Bezpečnosť a bezpečnostná politika očami slovenských a českých expertov

Viac pozornosti správe informačného systému

■ Ako hodnotíte bezpečnostnú politiku a zabezpečenie informačných systémov v praxi? Kde sa robia najväčšie chyby a prehrešky? Je rozdiel v tomto smere medzi veľkými, stredne veľkými a malými firmami? Aké sú teda vaše skúsenosti? Ako by mal argumentovať bezpečnostný manažér, aby presvedčil vedenie firmy o potrebe investícií a ďalších systémových krokov v tejto oblasti? S takýmito otázkami sme sa na úvod besedy obrátili na niektorých slovenských a českých odborníkov na informačnú bezpečnosť.

MARTIN ZAJÍČEK

Ing. Josef ŠUSTR, vedúci bezpečnostných projektov v spoločnosti INFOSEC: - Najväčšou chybou je, že v porovnaní s technickými otázkami sa venuje malá pozornosť správe. To sa prejavuje v zlej konfigurácii firewallov, antivírusových systémov atď. Ďalšou chybou je, že sa bezpečnostné problémy riešia násilím, kampaňami. Napokon je zrejmá určitá netrpezlivosť. Niektorí vedúci si myslia, že sa od bodu blízkemu nule (povedzme skôr 10 %) dostanú do bodu 100 % za 3 až 6 mesiacov. To je nemožné. Nevidím rozdiel medzi veľkým a, povedzme, stredným podnikom. A čo poradiť bezpečnostným manažérom?

JOSEF ŠUSTR

Podľa môjho názoru prvou podmienkou ich úspechu je, keď si títo pracovníci uvedomia, že pracujú s nevedomými a chyby robiacimi ľuďmi, a nie so strojmi. Ďalšia dôležitá rada: autoritu si vybojujete tým, že budete užívateľom pomáhať, a nie ich trestať. A azda najdôležitejšou vlastnosťou bezpečnostného manažéra je trpezlivosť. Treba postupovať pomaly, nenechať sa otráviť. A v neposlednom rade ako presvedčiť vedenie? Trvalým prísunom pravdivých informácií prezentovaných zrozumiteľnou formou, vrátane porovnaní, ako to robia inde. Získanie týchto informácií a vybudovanie informačných kanálov smerom k vedeniu je základnou úlohou bezpečnostného manažéra.

Martin ZAJÍČEK, senior konzultant a manažér projektov v spoločnosť DCIT ČR: - Spoločnosti a najmä ich úseky IT si začínajú uvedomovať, že v tejto oblasti treba niečo robiť. Prevenciou možno obmedziť dôsledky prípadného incidentu. Otázka už nestojí tak, akou sme inštitúciou a aké dôverné dáta vlastníme. Súčasné útoky sa uskutočňujú automatizovane, bez ohľadu na to, či ide o banku alebo výrobcu nábytku. Takže správna otázka znie: ako sme zabezpečení voči aktuálnym hrozbám? Hoci pomaly, ale predsa cítiť postupný pozitívny posun v úrovni zabezpečenia a v samom myslení. Asi najzávažnejším prehreškom je ignorovanie tejto oblasti. Akákoľvek iniciatíva je pozitívna a už aj malými krokmi možno dosiahnuť jasný posun. Rozdielnosť riešenia tejto problematiky viac závisí od samotného manažmentu ako od veľkosti organizácie. Samozrejme, väčšie spoločnosti môžu mať lepšie možnosti získať finančné prostriedky. Hlavným menovateľom úspechu v tejto oblasti je však práve manažment.

Jozef VYSKOČ, certifikovaný audítor informačných systémov, spoločnosť VaF: - Prax ukazuje, že zabezpečenie IS trpí nedostatočným pochopením problému, ako aj prístupom, ktorý by som nazval alibistickým. Veľká pozornosť sa venuje tomu, aby sa v prípade bezpečnostného incidentu dala priradiť zodpovednosť konkrétnej osobe alebo osobám. Oveľa menšia pozornosť sa však venuje opatreniam, ktoré by sa orientovali na to, aby bezpečnostným incidentom zabránili, resp. aby zmenšili spôsobené škody. Netreba zabudnúť ani na veľmi časté vnímanie bezpečnosti IS ako čohosi, čo sa implicitne chápe ako výlučná vec útvaru informatiky. V dôsledku toho ostatní zamestnanci - používatelia IS, ani manažment organizácie nepociťujú potrebu väčšej angažovanosti, resp. zodpovednosti za náležitú úroveň bezpečnosti IS. Úlohu tu do značnej miery zohráva aj veľkosť firmy. Kým väčšie firmy sa váhavo, ale predsa samy zaujímajú o bezpečnosť, smerom k menším firmám je hlavným motívom na bezpečnostné opatrenia skôr legislatíva, ktorá ich k tomu núti. Významnú úlohu tu zohral predovšetkým zákon č. 428/2002 Z. z. o ochrane osobných údajov. Značným problémom je i to, že bezpečnosť sa u nás stále vníma predovšetkým ako ochrana citlivých údajov pred únikom. A keď majú zodpovední pracovníci pocit, že v ich IS sa také údaje nenachádzajú, resp. nie sú pre nikoho dostatočne zaujímavé, klesá aj ich záujem o zaistenie bezpečnosti IS. Je to dosť častý jav osobitne pre menšie firmy.

