

Útoky hackerov sú čoraz rafinovanejšie. Každodenne sa o tom presvedčajú spoločnosti všetkých veľkostí, ktorým hackeri nabúravaju webové stránky, rozširujú nepravdivé informácie, alebo sa dostávajú k citlivým údajom o spoločnosti, ich zamestnancoch alebo zákazníkoch. Takéto zásahy majú za následok nielen poškodenie mena spoločnosti, ale aj obrovské finančné straty. O tom, aké možnosti obrany pred elektronickými útokmi majú organizácie, hovoríme s obchodným riaditeľom spoločnosti Cisco pre verejný sektor a veľké podniky Františkom BARANCOM.



Inteligentná sieť sa vie ochrániť sama



Akým typom elektronických útokov dnes najčastejšie musia čeliť organizácie?

Ich povaha sa rýchlo mení. Ak sa v minulosti vírusy, s ktorými si ľudia najčastejšie spájajú tento typ útokov, šírili prevažne cez infikované súbory na disketách, v posledných rokoch sa bojisko prenieslo na pole internetu. Zmenil sa aj charakter útokov. Kedysi obávané vírusy predstavujú tú najprimitívnejšiu formu, avšak škody nimi spôsobené majú z finančného hľadiska pre organizácie celosvetovo najväčší dopad. Medzičasom sa objavili ešte oveľa účinnejšie, škodlivejšie a ťažšie odhaliteľné spôsoby, ako infikovať počítač. Trójske kone, červy, hijacky, spyware či keyloggery sú len niektoré z nich. Ani tie však už v súčasnosti nepredstavujú absolútnu špičku elektronických útokov.

Čo teda predstavuje najväčšie nebezpečenstvo?

V prvom rade si treba uvedomiť, že škodlivé kódy spravidla už nie sú výtvarom jedinca, ale na ich vývoji sa podieľajú celé skupiny hackerov. Objavili sa dokonca aj prípady, keď legálne firmy financovali vývoj škodlivých kódov, aby ohrozili konkurenciu. Je to dôsledok toho, že zabezpečenie informačných systémov je oproti minulým rokom na oveľa vyššej úrovni a ich prelomenie nie je také jednoduché. Triviálne vírusy takmer úplne vymizli, zato ostatné typy útokov sú neporovnateľne sofistikovanejšie. Výsledok práce hackerských skupín je zväčša verejne dostupný na internete a ktokoľvek si môže návod na atak stiahnuť a použiť.

Na čo by si mali organizácie dávať najväčší pozor?

Bezpečnosť je veľmi komplexná oblasť, preto aj organizácie by sa mali na ňu pozerat komplexne, nestačí používanie jedného nástroja. (Aj v automobile sa základná bezpečnosť pomocou bezpečnostných pásov doplní airbagmi a zložitou elektronikou.) My ponúkame ucelený systém na riešenie bezpečnosti – systém na ochranu koncových zariadení, siete, aplikačnú bezpečnosť, bezpečnosť obsahu a samozrejme systémy na manažment bezpečnosti. V každej z týchto oblastí ponúkame niekoľko použiteľných nástrojov, ktoré navzájom spolupracujú. Veľkú časť hrozieb tvoria vírusy prichádzajúce z internetu, niekedy vedú paralyzovať aj veľké organizácie. Veľa útokov sa realizuje aj cez spam, čiže nevyžiadajú elektronickú komunikáciu. Spam sám osebe ešte nemusí byť nebezpečný. Jeho škodlivosť spočíva v tom, že pri cieľených útokoch zaberá značnú šírku pásma a obmedzuje tak prevádzku v sieti, nehovoriac o tom, že obťažuje používateľov. Spam však môže byť i nositeľom alebo sprostredkovateľom škodlivých kódov, keďže do neho možno zabaliť odkazy na nebezpečné stránky. Keď sa používateľ nechá zlákať a klikne na takúto stránku, v prípade že nemá dostatočne zabezpečený počítač, riskuje jeho infikovanie napríklad keyloggerom, ktorý monitoruje stláčanie kláves. Na základe toho potom hackeri môžu získať prístupové heslo k jeho bankovému kontu.

Aké ďalšie hrozby číhajú na internete?

Veľmi „oblúbenou“ metódou je aj tzv. phishing. To je metóda, kedy hackeri používateľovi napríklad cez spam podvrhnú odkaz na falošnú webo-

vú stránku, ktorá vyzerá identicky ako originálna stránka nejakej inštitúcie. Predstavte si situáciu, že vám príde e-mail s oznámením, že vaša banka v rámci zvýšenia bezpečnosti začala používať novú verziu internet bankingu, ktorú si aktivujete vyplnením prístupových údajov a ich spätnom odoslaní. Neverili by ste, koľko ľudí dokáže na tento trik naletieť a dobrovoľne zverejniť prihlasovacie meno a heslo. Napríklad pri sťahovaní populárneho obsahu z internetu sa na pozadí tejto aktivity môže uskutočňovať inštalácia červa alebo vírusu do vášho počítača.

