Bezpečnostní software a podniková bezpečnost

JAN VACLAVÍK

Pojem bezpečnosti počítačových sítí a informačních technologií bývá v poslední době poměrně intenzivně skloňován. Této skutečnosti výrazně napomohla celá řad ne zcela příjemných situací, které se v poslední době objevily.

Za poslední rok jsme zaznamenali nebývale vysoký počet útoků typu DDoS, cílené útoky na státní a bankovní instituce a celou řadu cílených útoků na soukromý podnikatelský sektor. To vše v rámci našeho regionu. Všechny tyto nepříjemné skutečnosti pomáhají pomyslně otevřít oči všem zúčastněným stranám, které si konečně začínají uvědomovat vážnost situace kolem zabezpečení počítačových systémů a sítí.

Predátor a jeho oběť

Podíváme-li se na problematiku z pohledu útočníka, který se rozhodl napadnout počítačovou síť své oběti, je znepokojující, že jeho situace je snadnější než kdy předtím. Takový útočník má na výběr celou řadu prostředků, vůči kterým může zacílit svůj útok, a získat tak přístup do chráněné části sítě. Tak jak stoupá počet zařízení připojených k síti, stoupá i počet potenciálních zranitelností. Běžný uživatel je dnes vybaven celou řadou zařízení, která používá ke své práci. Má běžně pracovní stanici, (nebo) notebook, k tomu už i tablet, alespoň jeden chytrý mobilní telefon s připojením k internetu i mobilní datové síti. Velmi často si ke korporátní počítačové síti připojuje své soukromé zařízení, které je zcela mimo kontrolu.

Jedno je však jisté. Různými bezpečnostními zranitelnostmi trpí všechna tato zařízení. Je jedno, jaký operační systém na nich běží, nebo jakou architekturu používají. Řada laiků i odborníků žije v omylu, když předpokládá, že aktualizací operačních systémů a používaných aplikací takovým útokům efektivně zamezuje. Není to pravda. Záplata vychází až s poměrně velkým časovým zpožděním, od identifikace dané zranitelnosti útočníkem. Navíc některé systémy už aktualizovat ani nelze, např. kvůli ukončené podpoře, a i přes to je uživatelé stále používají. Šikovný útočník dokáže využít těchto slabin operačních systémů nebo aplikací pro získání neautorizovaného přístupu.

Komplexní přístup

Na bezpečnost je potřeba dívat se jako na komplexní problém. Zajistit stoprocentní ochranu zabezpečované sítě prakticky ani teoreticky nelze, je však povinností každé odpovědné osoby, udělat maximum pro přiblížení se k této úrovni.

Off-net policy

Základem zabezpečení pracovní stanice, notebooku, tabletu nebo jiného mobilního zařízení je jednoznačně instalovaný bezpečnostní software. Na trhu jich existuje velké množství. Některé jsou zdarma, jiné placené, stačí si vybrat. Jeden výrobce nabízí antivirové funkce, další přidává personální firewall atd. Skutečně kvalitní a v praxi dobře použitelný produkt poznáte podle toho, jak je integrován do dalších celků zabezpečení sítě. Dnes se velmi prosazuje myšlenka tzv. off-net policy, která se skládá ze dvou částí. První tvoří softwarový klient pro pracovní stanici, notebook či chytré mobilní zařízení. Klientský software zastává funkci antiviru, firewallu, kategorizátoru webových stránek a nástroje pro kontrolu používaných aplikací. Druhou část tvoří prvek pro centrální správu většího počtu instalací – tzn. nástroj pro definování bezpečnostní politiky. A vzhledem k tomu, že je zde shoda s rolí UTM-NG firewallu, někteří výrobci tyto funkce integrují do takovýchto zařízení.

Elegantní na celé věci je, jak celá záležitost pracuje: Pokud sedí uživatel „za“ firewallem, tedy připojený uvnitř korporátní sítě, je jeho komunikace chráněna zejména perimetrovým firewallem. Odpojí-li však svoje zařízení a odnese ho mimo dosah chráněné korporátní konektivity, automaticky se nastartují bezpečnostní funkce v instalovaném softwaru, který svou konfiguraci převzal na základě již zmiňované centrální správy. Máme tedy zajištěnu prakticky stejnou míru zabezpečení takto chráněného pracovního nástroje. Bezpečnostní politika je tedy definována v jednom místě a všechna takto chráněná zařízení ji používají.