Marián SVETLÍK, vedúci Znaleckého ústavu Risk Analysis Consultants: - Podľa mňa sme sa už dostali do štádia, keď môžeme vyhlásiť, že naša spoločnosť je spoločnosťou informačnou. Neznamená to, že sme presýtení počítačovou technikou, ale to, že hodnoty spoločnosti sa výrazne presunuli z materiálnej podoby do podoby informácií. Ak sme sa desiatky a stovky rokov učili chrániť si materiálne hodnoty, ak si automaticky dávame pozor na peniaze a na doklady, s informáciami to nie je také samozrejmé. Tým prvým zo zásadných nedostatkov, ktoré v zabezpečení informácií vidím, je práve táto skutočnosť - ešte si málo uvedomujeme ich hodnotu, a tým sa stáva, že sa podľa toho k informáciám aj správame. Druhým zásadným nedostatkom je, že informácie, a tým aj ich bezpečnosť, spájame priamo a výhradne s počítačovou technikou. To ako keby sme v súvislosti s ochranou peňazí hovorili výhradne len o trezorových systémoch.

Najslabším článkom reťaze však je, napokon ako vždy, človek, ľudia. Až si skutočne, reálne uvedomíme hodnotu informácií, potom sa k nim budeme aj zodpovedajúcim spôsobom správať, potom si uvedomíme, že aj počítačová technika (ako jeden z článkov, ktorými sa informácie spracúvajú) potrebuje určitú mieru zabezpečenia, že to nie je len o výkone a peknej grafike, ale že najmä ľudia, ktorí s informáciami pracujú (aj pomocou počítačovej techniky), sa potrebujú naučiť elementárnym zručnostiam, povedal by som doslova reflexom, ktoré dajú predpoklady na to, aby sa informácie zodpovedajúcim spôsobom chránili.

■ Dozrel podľa vás čas na to, aby sa zabezpečenie informačných systémov dalo riešiť formou outsourcingu? Ak áno, čo je nevyhnutnou podmienkou, aby outsourcing bol úspešný a spokojné boli nakoniec obe strany – dodávateľ aj objednávateľ?

J. ŠUSTR: - Určite áno. V čiastkových technických otázkach, napríklad bezpečného pripojenia na internet, sa tak už roky robí. Samozrejme, možno ísť ďalej, ale má to svoje hranice. V každej organizácii vždy bude musieť existovať niekto, kto je schopný outsourcing riadiť, byť garantom záujmu spoločnosti, prenášať tieto záujmy do zmluvných vzťahov, definovať bezpečnostnú politiku, úlohy... Myslím tým na bezpečnostného manažéra. Bez tohto postu sa nedá dosť dobre obísť. Samozrejme, možno aj činnosť bezpečnostného manažéra outsourcovať, potom však inde, než sa outsourcuje výkonná informačná bezpečnosť. Neodporúčam to, je tu potrebná dokonalá znalosť miestneho prostredia, a to býva pre externého dodávateľa problém.

M. ZAJÍČEK: - Outsourcing a bezpečnosť? Určite je to alternatíva pre spoločnosti, ktoré si nemôžu dovoliť vlastného špecialistu/špecialistov v oblasti bezpečnosti. Sú oblasti, v ktorých je externá spolupráca efektívnejšia a prínosom pre spoločnosť je práve externista, prípadne ich pravidelné obmieňanie (penetračné testy, audity serverov, analýza rizík, tvorba BP, atď.). Úspešnosť, samozrejme, závisí od seriózności partnerov a presného definovania rozsahu, podmienok a podobne.

J. VYSKOČ: - Nevidím dôvod na odmietanie outsourcingu. Podobne, ako si väčšina organizácií neudržiava vlastný hasičský útvar či bezpečnostnú službu, nedá sa očakávať, že si môžu dovoliť jedného alebo viacerých kvalifikovaných špecialistov na informačnú bezpečnosť. Osobitne ak náklady na nich sa dosť ťažko odôvodňujú v čase, keď sa organizácia nezmieta v problémoch spôsobených bezpečnostnými incidentmi. Je totiž dosť ťažké rozlíšiť, či absenciu incidentov spôsobuje dobrá práca bezpečnostných špecialistov, alebo iba to, že momentálne organizácia, resp. jej systémy nikoho neupútali natoľko, aby sa o nejaký útok proti nej pokúsil.

