Bezpečnosť firemných informácií – ako ju vidia odborníci

Na jednej strane nepochybný prínos informačných a komunikačných technológií (IKT), na strane druhej neistota o utajenie a ochranu dôverných osobných či firemných informácií. Technologický vývoj umožňuje napredovať všetkým zúčastneným – výrobcom a používateľom IKT ako aj tým, ktorí chcú zneužiť informácie vo svoj prospech, resp. v neprospech niekoho iného. Dostupnosť informácií a ich bezpečnosť často rozhoduje o úspechu v mnohých oblastiach. K riešeniu otázok týkajúcich sa bezpečnosti informácií sa vyjadrili zástupcovia významných spoločností pôsobiacich na slovenskom trhu IKT – Ivan Masný, analytik a bezpečnostný architekt spoločnosti EMM, s. r. o., Ján Schwarz, technický riaditeľ spoločnosti Softip, a Gabriel Fedorko, technický riaditeľ spoločnosti Microsoft Slovakia.


Ivan Masný


Ján Schwarz


Gabriel Fedorko

Ako začať s riešením bezpečnosti

Investície do technológií sú v súčasnosti nákladné, a preto si zákazníci strážia bezpečnosť informačných systémov. K zneužitiu cenných informácií dochádza nielen v dôsledku útokov hackerov a kyberterorizmu. Príčinou je aj nedostatok interných zdrojov na prevádzku informačných systémov a zlá interná politika voči zamestnancom. Neustále sa komunikuje on-line, rýchlo sa rozvíja elektronický obchod, informačné systémy sú otvorené a prepojené, a pritom sa v nich nachádzajú cenné informácie. To všetko sú dôvody, prečo treba riešiť ich bezpečnosť komplexne a nie iba čiastkovo. *„Na zabezpečenie informačného systému treba vypracovať projekt, ktorý bude zosúlaďovať legislatívne požiadavky na danú firmu a jej informačný systém s požiadavkami na podnikanie a firemnými cieľmi. Samozrejme, je dôležité budovať bezpečnosť na štandardoch, či už sú to naše slovenské normy STN alebo medzinárodné štandardy.“*, konštatuje Ivan Masný.

Bezpečnostný projekt by mal stavať na štúdii, ktorá zadefinuje, čo a v akom rozsahu treba v rámci firmy riešiť. Ďalšou dôležitou fázou je analýza rizík daného systému, ktorá povie, kde sú slabé miesta a do čoho treba investovať v rámci ochrany aktív, ktorými môžu byť nielen technológie. Bez analýzy rizík sa nedá urobiť kvalitný návrh bezpečnostného projektu. Pri jej absencii môže dôjsť aj k tomu, že firma preinvestuje zbytočne veľa financií.

Celý proces budovania bezpečnosti treba rozbehnúť v troch hlavných líniách:

- vybudovanie infraštruktúry,
- vytvorenie bezpečnostného povedomia zamestnancov (neustále ich informovať o tom, aké informácie sú pre firmu dôležité a ako sa takéto informácie majú chrániť),
- postavenie architektúry bezpečnostného systému a prevádzkovej časti, na ktorej bude celý systém fungovať; bezpečnostná architektúra určí, akým spôsobom aplikovať vo firme bezpečnosť informácií (určí sa napríklad, že prenos informácií bude chránený, a to šifrovaním s určitou silou a pod).

Keď hovoríme o legislatívnej rovine bezpečnosti informácií v rámci firmy, treba zostaviť bezpečnostný manuál – súbor pravidiel hry pre zamestnancov, dodávateľov, zákazníkov a pod., teda pre všetky subjekty, ktoré sa podieľajú na fungovaní firmy. Vrcholový dokument je bezpečnostná doktrína, ktorú schváli vrcholový manažment a zaväzuje všetkých dodržiavať pravidlá bezpečnosti informačných technológií a investovať do nich.

