vytvořit privátní WiFi síť ve firemním prostředí (např. připojením vlastního přístupového bodu do firemní sítě) a zajistit tak přístup k internetu pro svá mobilní zařízení a zařízení svých kolegů.

V obou uvedených případech se otevírá cesta do firemní sítě, která v krajních případech může znamenat přístup k firemním systémům a únik firemních informací.

Zabezpečení bezdrátových sítí

Bezdrátové sítě mají ve firemním prostředí velký potenciál. Před jejich nasazením je ale nejdříve nutné dosáhnout stejné úrovně zabezpečení dostupných informací a služeb jako u kabelových sítí (viz vsuvka).

I nejlepší metody šifrování však řeší pouze problematiku vysílání chráněných informací do bezdrátového prostředí a jako autentizační prvek k přístupovému bodu.

Řízení přístupu v bezdrátových sítích

Na rozdíl od WiFi jsou kabelové sítě snadno definovatelné v prostoru v podobě koncových přístupových bodů. Nedá se předpokládat, že by konektivity chtivý uživatel otevřel kolektor s rozvody datových kabelů, vytáhl náhodně vybraný kabel, nacvakl příslušnou koncovku a následně se připojil do sítě. Ovšem u bezdrátových sítí je tato činnost naprosto běžným jevem. Zařízení s podporou WiFi neustále monitorují dostupné sítě a v případě shody s definovaným přístupovým bodem v paměti zařízení se pokouší o spojení.

Bezdrátové sítě jsou plánovány pro maximální možné pokrytí prostoru signálem. Bohužel právě díky této vlastnosti dochází k přesahu signálu i mimo prostory, pro které byl provoz bezdrátových zařízení původně plánován. Signál se tak stává dostupný i pro veřejnost a představuje jakousi vstupní bránu do firemní sítě.

Problematické jsou zejména již zmiňované přístupové body, které si nainstalují sami zaměstnanci, bez dalšího schválení nebo nastavení od pracovníků IT zodpovídajících za provoz počítačové sítě. Takto vytvořené přístupové body jsou méně odolné vůči útokům a nejsou nijak svázané se systémy detekce, prevence průniků a řešení zranitelností.

S ohledem na všudypřítomnost bezdrátových signálů je tedy více než vhodné provádět monitorování prostorů, které lze považovat za neveřejné. Audit bezdrátových sítí a jejich klientů je jedním ze základních prvků pro globální bezpečnost ICT zdrojů ve firemním prostředí.

Pasivní detekce

Existuje několik technik, jak bezdrátové prostředí kontrolovat. Pasivní monitoring představuje základní techniku, kdy zaměstnanec v pracovní době obejde s mobilním skenovacím zařízením (notebook, PDA, mobilní telefon, tablet) vytipovaná místa chráněného prostoru, otestuje aktuální stav sítí a klientů a následně zpracuje analýzu provozu.

Zásadní slabinou této metody je výskyt monitorovacího zařízení na daném místě jen po velmi krátkou dobu, maximálně v desítkách minut, což nezaručuje zachycení veškerého provozu. Následná analýza nalezených sítí a jejich uživatelů je poměrně časově náročný proces, který zbytečně zatěžuje zaměstnance IT oddělení zodpovědné za bezpečnost síťové infrastruktury.

Automatizovaná analýza

Sofistikovanější systémy již dnes mají zpracované metodiky pro automatické vyhodnocování získaných dat, a značně tak ulehčují a zrychlují celkovou analýzu. Využívají upravená zařízení umožňující přesnější snímání v definovaných místech chráněného

Historie zabezpečení WiFi

Nejstarším mechanismem pro zabezpečení bezdrátových WiFi sítí je šifrování WEP. Základním prvkem zabezpečení se stal WEP na základě původního standardu IEEE 802.11 z roku 1997. Šifrování WEP je dodnes hojně využíváno, a to i přes to, že už více jak deset let není považováno za bezpečné a jeho prolomení trvá průměrnému uživateli ne více jak deset minut. V roce 2001 byl přijat nový standart IEEE 802.11i pro zabezpečení bezdrátových sítí a následně WPA2 odstraňující nedostatky starší verze standardu WPA, které do něj byly zavlečeny z důvodu zpětné kompatibility se zařízeními podporujícími pouze šifrování WEP.

Obr. 1: Stacionární aktivní senzor pro nepřetržitý sběr informací o provozu v bezdrátovém prostředí, přístupový bod a appliance s možností instalace do racku

prostoru, a tím i částečnou lokalizaci sítí a uživatelů.