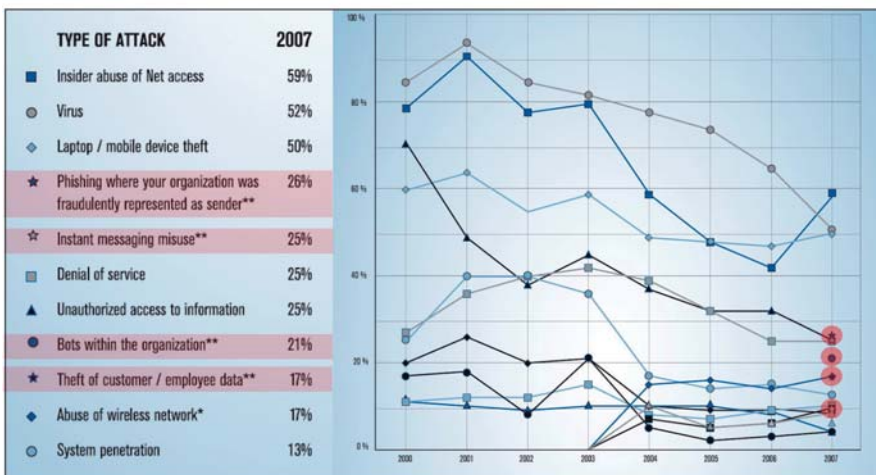
To sú však útoky, ktorých cieľom sú jednotlivci, resp. koncové stanice. Bývajú terčom útokov aj organizácie, ich siete a informačné systémy?

Samozrejme. Jednou z najčastejších metód sú tzv. Denial of Service (DoS) útoky, alebo ich nebezpečnejšia forma Distributed Denial of Service (DDoS). Pod týmto názvom sa skrývajú útoky, pri ktorých hackeri zvonka atakujú servery nejakej organizácie obrovským množstvom legitímnych požiadaviek s cieľom zahltiť ich a vyradiť z prevádzky. Pre spoločnosti, ktoré sú závislé od internetových služieb, výpadok servera, resp. obmedzenie jeho prevádzky prináša značné ekonomické straty, nehovoriac o naštrení ich dôveryhodnosti. Zákazníka nezaujímajú dôvody, prečo nefunguje internetový obchod s knihami, internetbanking, alebo on-line sťahovanie súborov.

Ako prebieha takýto útok?

Tento typ útokov sa pripravuje vopred, pričom v prípade DDoS sa do nich zapája obrovské množ-

The Evolving Security Challenge: Emergence of New Attack Types



Source: 2007 CSI Survey

stvo počítačov. Hackeri rozpošľú malý vírus alebo trójskeho koňa, ktorým sa nainfikujú milióny počítačov. Škodlivý kód prežíva v infikovaných počítačoch v pasívnej skrytej forme. V istom časovom okamžiku sa aktivuje a všetky nakazené počítače začnú naraz, automaticky a bez vedomia používateľa vysielajú požiadavky na server, ktorý je cieľom útoku. Ide pritom o legítimné požiadavky, napríklad príkaz na otvorenie domovskej stránky. Keďže je ich však veľmi veľa, server ich nie je schopný spracovať. Otvorenie internetovej stránky je normálna aktivita, ale keď sa o to v jednej sekunde niekto pokúsi miliónkrát, môže to byť jedine snaha o obmedzenie prevádzky servera. Práve preto, že ide o legítimné požiadavky, bežné ochranné prostriedky nedokážu takýto útok odhaliť a teda ani eliminovať.

Akým spôsobom sa organizácie môžu brániť?

Cisco je jediná firma na svete, ktorá dokáže zastaviť DoS a DDoS útoky skôr, ako spôsobia škodu. Máme technické prostriedky, ktoré umožňujú odhaliť a odfiltrovať škodlivé toky dát z internetovej prevádzky. Na základe on-line analýzy množstva parametrov dátového toku vieme rozoznať, či ide o útok alebo nie. Je to výsledok dlhodobého výskumu, na ktorý Cisco vynakladá viac ako štyri miliardy dolárov ročne. Relatívne najväčšiu časť z tejto sumy dávame práve na oblasť bezpečnosti. Vyradíme informačné systémy z prevádzky hackerským útokom je totiž stále pomerne časté.

Časté?

