Trendy v bezpečnosti počítačových sítí

Václav Lorenc, Honeywell, spol. s r.o.

Netflou sondy, fájrvóly,
bezpečnostní Velká zeď.
Dat nám z toho lezou hory,
jenže … co s tím dělat teď?

Ve světě počítačových sítí je možné pozorovat poměrně rychlý vývoj techniky, která lidem umožňuje vyměňovat si vzájemně informace. V souvislosti s tím se však objevuje celá řada problémů, zejména stran bezpečnosti uživatelů a dat. Jaké pokroky a vyhlídky je možné očekávat v této oblasti?

1 Čeho je moc, toho je příliš

Počítačové sítě byly původně prostředím přátelským, ve kterém se jednotliví účastníci snažili k sobě chovat slušně a spořádaně. Později přišly první útoky a s nimi i první obranné mechanismy. S většími sítěmi a méně technicky znalými uživateli se ukázalo, že bude možná vhodnější umisťovat různé linie obrany ještě před nicnetušící uživatele. A tak se začala objevovat jednoduchá pravidla bránící důležité součásti firemních i akademických sítí. Stejně jako slavnostní pořízení prvního modemu, prvního serveru a prvního displeje z tekutých krystalů, i provoz firewallů byl pln očekávání a obav, naplněných i lichých.

Jedna ze zajímavých průvodních vlastností firewallů je ta, že rády povídají svým administrátorům, co všechno se jim děje. To samé umí i chytřejší aktivní síťové prvky. Jsou-li takových zařízení nejvýše jednotky, ještě se to dá vše zvládnout. Pokud jich je několik desítek, přestává už být v silách i těch nejšikovnějších správců pročítat denní hlášení a včas reagovat na potenciální problémy.

Na ÚVT vznikla před několika lety pro potřeby Oddělení datových sítí závěrečná práce, která zpracovávala část informací generovaných aktivními prvky – systémové logy, tzv. syslog. Díky tomu je možné každé ráno obdržet nejen souhrnný přehled toho, co si jednotlivé stroje myslí o chování vlastním i připojených zařízení, ale i výčet podivností, rozličných nekonzistencí a případných bezpečnostních incidentů, které tato zařízení uměla rozpoznat a povšimla si jich za minulý den.

Jednalo se o výrazné, byť pouze dočasné zlepšení. Záhy se totiž objevila nová vlna internetových červů, které mají v popisu práce vyhledávat zranitelnosti připojených strojů a co nejrychleji se šířit dál. Hlášení podávané ráno tak bylo stále zajímavé, ale aktuální problémy bylo nutné odhalovat a řešit rychleji.

Navíc se kvůli rozvoji služeb instalovala celá řada dalších a dalších zařízení dožadujících se moudrého a vlídného dohledu – bezdrátové sítě a jejich centrální řídící prvky, autentizační a autorizační servery, systémy na detekci a prevenci síťových útoků (IDS, IPS), sondy sbírající informace o provozu v síti, síť Eduroam a s ní i autentizační protokol 802.1x…

Ačkoliv každé zařízení hlásilo něco jiného, jednu složku všechny zprávy měly společnou – jednalo se o hlášení související s počítačovou sítí, v tomto případě sítí Masarykovy univerzity. Z různých pohledů a aspektů, které byly natolik roztříštěné, že zvažovat jeden jediný nemuselo dávat kdovíjak smysluplné či důležité informace.

2 SIEM – Security Information and Events Management

Zkrátka – ukazuje se, že mnoho šikovných zařízení má o provozu na síti co říci. Současně se zdá zřejmé, že různé informace mají různou prioritu. A že události, které na první pohled a s odstupem pár minut vypadají neškodně a bezzubě, se mohou v denním či týdenním přehledu objevit ve vší své zubaté žraločí kráse. Jeden z větších takových projektů, který se snažil obsáhnout a zjednodušit analýzu souvisejících událostí v počítačové síti byl ambiciozní produkt fy Cisco, *CS Mars* (*Cisco Security Monitoring, Analysis and Response System*). I přes odvážná tvrzení masivní obchodní kampaně se začaly ukazovat různé drobnosti, které nakonec vedly k tomu, že společnost Cisco celý projekt nedávno oficiálně ukončila.

