



Redakční otázky k tématu

OCHRANA PERIMETRU SÍTĚ - IDS/IPS, FIREWALLY A JINÉ BEZPEČNOSTNÍ SÍŤOVÉ PRVKY

odborného on-line magazínu ICT SECURITY – www.ictsecurity.cz

Jak může vhodně vybrané bezpečnostní řešení ulehčit práci bezpečnostním technikům

Autor odpovědí:

Marian Lysák, Senior Security Consultant, COMGUARD a.s.

1) Které bezpečnostní síťové komponenty jsou pro perimeter „need to have“ (postačuje firewall?) a které „nice to have“?

Firewall v dnešní době není jen jednoúčelové řešení, které reguluje provoz na perimetru. Kvalitní firewall od stabilní společnosti nabízí modulární řešení, které pokrývá všechny možné způsoby útoků na servery nebo počítače uživatelů ve vnitřní síti. Kromě řešení základního bezpečnostního problému, oddělit neznámou, tedy potenciálně nebezpečnou síť od té, kterou známe a chceme chránit, nebo oddělení dvou sítí, které slouží pro různé účely, a tím eliminovat bezpečnostní rizika komunikace mezi nimi, tu máme v současnosti daleko větší nároky kladené na tyto zařízení.

Do základního seznamu řešení patří regulace provozu na základě parametrů TCP spojení (portů, adres apod.), kontrola samotných aplikačních protokolů (http, smtp, dns apod.), oddělení toku dat na proxy branách (dlouhodobě největší zkušenosti mají ve firmě McAfee při dlouhodobém vývoji Enterprise Firewallu, dříve firewall Sidewinder od společnosti Secure Computing). Proxy brány a aplikační ochrana umožňuje kontrolu provozu na známé hrozby (signatury antiviru a antispyware řešení). Vyspělejší firewally nabízí i modul IPS, který umí detekovat a blokovat známé i neznámé útoky. Zároveň pak umí reportovat dané události do srozumitelné formy, aby bezpečnostní pracovník mohl vyhodnocovat rizika a problémy na síti a reportovat situaci managementu.

Nyní jsme v situaci, kdy "Nice to have" u enterprise řešení je určitě v situaci "need to have". Samozřejmostí je definice provozu na základě uživatelů v adresářové struktuře nebo detekce aplikací bez znalosti dodatečných parametrů dané aplikace (na kterém portu komunikuje). Při výběru řešení se určitě ptejte, jestli kromě samotných základních funkcionalit firewallu dostanete i něco navíc. Důležitý je například samostatný reportovací nástroj se sběrem dat a analyzátor problémů na síti (např. McAfee Firewall Profiler).

Kolik stojí tyto dodatečné funkcionality? Je to zdarma nebo za příplatek? Ptejte se na to Vašich dodavatelů. Zabráníte tak nemilému překvapení, že navenek robustní řešení po zakoupení má jen zlomek toho, co dodavatel slíbil nebo čím Vás zaujal.



2) Jaké jsou trendy pro co nejlepší zabezpečení firemního perimetru?

Velkým současným trendem je detekce aplikací a detekce uživatelů, kteří komunikují přes firewall. Musíme si uvědomit, že správa takového prvku je velmi komplikovaná. Vyžaduje, aby správci firewallu byli pravidelně školeni na nové verze a hlavně na to, aby dostatečně podrobně znali situaci na síti a uměli analyzovat provoz, který prochází přes zařízení. Znamená to velké výdaje do potřebných celkových znalostí, aby toto zařízení mohl úspěšně spravovat.

Co kdyby správu firewallu mohli zvládnout i méně znalí uživatelé/správci, co kdyby problémy na síti odhalovali ještě rychleji než ti, co spravují tato řešení roky a používají standardní řešení? Nad tímto se zamysleli největší výrobci bezpečnostních technologií a vyvinuli model detekce aplikací (např. AppPrism od McAfee) a uživatelů (např. Logon Collector od McAfee). Administrátor nemusí již zjišťovat detailní informace (na jakém portu daná aplikace komunikuje nebo jakou IP adresu má daný počítač), aby vyřešil problém. Stačí vědět jméno aplikace a jméno uživatele pro definici přístupu.