Áno, lebo šírenie škodlivých kódov sa vďaka rozvoju internetu a sietí zrýchľuje. Kým ešte pred dvadsiatimi rokmi objavenie sa nového vírusu a jeho rozšírenie trvalo týždne, dnes sú to minúty alebo sekundy. Okrem toho existuje množstvo ďalších nástrojov na napadnutie informačných systémov. Navyše, ak dnes niekto chce byť hackerom, nepotrebuje na to ani žiadne extra znalosti. Na internete nájde podrobné návody, ako sa nabúrať do systémov. Ak do vyhľadávacieho zariadenia zadáte reťazec slov „How to hack“, ponúkne vám vyše 31 miliónov odkazov. Útoky sa pritom presúvajú z počítačov už aj na iné koncové zariadenia – inteligentné telefóny a PDA prístroje. Takmer s každou novou verziou operačného systému pre iPhone sa prakticky súčasne na internete objavujú aj návody, ako obísť jeho ochranné nastavenia, aby sa dal používať i v sieťach iných operátorov.

Dá sa voči tomu vôbec brániť?

Cisco pristupuje k riešeniu bezpečnosti informačných systémov z dvoch základných pozícií. Tou prvou je stratégia „Network as the platform“. Keďže sieťová infraštruktúra dnes spája všetky typy infokomunikačných zariadení, snažíme sa práve do nej zakomponovať čo najviac inteligentných prvkov. Vďaka tomu, že sieť je spoločnou platformou pre počítače, tlačiarne, notebooky aj telefóny, je zároveň ideálnym kanálom, pomocou ktorého si organizácie môžu vynucovať uplatňovanie bezpečnostných pravidiel. Prístup a právomoci jednotlivých skupín používateľov nemusia implementovať do stoviek alebo tisícov koncových zariadení, ale môžu ich presadzovať cez sieť. Zároveň majú pod kontrolou, že všetky zariadenia v podnikovej sieti sú zabezpečené.

Ako to myslíte?

Môžem to vysvetliť na technológii Network Admission Control, ktorú možno prevádzkovať na

inteligentných sieťach. Ide o súbor nástrojov pre kontrolu a riadenie prístupov do firemnej siete, ktoré vyvinula spoločnosť Cisco. Prostredníctvom tejto technológie možno nastaviť, kto a za akých podmienok sa môže pripojiť k sieti. Totiž každé nezabezpečené zariadenie v sieti je potenciálnym zdrojom infiltrácie, tzn. napadnutia celej siete. Ak zamestnanec nemá vo svojom notebooku nainštalovanú napríklad najnovšiu verziu antivírovej ochrany a pripája sa, sieť mu neumožní prihlásiť sa do nej, resp. len v obmedzenej miere, aby si mohol stiahnuť a doinštalovať potrebné aktualizácie. Sieť si takýmto spôsobom dokáže vynútiť, aby každé jedno pripojené zariadenie bolo zabezpečené. Network Admission Control je veľmi silný nástroj nielen na zvyšovanie bezpečnosti, ale aj na vynucovanie si firemnej politiky. Pomocou neho si spoločnosť môže vynucovať správanie svojich dodávateľov, partnerských organizácií. Môže nastavovať obchodné pravidlá vnútri organizácie – napríklad nútiť zamestnancov vykonať školenia, testy, prečítať si dôležitý oznam a podobne. Takto sa bezpečnostné technológie začali využívať na business procesy.

Nákazu možno dostať do organizácie aj na CD. Dokáže sa inteligentná sieť ochrániť aj pre útokmi zvnútra?

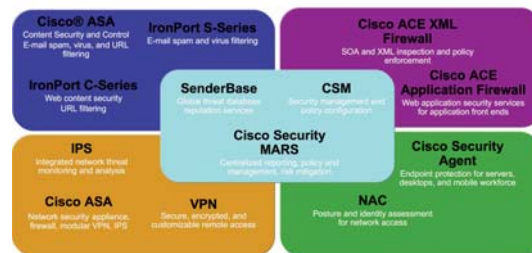
Jedným z bezpečnostných komponentov, ktorý to dokáže, je Cisco Security Agent (CSA). Je to niečo podobné ako antivírusový program, funguje však na odlišnom princípe. Kým antivírus vyhledáva a zachytáva škodlivé kódy na základe porovnávania špecifických reťazcov dát, tzv. signatúr, CSA si všima správanie počítača a reaguje na odlišnosti od normálneho stavu. Ak sa počítač alebo skupina počítačov pokúsi vykonať aktivitu, ktorá nie je uložená v profile, CSA to považuje za odchýlku od štandardu správania. Upozorní na ňu, alebo ju rovno odmietne uskutočniť. Ako anomáliu možno nastaviť aj zasunutie flash disku do USB portu alebo CD do mechaniky. Škodlivý kód sa tak potom nemá šancu cez tieto médiá dostať do počítača a siete. Pomocou CSA môžeme zabrániť aj vyneseniu citlivých dát z organizácie. Stačí len zadefinovať skupinu používateľov, ktorým chceme zakázať kopírovať dáta na flash disky, alebo ich napalovať na optické nosiče. Systém im to nielenže neumožní, ale zároveň zaznamená pokus o zakázanú aktivitu a oznámi to do centrálného Security manažmentu.

