

foto Martin Kovář

NEEXISTUJE STOPROCENTNÍ OBRANA

Za redakci se ptal Michal Hroch

S Hanušem Adlerem z firmy Actinet jsme hovořili o tom, jestli existuje hrozba, proti níž se nelze bránit, zda nás spasí dnes populární preventivní systémy a zda může být situace v IT z pohledu bezpečnosti ještě horší, než je v současnosti.

Jakým jedním slovem byste vyjádřil aktuální stav informačních technologií z pohledu firmy, která se zabývá bezpečností, a proč?

Nemám v oblibě jednoslovné odpovědi, protože se jim málokdy podaří vystihnout realitu. Právě v oblasti bezpečnosti IT je taková odpověď zvláště těžká, protože úroveň zabezpečení se v konkrétních případech pohybuje od katastrofální až po vynikající. Pokud mohu soudit z našich zkušeností, převažuje zatím spíše nedostatečná úroveň zabezpečení.

Jsme nyní již v kritické situaci z pohledu virových a červových nájezdů, nebo může být stav ještě daleko horší?

Nemyslím si, že jsme v kritické situaci. Kritická situace by nastala, kdyby některý z těch úspěšných virů posledních týdnů byl skutečně napsán s úmyslem rychle a co nejvíc škodit.

Představme si virus, jehož účelem je se během co nejkratší doby maximálně rozšířit, a ještě než se většině uživatelů podaří počítače odvírovat, přeformátovat jejich disky. Nebo virus, který spolu se sebou samým rozešle na náhodně vybrané adresy vaše texty, tabulky, prezentace, kopie e-mailů apod.

Existují typy útoků, kterým se firma v současnosti prostě nemůže bránit? Pokud ano, jaké?

Ne. Bránit se můžete proti každému útoku, dokonce i proti distribuovanému DoSu nebo spamu, otázka je, zda budete vždy dostatečně úspěšní. Mnohé z útoků totiž vyžadují obranu, která se nedá snadno koupit, která se dlouho a mnohdy bolestně vyvíjí u jednotlivých zaměstnanců - vzdělání, znalosti, myšlení, loajalitu. Firma může (a musí, myslí-li to s bezpečností vážně) mít bezpečnostní politiku, výkonné technické ochranné prostředky - firewally, bezpečnou autentizaci, šifrování, antiviry, content filtering a IDS/IPS, a přece stačí jeden neukázněný zaměstnanec, který většinou z nepozornosti, hlouposti nebo lenosti provede něco, co firmu ohrozí.

Nejdůležitějším úkolem současnosti je rozbít mýtus, že uživatel nemusí o počítačích vědět vůbec nic, že stačí umět klikat na ikonky a psát na psacím stroji. Každý uživatel by se měl vzdělávat v počítačové bezpečnosti a naučit se při práci s počítačem

přemýšlet o tom, co vlastně dělá, aby se nestal pro svého zaměstnavatele hrozbou.

Co říkáte na aktuální politiku společnosti Microsoft zaměřenou především na bezpečnost?

Velmi oceňuji fakt, že Microsoft se už druhým rokem zabývá bezpečností svých produktů, zvláště vzhledem k jejich rozšířenosti je to nesmírně potřebné. Zároveň si uvědomuji, jak je to složitá a zdouhavá práce, jak je ztížena tím, že mnohé produkty Microsoftu byly od samého počátku vyvíjeny s minimálním přihlédnutím k požadavkům bezpečnosti, že tzv. uživatelská přítulnost měla vždy přednost před zabezpečením. Důsledkem toho je, že Microsoft nyní musí nesmírně obtížně řešit bezpečnostní problémy, které by při lepším přístupu k vývoji nejspíš vůbec nebyly vznikly; musí „roubovat“ bezpečnostní záplaty na software, který má v sobě nejen obyčejné chyby, ale který je od samého počátku postižen chybným a nebezpečným návrhem.

Dokážete odhadnout, na kolik jsou řešení IDS/IPS úspěšná v odchyťování reálných útoků na síť v poměru ke znemožněným „legálním“ pokusům o komunikaci?

Odpověď záleží na schopnostech administrátorů těchto zařízení. Z našich zkušeností vyplývá, že bez patřičného odladění je míra falešných poplachů příliš vysoká a celkově pak nasazení IDS/IPS ztrácí smysl. Dobře konfigurovaný systém naopak může při zabezpečování sítí významně prospět.

Vaše firma se zabývá prováděním penetračních testů na zakázku. Jaké firmy jsou nejčastějšími zákazníky a kolik celkových zákazníků máte průměrně za jeden měsíc?



Penetrační testy provádíme většinou jako pravidelnou dlouhodobou službu. Snažíme se dodržovat zásadu, že penetrační testy má provádět jiný dodavatel než dodavatel zabezpečení, aby jejich výsledky byly naprosto nestranné. K nejčastějším zákazníkům patří obecně ty organizace, u kterých je potřebná vysoká úroveň zabezpečení IT, jako např. finanční instituce, některé státní úřady apod.

Co je výstupem penetračního testu?

Výstup má několik součástí. Na začátku je seznam strojově nalezených potenciálních problémů – těch je vždy více než problémů skutečných. Úkolem konzultanta je odlišit podstatné od nepodstatného, zhodnotit reakci personálu zákazníka na útok a co možná nejsrozumitelněji mu vysvětlit zjištěné problémy. Dále je třeba doporučit jejich řešení a případně poskytnout pomoc, pokud zákazník sám nebo jeho dodavatel bezpečnostního řešení nemá potřebné schopnosti.

