Zabezpečenie internetu: Cena len pre víťaza

Roger Halbheer je ako hlavný poradca v spoločnosti Microsoft pre bezpečnosť zodpovedný za sieť konzultantov v Európe, Afrike a na Blízkom východe. Sám často vystupuje ako poradca vrcholových manažérov a orgánov štátnej správy. V rámci tohtoročnej IDC IT Security Roadshow vystúpil v Bratislave so svojou prezentáciou.

V úvode vystúpenia pripomenul rozhovor s bezpečnostným riaditeľom jednej spoločnosti, ktorý chcel vedieť, kedy nebude treba investovať do bezpečnosti informačných technológií. „Moja odpoveď bola jasná: Môžete prestať investovať do IT bezpečnosti vtedy, keď sa odstráni cyber kriminalita, čo je v tomto momente v nedohľadne," povedal a zdôraznil, že nejde len o zneužívanie informačných systémov, ale najmä o ich rizikový manažment.

POUŽÍVATELIA CHCÚ VÄČŠIU FLEXIBILITU

Preto začal štyrmi faktami zo života, ktoré významne ovplyvňujú IT bezpečnosť. Prvým je, že používatelia žiadajú stále väčšiu flexibilitu. Je to preto, že ľudia potrebujú využívať informačné technológie čoraz flexibilnejšie. Ukázal to na svojom príklade. „Veľmi rád cestujem po regióne EMEA a striedam rôzne prostredia. Niekde som v priestoroch, kde mám veľmi dobrý prístup na internet, inde zasa nie je vôbec natiahnutý. Raz pracujem doma, druhý raz v hotelovej izbe či na letisku. Spájajú sa teda dve veci. Na jednej strane je to prostredie informačných technológií, na druhej strane je to človek, ktorý príde do práce, dostane počítač alebo laptop, internetový prístup a má možnosť dostať sa k veľmi dôležitým údajom. Pritom sa výrazne usilujeme znížiť počet pracovníkov, ktorých do určitej miery nahrádzame počítačovou prácou. Používa sa hardvér a prvou vecou je nadstaviť si počítač. Testujú sa všetky aplikácie. My sme možno v tom zruční, ale máte spoločnosti napríklad v ropnom priemysle, ako je BP, kde momentálne testujú, či môžu použiť pre zručných ľudí podobný on-line modul. Je to teda určité IT prostredie. Ak zamestnanec dokáže, že je schopný v IT prostredí sám fungovať, používať ho, dostáva väčšie peniaze. Keď sa tak stane, potom musí sám dávať pozor na IT prostredie. Výsledkom je zvýšená produktivita.

Na druhej strane dochádza k zmene spôsobu, ktorým sa musia riadiť IT riziká. Ďalej už totiž z pozície zodpovedného za bezpečnosť nekontrolujete konkrétne počítače. Na to sa používajú rôzne technológie na ochranu. V Microsofte to ide ruka v ruke so samotnou politikou spoločnosti. Na konci pracovného dňa je však mojou povinnosťou ako riaditeľa pre bezpečnosť pozrieť sa, čo všetko sa použilo," povedal.

BEZPEČNOSŤ A BIZNIS

Druhým faktom, ktorý ovplyvňuje život Rogera Halbheera, je otázka samotnej bezpečnosti. „Dlhé roky som pracoval ako konzultant v oblasti IT bezpečnosti. Najprv som sa stretával v spoločnostiach s tým, že mi bezpečnostní riaditelia vyčíslili všetky možné ohrozenia, ktorým musia čeliť. Nezabudli dodať, že na to, aby ich obmedzili, potrebujú peniaze, ktoré sa dostávajú ťažko. Ak to však otočíte a zoberiete IT bezpečnosť nielen z pohľadu peňazí, ale najmä z pohľadu riadenia, tak môže byť riešenie iné.