Stoupáme éterem

Když budeme logicky přistupovat dále od uživatele, narazíme na bezdrátový přístupový bod nebo bezdrátovou síť, případně na síťový přepínač. Řada bezdrátových sítí je v korporacích stavěna na izolovaných přístupových bodech, jejichž konfigurace je velmi obtížná a uživatelský komfort není uspokojivý. V případě bezpečnostních incidentů často dochází k výpadku některých přístupových bodů. Takové problémy se pak velmi složitě hledají a napravují. Síť tohoto druhu má kromě bezpečnostních potíží i mnohdy potíže existencionální, zkrátka nefunguje dobře nebo někdy ani vůbec. Mnohem elegantnějším řešením je zvolit bezdrátovou síť založenou na centrálním mozku (kontroléru) a jednoduchých přístupových bodech. Kontrolér se pak automaticky stará o co nejlepší chod bezdrátové sítě jako celku. V případě bezpečnostního incidentu disponuje kontrolér větší skupinou dálkově řízených přístupových bodů, které dokáží útočníka zahlušit tak, aby ve své nekalé činnosti nemohl pokračovat. Takováto síť má obrovský přínos jak z pohledu bezpečnosti, tak i z pohledu uživatelského komfortu, který nabízí. Navíc se dá využít pro celou řadu dalších funkcí, jako je například přístup pro hosty, zaměřování bezdrátových klientů atp.

Přepínače – jak je to špatně a jak dobře

I na tak zdánlivě jednoduchý prvek, jakým je síťový přepínač (switch), jsou kladeny z pohledu bezpečnosti obrovské nároky. Ne každý výrobce je však dokáže naplnit, ne každý zákazník ví o tom, že by je měl naprosto bez kompromisů vyžadovat. Každá ethernetová zásuvka je pro útočníka potenciálním přístupovým bodem. Je tedy naprosto nezbytné používat takové inteligentní síťové přepínače, které dokáží na principu certifikátu nebo jiné formy ověření rozlišit důvěryhodného uživatele od potenciálního útočníka.

Často se setkáváme s konfigurací switche rozdělenou na logické celky, kde je každý celek vyveden pomocí rozvodů do jiných částí prostor společnosti. Jinou konfiguraci mají porty v technickém oddělení, jinou na recepci, jinou v zasedacích místnostech,

atp. Každý takový logický celek má jinou konfiguraci z pohledu přístupových oprávnění, jakou ethernetovou zásuvku použiju, taková bezpečnostní politika se aplikuje na mou komunikaci. Toto je však špatně. Konfigurace ethernetových zásuvek nemůže být vázána na to, kde je daná zásuvka fyzicky umístěna, ale na to, kdo se k ní připojí a jakým způsobem se ověří.

Firewally

Dalším krokem v řetězci bezpečnosti je firewall. Firewall je velmi komplexní zařízení, existují různé druhy firewallů, jejich popis je však nad rámec tohoto článku. Pokusíme se jenom stručně představit, jaké funkce mají moderní a prakticky velmi účinné a efektivní firewally implementovány.

Postupně jsme si zvykli, že firewall dokáže oddělit běžnou a neškodnou komunikaci od té škodlivé na základě signaturového popisu. Podobným způsobem dokáže odhalit i škodlivý kód. Firewall rozumí webovým stránkám, odhalí, do jaké kategorie patří, dokáže filtrovat, co můžeme a nemůžeme na internetu vidět. Svou bezpečnostní politiku dokáže uplatňovat nejen na IP adresy nebo jejich množiny, ale i na uživatele či skupiny uživatelů v režimu single sign on. Moderní firewall však musí umět něco více. Mezi nově implementované funkce v takto vyspělých zařízeních patří například možnost aplikovat bezpečnostní politiku na určitá zařízení podle jejich druhu. Znamená to tedy, že komunikace z osobního počítače s operačním systémem MS Windows bude podléhat zcela jiným pravidlům a přístupovým listům (ACL) než komunikace z mobilního telefonu či tabletu, který je připojen do stejného segmentu sítě pomocí technologie Wi-Fi.

Obrovský pokrok zaznamenávají moderní firewally s bojem proti malwaru, kde běžné signatury již přestávají stíhat rychle se zvyšující počty nových a nových vzorků škodlivého kódu. Velmi efektivním řešením je tzv. sandboxing. Technicky jde o dramatické vylepšení dříve dobře známé heuristické analýzy, která provádí tzv. statickou analýzu spustitelného kódu, která dnes již není dostatečná. Metoda sandboxingu pracuje naopak s dynamickou analýzou spustitelného kódu, a to zjednodušeně řečeno tak, že daný kód opravdu spustí v izolovaném prostředí (tzv. sandboxu) a sleduje, co se děje. Sleduje, co daný kód provádí, kam zapisuje na disk, jaká data modifikuje v registrech, kterým směrem do počítačové sítě se pokouší komunikovat. Na základě těchto a dalších pozorování se po čase stanoví skóre, které se propojí s kontrolním součtem daného kódu, a tato informace se spolu s výsledkem analýzy „sdílí“ v celé síti. Takto se velmi snadno buduje živá databáze dosud neodhalených vzorků škodlivého kódu.