Neustály tlak na šetrenie, resp. odôvodňovanie nákladov robí značne komplikovaným udržiavanie vlastného - hoci aj jednočlenného - útvaru špecializovaného na informačnú bezpečnosť. Nehovoriac o tom, že potenciálne potrebný rozsah špeciálnych znalostí (napríklad pre prípad riešenia bezpečnostných incidentov) skôr volá po celej skupine kvalifikovaných špecialistov. Ako to býva aj v prípade outsourcingu ostatných činností, nevyhnutnou podmienkou obojstrannej spokojnosti je dobre postavená zmluva. Väčšie prekážky outsourcingu v súčasnosti v tomto zmysle vidím práve v tom, že manažment organizácií zatiaľ nemá dosť dobrú, resp. realistickú predstavu o tom, čo sa vlastne dá „zaručiť" pri riešení bezpečnosti, ako aj v tom, ako vlastne „merať" odborné schopnosti poskytovateľa v tejto špeciálnej oblasti.

M. SVETLÍK: - Keď na jednej strane vidím, ako málo a najmä ako nesystémovo je zaistená informačná bezpečnosť, zdá sa mi až schizofrenické, keď sa okolo jej

MARIÁN SVETLÍK

outsourcingu chodí ako okolo horúcej kaše. Je až zarážajúce, že fyzickú bezpečnosť outsourcujeme už úplne prirodzene takmer automaticky a o outsourcingu informačnej bezpečnosti sa na druhej strane hovorí ako o tabu. Ak je pre organizáciu ekonomicky neefektívne zaisťovať takú relatívne jednoduchú záležitosť, akou je fyzická bezpečnosť, vlastnými zdrojmi, je čudné, že oveľa zložitejšiemu problému - outsourcingu informačnej bezpečnosti sa bráni a zabezpečuje si ju často neefektívne vlastnými silami. Vyplýva z toho jediné (a tu zovšeobecňujem, neplatí to prirodzene všade) - na informačnú bezpečnosť sa vynakladajú prostriedky neefektívne a nesystémovo, odčerpáva to sily organizácie. Informačná bezpečnosť totiž nie je len zabezpečenie počítačovej techniky na systémovej úrovni, je to o fyzickej bezpečnosti, o personálnej bezpečnosti a vzdelávaní, o organizácii a riadení a pod. Osobne si myslím, že pre organizácie je výhodnejšie špecifické činnosti outsourcovať. Som presvedčený, že sa môžu robiť kvalitnejšie a organizácia sa môže venovať len svojmu corebiznisu. Outsourcing informačnej bezpečnosti, ako každý iný outsourcing, je najmä otázkou ekonomickej efektívnosti. Prestaňme robiť z informačnej bezpečnosti tabu a správajme sa k nej ako k ostatným službám, o ktorých uvažujeme, či ich outsourcovať alebo nie. Myslím si, že celý problém outsourcingu informačnej bezpečnosti je umelo nafúknutá bublina a jeho podstata nezodpovedá reálnemu správaniu sa našich organizácií v tejto oblasti.

■ Externý audit – čo môže a čo nemôže poskytnúť? Aké môže dať záruky a aká je jeho zodpovednosť?

J. ŠUSTR: - Externý audit poskytuje nevyhnutné informácie pre vlastníkov spoločností. I keď sme v súčasnosti svedkami toho, že sa externí audítori zaoberajú aj pomerne podrobne procesmi a dokonca technickými záležitosťami na úrovni prevádzky informačných systémov, napriek tomu ich závery a odporúčania nemôžu slúžiť ako návod na konkrétne riešenia. To od nich ani nikto neočakáva. Dôležité je, že využívajú svoje bohaté skúsenosti a medzinárodné porovnávania a s nadhľadom môžu poukázať na nedostatky, ktoré si vyžadujú systémové rozhodnutia. A záruky? Kto môže poskytnúť záruky? Možno meno renomovanej firmy. Možno...