Dalším průlomem je detekce problémů na síti. Účetní nemůže přistoupit na bankovní portál. Obchodník nemůže zadat objednávku do systému. Všechny tyto problémy znamenají pro firmu finanční ztráty z důvodu pozastavené práce. Administrátor je postaven do nelehké role. Musí analyzovat, kdo a kam chce přistupovat a proč tento přístup není umožněn. Musí se dívat do různých logů na různých místech, do pravidel na firewallu, ve snaze zjistit příčinu těchto problémů. Nejmodernější technologie Vás ale zbaví těchto problémů. Proč by toto hledání a zkoumání nemohl udělat stroj? Na Vás bude jen podívat se, kde je problém a jak jej vyřešit. Příkladem, lépe řečeno průkopníkem, je řešení McAfee Firewall Profiler, který Vám tak pomůže se spoustou starostí a práce, kterou nyní dělá stroj a ne člověk.

3) Jak se liší zabezpečení perimetru v závislosti na službách, které chceme chránit?

Vždy je otázkou, jak si firma cení aktiv, které musí být chráněny, a jak moc se rozhodne aktiva chránit. Některým podnikům stačí firewally, které nedisponují všemi dostupnými technologiemi, ale které nabízí základní řešení postačující pro ochranu dat a uživatelů. Naopak jsou firmy, u kterých v případě odcizení produktu, dat nebo know-how může dojít k velkým problémům, zhoršení konkurenceschopnosti, případně i pádu podniku. Pro tyto firmy je velmi důležité jít s dobou a obstarat si nejnovější technologie a plnohodnotnou bezpečnost. Nejnovější technologie jsou nejbližší ideální bezpečnosti a tím mají největší pravděpodobnost úspěchu při ochraně aktiv firmy.



4) Jaké typy zařízení byste doporučili implementovat do oblasti perimetru (případně do vnitřní sítě či jinam) v těchto případech:

- a) **Menší výrobní společnost (do 20 zaměstnanců) má v DMZ emailový server a file share. Zaměstnanci mají zevnitř povolený přístup na http/https a z Internetu vzdálený přístup do DMZ a vnitřní sítě (webový sever je v hosting centru).**

Z portfolia firmy COMGUARD (VAD distributora řešení IT bezpečnosti v ČR a SK) bych se podíval po řešení firewallu Cyberoam. Tento firewall výborně splňuje nároky malých firem a zároveň svojí funkcionalitou překoná konkurenční řešení.

- b) **Středně velká společnost – zásilková služba s tracking systémem (cca 100 zaměstnanců) má v DMZ emailový server, webový server a file share. Zaměstnanci mají zevnitř povolený přístup na http/https a z Internetu vzdálený přístup do DMZ.**

Z portfolia firmy COMGUARD (VAD distributora řešení IT bezpečnosti v ČR a SK) bych se podíval po řešení firewallu McAfee Firewall Enterprise. Tento firewall přináší plnou funkcionalitu enterprise firewallu bez dodatečných omezení nebo vypnutých modulů. Obsahuje všechny prvky ochrany již v základu – aplikační kontrolu / proxy brány, IDS/IPS, TrustedSource, Antivirus, Antimalware, AppPrism, Logon Collector, Firewall Reporter, Firewall Profiler, atd.

5) Jaké máte nové produkty či řešení pro zabezpečení firemního perimetru?

Jak už jsem naznačoval v odpovědi na otázku č. 2, jedná se především o systémy pro detekci aplikací a uživatelů McAfee Logon Collector a AppPrism a také systém pro odstraňování problémů na síti McAfee Firewall Profiler. McAfee Logon Collector aktivně sleduje přihlašování uživatelů do sítě a tento stav reportuje firewallu, který pak reguluje provoz na základě takto získaných dat. Na firewallu se tak dají používat jména skupin nebo uživatelů z adresářové struktury (Active Directory). Podobně jako Antivir má databázi signatur virů, pomocí níž se detekují viry, tak i pro detekci aplikací je potřeba databáze. AppPrism je databáze signatur aplikací. Administrátor zadává jen jméno aplikace, kterou chce povolit přes firewall, a nemusí ho zajímat, na jakých portech daná aplikace funguje. Zkoušeli jste povolit aplikaci, která používá náhodné porty? Pokud ano, tak již nyní tušíte, že AppPrism Vám ušetří spoustu práce.

Další novou technologií určenou pro ušetření práce je McAfee Firewall Profiler. Každý administrátor řeší denně problémy typu, že někde něco nefunguje. Analyzuje situaci tím, že se dívá do různých logů, do pravidel na firewallu řeší, proč někde nefunguje určitá komunikace. McAfee Firewall Profiler ušetří mnoho práce tím, že tyto problémy sám odhaluje a ukazuje, co je potřeba změnit na síťových prvcích tak, aby komunikace fungovala zase v pořádku.