Cisco Security Agent vie odhaliť aj vírusy a iné škodlivé kódy?

Nevie ich detegovať, na to napokon ani nie je určený, ale môže zabrániť tomu, aby spôsobili škodu. Ak v profile zakážeme meniť konfiguračné súbory, formátovať disky alebo vymazávať určité typy dát, aj keď sa škodlivý kód aktivuje a pokúsi sa tieto činnosti vykonať, nepodarí sa mu to, lebo CSA to jednoducho neumožní. Obrovskou výhodou tohto nástroja je, že potrebuje oveľa menej systémových prostriedkov ako antivírusový program. Okrem toho všetky pokusy o nepovolené aktivity zaznamenáva. Najnovšia verzia CSA už dokonca umožňuje označovať citlivé typy dát a sledovať ich putovanie po sieti, alebo kopírovanie. Výrazne to zjednodušuje dokazovanie prípadných bezpečnostných incidentov.

Spomínali ste, že Cisco uplatňuje v oblasti bezpečnosti dve stratégie. Prvou je riadenie prístupu do siete a jeho kontrola už na vstupe, čiže na porte. Ktorá je tá druhá?

Changing the Game: End-to-End IT Security Solution



Všetky sieťové komponenty, ktoré vyrábame, majú v sebe zabudované bezpečnostné prvky. Tieto komponenty však okrem toho spolu dokážu komunikovať a vymieňať si bezpečnostné informácie. Tento prístup označujeme ako Self Defending Network (SDN). Ide o iniciatívu, ktorá umožňuje budovať siete novej generácie. Čiže sieť sa stáva nástrojom na identifikáciu, prevenciu a obranu pred útokmi. Sieť, ktorá je inteligentná, má potom aj tendenciu sama sa chrániť.

Akým spôsobom sa dokáže sama ochrániť?

Tým, že sú do všetkých komponentov a bodov siete integrované bezpečnostné prvky, ktoré spolu vedú komunikovať a spolupracovať, sa takáto sieť dokáže „naučiť“ odolávať novým útokom. V sieťovej infraštruktúre sa nachádzajú dva typy sond – Intrusion Detection System a Intrusion Prevention System. Kým prvé zaznamenávajú podozrivé aktivity, druhé im dokážu aj brániť. Cez ne sa o nich dozvedia aj ostatné zariadenia v sieti. Práve naučia sa, že toto sú nebezpečné dáta a treba ich eliminovať.

Čo ešte okrem týchto riešení môže Cisco ponúknuť v oblasti bezpečnosti?

Prakticky všetko. Cisco má ako jedna z mála firiem na svete kompletné portfólio end-to-end bezpečnostných riešení. Pre zákazníka je to veľmi dôležité, pretože bezpečnosť sa nedá riešiť čiastočne, ale len systémovo. Sieť postavená na našich komponentoch obsahuje bezpečnostné prvky v každom bode komunikačného systému, či už sú to počítače, bezdrôtové zariadenia, prepínače, smerovače alebo riadiace systémy. Zaoberáme sa aj aplikačnou bezpečnosťou. Najnovšie sme začali poskytovať aj riešenia fyzickej ochrany, ako sú kamerové, dohľadové a monitorovacie systémy. Je to nová oblasť, ktorú dnes vieme začleniť do nášho komplexného riešenia. Nad všetkými komponentmi a aplikáciami vieme ponúkať bezpečnostné manažmenty, ktoré prácu s týmito zložitými bezpečnostnými riešeniami významne zjednodušujú.

Slovo na záver.....

Rád by som spomenul, že naša spoločnosť získala v máji tohto roku celosvetovo uznávaný certifikát od medzinárodnej organizácie pre počítačovú bezpečnosť Common Criteria pre celý rad technológií a zariadení ako sú smerovače a prepínače a operačný systém Cisco IOS IPsec pre podporu bezpečnosti. Tento certifikát dáva možnosti aj vládnym organizáciám použiť naše technológie pre zvýšenie bezpečnosti v komunikačných a informačných systémoch. Common Criteria certifikát je významným predpokladom pre lokálnu certifikáciu vládných inštitúcií, pre ktorých je bezpečnosť informácií kritickou požiadavkou. Certifikát je možné nájsť na stránke www.commoncriteriaportal.org