Avšak i tyto systémy trpí stejným problémem jako prvně zmíněné, jedná se stále o pasivní snímání v omezeném čase. Zařízení jsou primárně určena pro přehledovou detekci bezdrátových zařízení, interferencí v rádiových signálech a dodržování základních bezpečnostních politik pro bezdrátové sítě. Tento způsob monitoringu není schopný ve většině případů detekovat aktivní útoky na bezdrátové přístupové body nebo klienty. Stejně tak jako není schopný odhalit dočasné přístupové body a ad hoc sítě vytvářené přímo mezi klienty bez použití přístupových bodů.

Aktivní prevence

Přední dodavatelé a vývojáři bezdrátových detekčních a prevenčních systémů jsou si plně vědomi nedostatků stávajících řešení. Proto se na trhu poslední dva roky objevují nová řešení založená na stacionárních aktivních senzorech rozmístěných v chráněném prostoru, zajišťující nepřetržitý sběr informací o provozu v bezdrátovém prostředí. Vyhodnocování získaných dat je prováděno na firemních serverových stanicích (appliance), popřípadě na zařízeních umístěných v zabezpečených cloudových datacentrech.

Stacionární senzory jsou dodávány výrobci ve formě specializovaného zařízení, které kromě pasivní detekce bezdrátových zařízení podporují i aktivní prevenci proti nežádoucím zařízením v pásmech 2,4 GHz a 5 GHz. Díky proaktivnímu přístupu k řešení hrozeb lze cíleně zablokovat nebo zarušit vybraná sítová spojení, omezit účinky útoku cíleného na odepření dostupnosti služeb (DoS), aktivní pokusy o prolomení šifrování na přístupových bodech, krádeže identit pomocí klonování MAC adres bez omezení autorizovaných uživatelů atp.

Aktivní přístup při řešení hrozeb a zranitelností tak posouvá bezdrátové sítě z pohledu zabezpečení téměř na úroveň kabelových sítí.

Novinky na poli WIPS

Jednotlivá řešení pro detekci a prevenci narušení bezdrátových sítí jsou dostupná jako součást plánované infrastruktury bezdrátových sítí, nebo jako zcela nezávislá zařízení, která jsou integrována do stávající bezdrátové sítě. Hitem nejnovějších produktů je možnost pořídit zařízení pro ochranu bezdrátových sítí jako software as a service (SaaS) a radikálně snížit náklady na zavedení služeb zabezpečení bezdrátových sítí. Nespornou výhodou je dostupnost uživatelského portálu přes internet přímo z datového centra a jednoduchost zabezpečení sítí provozovaných na pobočkách po celém světě. Motivací pro nasazení autonomních detekčních a prevenčních systémů jsou často interní politiky a bezpečnostní standardy, kterými se firmy musí řídit. Integrace detekčních a prevenčních systémů se systémy správy zranitelností dovoluje automaticky testovat veškeré bezdrátové vybavení na známé zranitelnosti, díky čemuž lze snadno dosáhnout a garantovat shodu s bezpečnostními standardy, jako jsou PCI DSS, Sarbanes-Oxley (SOX), HIPAA, GLBA, DoD Directive 8100.02.

Obr. 2: Přehled trhu WIPS pro rok 2010

	Silně negativní	S výstrahou	Nadějný	Pozitivní	Silně pozitivní
AirTight Networks				●	
Motorola (Air Defence)				●	
AirMagnet			●		
Aruba Networks			●		
Cisco			●		
AirPatrol		●			

Zdroj: Gartner (Červenec 2010)

Přehled trhu WIPS

Analytická společnost Gartner vydala v minulém roce zprávu o trhu řešení pro detekci a prevenci narušení bezdrátových sítí (WIPS). V přiložené tabulce (obr. 2) je uveden výsledný žebříček prodejců WIPS, který vznikl na základě součtu dílčích hodnotících kritérií definovaných analytiky Gartner. Trhu WIPS, dle uvedeného průzkumu, nedominuje žádný lídr s nejvýše udělovaným hodnocením „silně pozitivní“, nicméně čelu pomyslného pelotonu s druhým nejvýše udělovaným hodnocením „pozitivní“ vévodí dvě firmy. Společnost Airtight Networks s produktem SpectraGuard, který je nyní nabízen i ve formě cloudu jako SaaS, a společnost Motorola s produktovou řadou AirDefense, která vznikla na základě akvizice stejnojmenné společnosti z roku 2008.

Zdroje:

Edney, Jon, Arbaugh, William A. 2003. Real 802.11 Security: WI-Fi Protected Access and 802.11i. Addison-Wesley.

Autor je studentem doktorandského studijního programu na Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně a spolupracuje se společností Risk Analysis Consultants.