Jaké je procentuální vyjádření poměru nezabezpečených (špatně zabezpečených) a zabezpečených sítí, pokud vycházíme z výsledků penetračních testů?

Neděláme si v tomto směru statistiky, takže nemůžeme odpovědět přesně. Podle mých zkušeností je špatně zabezpečených sítí více.

Využíváte u vás ve firmě aplikačního firewallu? Pokud ano, proč jste zvolili tento typ firewallu?

Ano i ne, trochu použité přístupy kombinujeme. Myslím, že žádný typ firewallu není sám o sobě spasen, že nejlepší je kombinace stavového filtrování paketů s aplikační kontrolou prováděnou zvlášť zejména pro e-mail a běžně používané protokoly jako např. HTTP, FTP, DNS apod. Samotný firewall je hezká, ale sama o sobě poměrně málo účinná věc. Hodně záleží na tom, jak je zapojen, jaká je to

pologie sítí kolem něj, jak jsou nakonfigurována jeho pravidla, jaké jsou reakce obsluhy na jeho výstupy a jaké další bezpečnostní systémy mu pomáhají.

Co si myslíte o nových technologiích u firewallů jako deep packet inspection nebo port knocking?

Především si nemyslím, že se jedná o nové technologie (i když port knocking je zajímavá a poměrně nová myšlenka, která se mi velmi líbí). Deep Packet Inspection (nebo u jiných výrobců Application Intelligence) je něco, co v podstatě měly firewally už před mnoha lety – vlastně všechny aplikační brány měly to, co dnes marketing některých firem označuje za převratnou novinku. Dokonce i některé stavové paketové filtry, jako např. FireWall-1, měly možnosti provádět takovou kontrolu spojení, i když ji třeba využívaly jen pro malý počet vybraných protokolů (v případě FW-1 to bylo už ve verzi 4.1 např. DNS).

Jinak si myslím, že Deep Packet Inspection je samozřejmě krok správným směrem, směrem, který podle mne postupně smaže rozdíly mezi IDS a firewally. Ostatně, další víceméně marketingový termín – IPS – vznikl k označení téhož, jen tentokrát přichází z opačné strany, od výrobců IDS.

Myslíte si, že SSL VPN v budoucnu převládne? Používáte VPN a k čemu?


Nemyslím si, že převládne. Určitě si najdou své uživatele, stejně jako si je našly VPN založené na IPSECu nebo prostě jen šifrovaná spojení s tunelováním TCP spojení, samozřejmě mám na mysli SSH. Každá z těchto technologií má své výhody i nevýhody.

V naší firmě pochopitelně používáme VPN různých typů, je to dáno rozdíly mezi uživateli různých operačních systémů a osobními preferencemi. Například já mohu ze svého firewallu chráněného notebooku díky šifrovanému a bezpečně autentizovanému přístupu pracovat vzdáleně prakticky stejně efektivně a bezpečně, jako když sedím v kanceláři. Také veškeré vzdálené zásahy u našich zákazníků provádíme šifrovaným spojením, stejně tak zasílání poplachových zpráv a logů, které pro zákazníky schraňujeme a průběžně analyzujeme, se děje šifrovaně. □

HANUŠ ADLER

Hanuš Adler se zabývá bezpečností IT od r. 1996, kdy se mj. podílel na technickém zajištění vstupu společnosti Check Point na český trh. V současné době je ředitelem společnosti Actinet Informační systémy, s. r. o., která se zaměřuje na služby v oblasti bezpečnosti IT. Ve volném čase rád čte a zajímá se o starou hudbu.





STOP

obavám o bezpečnost


START

McAfee® ePolicy Orchestrator®


Aby Vaše firma rostla, musíte se soustředit na... svůj byznys. Ne na obavy o systémovou bezpečnost.

Naše doporučení: **McAfee® ePolicy Orchestrator™**. McAfee Security Vám pomůže identifikovat hrozby ve Vaší firmě a zastaví je. Nyní můžete z jediné konzole umístěné kdekoli ve Vaší organizaci, pod jednou taktovkou, dirigovat ochranu proti nepřátelským hrozbám na všech desktopech, noteboocích, serverech a vstupních branách.

Chcete se dozvědět více? Kontaktujte naše Elitní partnery nebo jděte na www.mcafeesecurity.com.



Vinohradská 184, 130 52 Praha
tel.: 267 311 402, obchod@aec.cz
www.aec.cz



Šátalská 1 c/d, 142 00 Praha 4
tel.: 241 091 003, dataguard@pcs.cz
www.dataguard.cz

www.mcafeesecurity.com
Vladimir_Broz@nai.com

Network Associates®

INZERCE ▼
Network Associates, McAfee, Entercapt a IntruShield jsou registrované ochranné známky společnosti Network Associates, Inc. a/nebo jejích sesterských společností na území Spojených států amerických a/nebo jiných států. Produkty značky Sniffer® jsou vyráběny pouze společností Network Associates, Inc. Veškeré ostatní registrované i neregistrované ochranné známky obsažené v tomto dokumentu jsou výhradním vlastnictvím daných právnických nebo fyzických osob. © 2004 Network Associates Technology, Inc. Všechna práva vyhrazena.