M. ZAJÍČEK: - Externý audit v každom prípade môže priniesť nezávislý pohľad audítora, nezaťaženého vzťahmi a procesmi v rámci auditovaného prostredia. Druhým významným hľadiskom môžu byť praktické skúsenosti z podobných projektov, špecializácia a praktická znalosť auditovanej problematiky. V niektorých momentoch však externý pohľad môže byť trošku povrchný v tom zmysle, že externý pracovník nie vždy dokáže úplne jasne odhaliť všetky vnútorné vzťahy a väzby. Je to, žiaľ, dôsledok obmedzených kapacít, ktoré sú na projekt určené a ktoré je klient ochotný zaplatiť. Zárukou sú podľa môjho názoru v oblasti bezpečnosti IS predovšetkým skúsenosti a čiastočne už aj štandardy a metodiky, ktoré sa postupne začínajú objavovať a používať. Žiaľ, zodpovednosť v tejto oblasti možno veľmi ťažko uchopiť. Oblasť tvorby informačných systémov sa pomaly dostáva už do polohy štandardizácie a samotná bezpečnosť je oblasťou ešte špecifickejšou.

J. VYSKOČ: - Stručná odpoveď - externý audit môže poskytnúť nezávislý pohľad, nezávislé zhodno-

JOZEF VYSKOČ

tenie stavu IS, koncepcie i aktuálneho stavu jeho bezpečnostných opatrení. Len ťažko môže poskytnúť detailné zhodnotenie, osobitne v prípade auditu celých rozsiahlych zložitých systémov (iná situácia môže byť v prípade ich dobre definovaných častí). Nemôže poskytnúť žiadne záruky - systém, ktorý bol v čase návštevy audítora nastavený a prevádzkoval sa úplne v zmysle vypracovaného bezpečnostného projektu, zodpovedajúceho najnovším poznatkom z informačnej bezpečnosti, môže byť deň po skončení auditu v úplne inom, z hľadiska bezpečnosti dokonca žalostnom stave, a to audítor nemôže ovplyvniť, ani za to zodpovedať.

Týmto nechcem povedať, že som proti externým auditom - určite majú svoje opodstatnenie a nakoniec sám ich aj vykonávam. Treba si len uvedomiť, aké sú ich možnosti. Externý audítor „vidí" len to, čo mu organizácia a jej zamestnanci umožnia vidieť, prípadne získa ďalšie informácie „navyše" - z hľadiska poznania detailov posudzovaného systému sa však externý audítor len ťažko môže porovnávať s interným, ktorý má na to predsa len viac času. Na druhej strane, externý audítor netrpí „prevádzkovou slepotou" na tých miestach, kde sa niektoré javy v organizácii všeobecne prijímajú ako normálne. Iba externý pohľad poukáže na ich bezpečnostné riziká. Externý audítor, na rozdiel od interného, v rámci výkonu auditu využíva oveľa širšie know-how, ktoré získal na základe skúseností z auditov aj iných organizácií - a časť tohto know-how organizácia získa vo forme poznatkov z jeho zistení, zo záverečnej správy či z jeho postupu a otázok, ktoré kladie v rámci výkonu auditu.

M. SVETLÍK: - Ak ide o externý audit, môžem len zopakovať obecne známe skutočnosti - objektivizácia zistených skutočností, eliminácia „vnútropodnikovej slepoty", interných organizačných a medziľudských vzťahov a pod., na druhej strane tento audit nemôže obsiahnuť veľa interných detailov a špecifík. Dôležitý je všeobecnejší pohľad. Určitá skupina organizácií má zo zákona povinnosť robiť externé ekonomické audity. V prípade informačnej bezpečnosti to neplatí, ale stojí za zamyslenie, prečo. Je všeobecne známe, že právne vedomie zaostáva za technologickým rozvojom. Preto sa nedivme, že externý audit informačnej bezpečnosti nie je ešte uzákonený - právne vedomie ešte nestihlo absorbovať to, že informácie majú na chod spoločnosti nemenej dôležitú úlohu ako financie. Ak si túto skutočnosť, na rozdiel od našich zákonodarcov, uvedomíme, môžeme externý audit informačnej bezpečnosti postaviť na úroveň ekonomického auditu - so všetkými zárukami, zodpovednosťou a, žiaľ, aj známymi nedostatkami. A ešte raz pripomínam a prihováram sa za „odtabuizovanie" problému zaisťovania informačnej bezpečnosti alebo jej auditu tretími subjektmi. Je to služba ako každá iná, so svojimi ekonomickými a bezpečnostnými dosahmi. Pri týchto úvahách sa riaďme vlastnou hlavou a vlastnými skúsenosťami. Nedávne problémy renomovaných audítorských spoločností len potvrdzujú, že vlastná skúsenosť je tou najlepšou skúsenosťou. Na poli informačnej bezpečnosti to platí tiež a solídna externá spoločnosť v tejto oblasti sa nepozná podľa reklamy a majetku, ale podľa referencií, ktoré sú podoprené vlastnou skúsenosťou.

Pripravil Jozef Šupšák