Problém nebyl ani tak ve špatné základní myšlence, tedy centrální analýze a korelaci událostí, ale zejména v tom, že úvodní nastavení celého

produktu bylo natolik komplikované, že v rozsáhlých sítích v podstatě nemohlo dojít k jeho úspěšnému nasazení. Správci byli buď zahlceni zbytečnými událostmi nebo naopak ani nedostávali ty důležité – správné vyhodnocení toho, co pro danou síť důležité je a co není, nebylo a není triviální úlohou.

Jiný problém byl současně i v tom, že ne všechny upovídané technologie jsou od jediného dodavatele. A pokud se každý výrobce vcelku oprávněně rozhodne, že nad svými zařízeními umí dělat inteligentní dohled lépe, než jiní, nastává trochu jiná verze původního problému – sice už někdo data předžvýkal a zjemnil do grafické a koláčové podoby, ale stále každému z těchto systémů může chybět důležitý kousek skládačky.

A tak se objevil nový marketingový pojem, tzv. „Security Information a Events Management“, tedy správa bezpečnostních informací a událostí. Cílem je, krom prodeje nových produktů a nových krabiček, vylepšit výsledky síťových dohledových systémů. A to nejlépe tak, že se budou integrovat výsledky jedněch dohledů do dohledů jiných, nad tím vším se provede nějaká rozumná úvaha a půjde-li vše dobře, dojde k propojení různých událostí správným způsobem a zlotřilý program bude zakázán programem moudrým.

3 Síť bez hranic

Ačkoliv se jedná o další z termínů používaných firmou Cisco, lze i na myšlence Sítí bez hranic (Borderless Networks) demonstrovat další zajímavý posun toho, jak se chování uživatelů v síti mění.

Dříve, bez existence mobilních zařízení, byla situace poměrně jednoduchá a přímočará. Pracovní počítač byl v práci, domácí spokojeně dlel doma. Navíc domácí počítače často nemusely mít ani připojení k internetu. Pracovní síť tak mohla být uzavřeným jezírkem – zlé věci se děly venku a bylo třeba správně kontrolovat přítoky, aby štiky nevpadly dovnitř.

Notebooky, bezdrátové sítě a chytré mobilní telefony přinesly do poklidných firemních rybníčků hejna dravých ryb. Podnikové sítě se tak stávají mnohem zranitelnějšími, neboť notebook, pečlivě chráněný před internetovým Zlem, se přenesením do kaváren, letištních sítí či sítí univerzit stává terčem nemalých zkoušek. A chytré mobilní telefony? Ty klid snad ani nezažily. Neodolají-li svodům vnějšího světa, jsou po připojení zpět do podnikové sítě zdrojem nenápadné interní nákazy.

Aby však bylo možné chránit i součásti sítí, které jsou velmi mobilní, bylo potřeba část centralizované inteligence schopné rozpoznat útoky přenést i na počítače a mobilní telefony. A s každým takovým zařízením přibývá pochopitelně i možných hlášení toho, co se jim děje za příkoří.

Jeden ze způsobů, kterak kontrolovat bezpečnost koncových stanic a alespoň trochu zmenšit množství generovaných informací, se skrývá pod jménem *Unified Access Control*. Celé řešení umožňuje kontroly připojovaných koncových bodů, např. aktualizace operačních systémů a antivirových programů, a to tak, aby v případě problémů mohly co nejrychleji, tedy automaticky, zareagovat například firewally a umístit takový stroj do karantény. Zajímavá na UAC není ani tak myšlenka spolupráce všech důležitých prvků a zařízení různých výrobců, ale skutečnost, že se tak autoři pokusili učinit prostřednictvím protokolu IF-MAP (*Interface for the Metadata Access Point*). Neboť jde o protokol otevřený, existují v současné době i volně dostupné implementace jeho serverové části.

4 Firewally nové generace

S rozvojem sítí, jejich rychlostí, schopností a provázaností, se objevily i nové typy poskytování služeb.