Sú rôzne projekty na využívanie siete, ale napokon je to vždy otázka prístupu spoločností. Často sa vyťahuje určitá časť služieb a outsourcuje sa. Tým sa však stráca kontrola nad dianím. Cítite sa možno lepšie, ale to na riešenie bezpečnosti IT nestačí, tak, ako nestačia len veľké firewally na konci siete. Pracoval som pre jednu veľkú banku, ktorej bezpečnostný riaditeľ mi povedal, že vymysleli nový model pre svojich IT ľudí. Bol vcelku zaujímavý. Zistili však, že architektúra je síce v pohode, ale nejde s požiadavkami biznisu. Samotné moduly boli super dobré, ale nekorešpondovali s úlohami banky," uviedol.

ZRANITEĽNOSŤ DÁT

Tretím faktom je otázka zraniteľnosti dát, ktorá zostáva. Zraniteľnosť sa musí znižovať. K tomu Roger Halbheer dodal: „Nemám rád, ak sa porovnávajú rovnocenné produkty s tým, že jedna

spoločnosť má s produktmi konkrétnej firmy dobré skúsenosti, ale druhá má zasa dobré skúsenosti s produktmi inej firmy, v oboch prípadoch je tu však problémom zraniteľnosť. Ak si ako výrobcovia bezpečnostných produktov zoberieme zraniteľnosť ako heslo, tak je to náš produkt a naša zraniteľnosť. Je to záležitosť obchodníkov. My s tým musíme pracovať, presvedčiť zákazníka, že vieme čeliť aj zraniteľnosti. Ťažko sa však dožijeme toho, že by sa niektoré riešenie dalo aplikovať plošne tak, aby úplne odstránilo zraniteľnosť. Je to preto, že ľudia jednoducho robia chyby. Je tu ľudský faktor. Navyše máme hackerov, ktorí nám sťažujú život. Nie sú hlúpi, vedia sa dostať do jednotlivých IT systémov. Aj preto otázka zraniteľnosti zostáva naďalej, ale musíme sa usilovať o to, aby sme si život zľahčovali."

Rada Európskej únie nedávno predstavila návrh, aby sa na celom svete začalo intenzívnejšie bojovať proti zneužívaniu internetu a počítačových technológií. Usiluje sa najmä o to, aby neboli rozdiely v nazeraní na nabúranie do systému, ktoré niekde kvalifikuje ako zločin, kým inde sa prinajmenšom toleruje. Na druhej strane by sa však podľa EÚ malo aj stanoviť, kedy a čo treba oznámiť vyšetrovacím orgánom. To by umožnilo znižovať tieto náklady.

HROZBOU JE CYBERCRIME

Štvrtým faktom života je cybercrime. „Predovšetkým o ňom je otázka bezpečnosti. Je veľmi významný prvok samotnej ekonomiky. Organizovaný zločin ide dnes cez internet. Veľakrát zjednodušujeme podmienky jeho pôsobenia. Všetko je to z viacerých dôvodov opäť o peniazoch," zdôraznil Roger Halbheer a priblížil výsledky štúdie o ekonomike zločinu, ktorú v roku 1995 vypracovali páni Clark a Davis. Netýka sa priamo cybercrime, lebo vtedy sa ešte takto nedefinoval, ale kriminality všeobecne. Podľa nich náklady na zločin nepredstavujú len zisky, ktoré svojím činom získa zločinec, ale tvorí ich aj ďalších päť častí. Bližšie sa pritom zastavil pri ďalších nákladoch, ktoré sa pri spáchaní zločinu vyskytnú. Na jednej strane sú to náklady, ktoré sa musia vynaložiť na ochranu siete a serverov. Na druhej strane niektoré spoločnosti po tom, čo zistia, že ich hacker nabúral, nejdú vždy na políciu. Musia však zo svojich zdrojov vykryť škodu, ktorú im napáchal, lebo nemôžu rátať s istou návratnosťou. Čo s tým? Rada Európskej únie nedávno predstavila návrh, aby sa na celom svete začalo intenzívnejšie bojovať proti zneužívaniu internetu a počítačových technológií. Usiluje sa najmä o to, aby neboli rozdiely v nazeraní na nabúranie do systému, ktoré niekde kvalifikuje ako zločin, kým inde sa prinajmenšom toleruje. Na druhej strane by sa však podľa EÚ malo aj stanoviť, kedy a čo treba oznámiť vyšetrovacím orgánom. To by umožnilo znižovať tieto náklady.