Další rolí vyspělých firewallů je práce s reputačním skóre každého uživatele. Každá činnost, kterou daný uživatel provádí je podle své rizikovosti klasifikována počtem bodů. Komunikace s firemním CRM systémem je velmi běžná, nemá žádné „trestné“ body. Komunikace s nějakou exotickou krajinou je však podezřelá, proto je hodnocena určitým počtem trestných bodů. Vše se kumuluje z klouzavých průměrů a výsledkem je poměrně jasná představa o podezřelosti chování daného uživatele, resp. jeho počítače.

Inteligentní analyzátory

Dalším krokem bývá často implementace inteligentních analyzátorů síťového provozu. Jde o technologie, které se instalují neinvazivně do sítě ve formě sond na různých místech. Taková sonda pak odposlouchává síťový provoz pomocí zrcadlení komunikace na síťových přepínačích a posbíraná data přeposílá na tzv. kolektor, který informace ze všech sond vyhodnocuje. Kolektor má tedy přístup k síťové komunikaci ze všech dohledovaných sítí, vidí odchozí i příchozí datový provoz z internetu a i vnitřní komunikaci mezi uživateli a servery. Jednou z nejzajímavějších funkcí kolektoru je tzv. NBA – Network Behaviour Anomaly, nebo také ADS – Anomaly Detection System. To je mechanizmus založený na pokročilých algoritmech a strojovém učení, který se dokáže naučit „běžný“ charakter komunikace v celé síti, ale i pro každý aktivní prvek zvlášť. Po určité době, během které se tento komplikovaný systém učí, získá detailní znalosti o chování sítě. Má tedy jasný přehled, který uživatel se kterým serverem běžně komunikuje, který počítač obvykle přistupuje a kam, který server obvykle generuje jakou sítovou komunikaci, jakou službu server hostuje atd. Pokud se v síti náhle objeví nějaká komunikace, která není běžná, vybočuje z naučených vzorců chování, systém na to dokáže upozornit. Příčinou takové změny v komunikačních způsobech bývá například nový škodlivý kód, jehož charakteristika dosud ještě nebyla stanovena. Nebo nový druh malwaru, který nedokáže odhalit ani dedikovaný nástroj založený na rozpoznávání signatur takového kódu. Nástroj ADS dokáže reagovat i na naprosto neznámý škodlivý kód. Kromě této funkce může být ADS použit i pro validaci bezpečností politiky v síti nebo dokáže upozornit na chybnou konfiguraci pracovních stanic nebo serverů.

Kdy a jak se chránit proti zahlcení

Často se zejména u větších zákazníků otevírá otázka nástroje na ochranu proti útokům typu DoS/DDoS. Zde se setkáváme celkem často s celou řadou mýtů a polopravd. Účinné řešení, které v pravou chvíli dokáže filtrovat validní komunikaci běžných uživatelů od komunikace inicializované útočníkem pocházející z velkého botnetu, existuje. Je však potřeba pomyslet na to, zda konektivita k internetu je dostatečná z pohledu šířky pásma. Takovéto řešení nemá smysl instalovat u zákazníka, jehož uplink je v řádu desítek megabitů za sekundu. Má však smysl, pokud se konektivita do internetu pohybuje v řádu stovek megabitů nebo jednotek gigabitu. Samozřejmě existují i zařízení, která mají ještě o řád větší výkonnost, ta však zpravidla poptávají poskytovatelé internetové konektivity a nabízejí je jako sdílenou službu pro své zákazníky.

Bezpečnost je kontinuální proces

V tomto výčtu by se dalo ještě dlouhou dobu pokračovat, implementace bezpečnosti vlastně nikdy nekončí, vždy je co zlepšovat, rozšiřovat a lze se více přibližovat oné magické stoprocentní ochraně. Každopádně je nezbytné se na problematiku dívat jak s nadhledem, tak i komplexně, jít do detailů a přemýšlet nad nimi. Trh nám však dává k dispozici úžasné nástroje, proč je tedy nevyužít.

Bezpečnost jako příležitost

- u každého zákazníka lze z pohledu bezpečnosti stále co zlepšovat;
- problematiku bezpečnosti informačních systémů a počítačových sítí dnes řeší všechny organizace, nezávisle na předmětu podnikání či velikosti;
- pro technicky orientovaného člověka je problematika bezpečnosti IT doslova výzvou;
- po obchodní stránce jde o komoditu s velkou marží, prodejem dalších služeb a servisních smluv.

Jan Vaclavík pracuje jako vedoucí oddělení předprodejní podpory ve společnosti Veracomp