Problém cestujících uživatelů nutil k zamyšlení i v jiném ohledu – když já jsem v Austrálii, kolega v Kolumbii a servery máme pouze na Jižní Moravě… Je to optimální? Například služby firmy Google jsou rozdistribuované po celém světě tak, aby si každý mohl najít „svůj nejbližší Google“. Tím se jednak zmenšuje zátěž tranzitních sítí, a jednak zlepšuje uživatelský zážitek z takové služby.

Umíte si však představit administrátora, jenž je postaven před úkol zabránit škodlivým serverům, aby traumatizovaly uživatele firemních notebooků? Pokud by chtěl povolit přístup na stránky Masarykovy univerzity či IS MU, má úkol v podstatě snadný, tyto servery opravdu na Jižní Moravě sídlí. Jenže co ostatní služby, rozstřelené promyšleně po celém globu?

Dá se říci, že IP adresa jako identifikátor serveru a související služby již nemusí dostačovat. Uživatelé totiž zpravidla chtějí „povolit Facebook“, „videa z Youtube“, případně si „pokecat na ICQ“. IP adresy pro ně nejsou důležité, důležitější jsou služby, které vyžadují.

A tak nezbylo, než vymyslet nový koncept zařízení, tentokrát z analytické společnosti Gartner, označovaných termínem „Next Generation Firewalls“. Jejich úkolem je usnadnit administrátorům orientaci v existujících službách, zkoumat důležité kousky provozu a následně zkusit odhadnout, o jaké služby se vlastně jedná. A buď je včas povolit, nebo zakázat.

„Chci používat P2P sítě typu XYZ“, „Potřebuji, aby mi fungovala videokonference a hlasové hovory“, „Což takhle ochránit náš SQL server před škodlivými dotazy?“. To je zhruba cíl toho, co by zkratka NGFW měla v budoucnu dokázat. S maximálními možnými rychlostmi a co nejvyšším uživatelským komfortem. V některých navrhovaných variantách se prý uvažuje i o tom, že by před povolením služby vyplňovali uživatelé dotazník, v němž by vysvětlili důvody pro povolení požadované služby a případně i spokojenost s nimi. Což opět může zrychlit procesy i evidenci existujících výjimek a umožňuje efektivně realizovat změny v pravidlech firewallů na základě zpětné vazby od uživatelů.

5 Kudy dál?

Zdá se tedy, že snahou výrobců bezpečnostních zařízení je umožnit uživatelům, aby používali své oblíbené služby bezpečně a současně správcům, aby ono bezpečí mohli zajistit v rámci nastavených firemních pravidel. S rozvojem nových konceptů a distribuovaných služeb se to i za cenu mírných změn pracovních postupů nejspíše daří. Nikoliv nějakými revolučními myšlenkami, ale spíš postupným vývojem těch existujících.

Jako u mnoha dalších oborů, i zde se ukazuje, že není problém vyrobit a vygenerovat vagóny dat, je problém v nich dostatečně rychle najít nejzajímavější informace pro konkrétní skupinu lidí. A v tom vidí budoucnost pravděpodobně i velké společnosti. Bezpečnost, vysokorychlostní sítě, distribuované aplikace a maximální mobilita uživatelů, to vše by mělo zajistit hladký chod aplikací a vznik nových myšlenek a konceptů.

Právě proto se na ÚVT MU testovalo nasazení SIEM nástrojů a uvažuje se o rozšíření projektu, v rámci kterého byla vyzkoušena a zdokonalena infrastruktura pro použití nástrojů unifikovaného řízení přístupu k síti. Kombinací těchto přístupů by bez omezování uživatelů mohlo dojít k výraznému posunu v obraně před nezvanými návštěvníky a snižování škod vzniklých nevhodnými programy.

Celé povídání by se dalo snad shrnout pod jediné slovo – spolupráce. Ať již mezi výrobci, jednotlivými zařízeními nebo správci a uživateli. Bez spolupráce na některé z těchto úrovní, nebo ideálně na všech, to zkrátka nejspíš nepůjde.

Literatura

[1] IF-MAP. Dostupné na `http://en.wikipedia.org/wiki/IF-MAP`.

[2] NGFW. Dostupné na `http://img1.custompublish.com/getfile.php/1434855.1861.sqqycbrdwq/Defining+the+Next-Generation+Firewall.pdf` □