NEVYHNUTNOSŤ ŠIROKEJ SPOLUPRÁCE

Na záver si Roger Halbheer položil rečnícku otázku: Čo to znamená pre nás? Ihneď si na ňu aj odpovedal: „Microsoft dodáva bezpečnostné technológie. Musíme ich správne riešiť, spolu s vami zdieľať rozvojové procesy, pozrieť sa na to, aké požiadavky majú zákazníci z hľadiska bezpečnosti, ochrany a zvládnutia riadenia rizík. Potom možno pripraviť modely šité na mieru. Dôležité je však o najlepšej praxi ďalej informovať. Je to proces, ktorý treba niekde začať. Na to máme bezpečnostné programy, ktoré teraz nechcem nejako rozvádzať. Máme aj výskumné tímy a v priebehu jednej až dvoch hodín vieme vyprodukovať kritickú infraštruktúru. Využívajú sa však aj ďalšie formy, najmä spolupráca technologických firiem venovaná riešeniu konkrétneho problému. Treba si uvedomiť, že žiadny problém nezmizne za deň či dva, ale vždy to záleží od ľudí, ktorí sa na riešení podieľajú a usilujú sa, aby to bolo čo najskôr. Vieme teda poskytnúť technologické riešenia, aby sme sa zbavili týchto „zlých ľudí", ako ich nazývame. Je to však otázka veľmi dobrej spolupráce a spoločného úsilia dopracovať sa k výsledkom. Je to aj otázka kritickej infraštruktúry, ktorej ochrana je trochu iná než chrániť ľudí.

Som presvedčený, že správnym smerom sú partnerstvá. Nedávno sa stal jeden prípad. Došlo k napadnutiu jedného zákazníka. Nebol tam nik, kto by mohol pomôcť. Zákazník totiž mal strach s niekým hovoriť, bolo mu nepríjemné, že ho hacker napadol. Trvalo mu dva dni, než začal zapájať jednotlivých partnerov a predajcov. Keď zistili, aká kritická bola situácia, tak mu bolo ľúto, že nekonal skôr. Stratil však veľa času, keď sa dalo škody znížiť.

Dôvera musí byť nie medzi konkrétnou predávajúcou firmou a zákazníkom, ale medzi tvorcami riešení a aplikácií na jednej strane a ich využívateľmi na strane druhej. Nedávno som čítal, že bezpečnostný trh je mŕtvy, lebo je v závese za zločincami. Musí ich predbehnúť. Craig Mundie, Chief Research and Strategy Officer Microsoftu uverejnil článok Dôvera od jedného konca po druhý. Chcel by som, aby ste išli na Microsoft Comments a pozreli sa na Bielu knihu o dôvere od jedného konca po druhý, ktorú pripravil viceprezident Microsoftu Scott Charney. Oba dokumenty sa sústreďujú na hľadanie odpovedí na otázky: Prečo je dôvera na internete výzvou, Čo sú nové výzvy a Čo potrebujeme? V prvom prípade je výzvou to, že internet má isté vlastnosti, pre ktoré ho obľubujú kriminálnici. Je globálny, viac-menej anonymný, veľmi ťažko sa dajú vystopovať jedinci a má cenné ciele. Novou výzvou je, že útoky už nesmerujú ani tak na operačné systémy, lebo sú lepšie chránené, ale na aplikácie a užívateľov, pričom väčšina útokov je založená na určitej manipulácii s prirodzenými ľudskými vlastnosťami, ako je chamtivosť či zvedavosť. Preto, to, čo potrebujeme, je už spomínaný verejný dialóg o cybercrime, aby sme pochopili, aké sú vyhliadky pre najbližšiu budúcnosť štyroch-piatich rokov." ■

Spracoval Marián Babic