„Na konci procesu budovania bezpečnosti je audit informačného systému. Ten poskytuje spätnú väzbu, aké riešenia sa implementovali, ako prebehla implementácia, a odpovie na otázky, čo sa pri zabezpečení urobilo zle a čo treba napraviť,“ hovorí I. Masný. *„Audit nijako nesúvisí s analýzou rizík. Ide o nestranný, nezávislý pohľad a zhodnotenie systému.“*

Internet a s ním súvisiace výzvy bezpečnosti

Približne v roku 1995 sa začal internet viac presadzovať nielen v akademickej, ale aj komerčnej sfére. Ukázalo sa, že prináša množstvo výhod – napr. efektívnejšiu komunikáciu. *„Rozvoj internetu dospel dnes do zaujímavých rozmerov a priniesol so sebou mnohé výzvy, hlavne z hľadiska bezpečnosti. Dôvodmi, prečo treba venovať bezpečnosti veľký význam, je napr. veľké množstvo produkcie chybného kódu, ktorý je čoraz sofistikovanejší, či technológie ako spyware a phishing. Tieto technológie umožňujú zneužiť informácie, ktoré sa prenášajú on-line,“* uvádza Gabriel Fedorko.

Medzi najrozšírenejšie IKT, ktoré sa používajú v praxi, patria nepochybne produkty spoločnosti Microsoft – operačný systém Windows, internetový prehľadávač Internet Explorer a iné. Čo v oblasti on-line bezpečnosti teda podniká Microsoft?

Aktivity spoločnosti Microsoft v oblasti bezpečnosti sa sústreďujú do troch oblastí:

1. Investície do technológií – Microsoft každoročne investuje do výskumu a vývoja viac ako 6 mld. USD. Z toho 1/3 dáva na vývoj bezpečnostných technológií. *„V dnešnom svete je bezpečnosť základnou funkčnosťou každého nového produktu. Ak firma ponúka produkt, ktorý nie je bezpečný, stáva sa ťažko predajným“*, tvrdí Fedorko.
2. Osveta – aby produkty prinášali zvýšenú úroveň bezpečnosti, Microsoft pripravuje pre používateľov návody, ako nasadzovať a najlepšie používať ich softvér.
3. Spolupráca – Microsoft spolupracuje s inými IT spoločnosťami, vládnymi inštitúciami a rôznymi organizáciami, aby mali používatelia k dispozícii efektívnejšie bezpečnostné technológie. Spoločne sa tiež zasadzujú o presadzovanie práva, aby boli potrestaní tí, ktorí porušujú právne normy. Napr. dosiaľ sa páchateľom trestných činov v oblasti spamu podarilo uložiť tresty vo výške 100 mil. USD.

Microsoft v oblasti bezpečnosti presadzuje izoláciu. *„Izoláciu možno chápať vo vzťahu k vonkajšiemu svetu, tzn. to, čo nie je povolené, sa ku mne nedostane. Ďalej sa izolácia týka aj bezpečného používania jednotlivých súčastí operačného systému. Príkladom je nasadenie Service Packu 2 pre Windows XP alebo Service Packu 1 pre Windows Server 2003, ale aj technológia AntiSpyware. V budúcnosti prinesie podstatne vyššiu úroveň zabezpečeného sieťového prístupu pripravovaný operačný systém Longhorn. Microsoft pripravuje aj nový internetový prehľadávač Internet Explorer 7.0, ktorý bude vo veľkej miere postavený na technológiách, ktoré majú používateľov chrániť pred novými hrozbami ako phishing, malware a spyware. Súčasťou IE 7.0 bude aj technológia na nasadenie korporátnej politiky, tzn. ako má fungovať IE, ak zamestnanci firmy navštevujú aj on-line zdroje“*, konštatuje Gabriel Fedorko. Microsoft kladie obrovský dôraz aj na autentifikáciu, ktorá je základným predpokladom bezpečnosti. Jeho autentifikačná technológia je postavená na Windows Active Directory.

Spam a phishing

Spam sa stal obrovským problémom, ktorý má okrem bezpečnostného aj komerčný dosah. Napríklad Hotmail a MSN denne zachytí 3,2 mld. spamov. V boji proti spamom sa Microsoft sústreďuje na tri oblasti:

1. legislatíva,
2. spolupráca s inými firmami na tvorbe štandardov a ich implementácia do riešení,
3. vzdelávanie používateľov.

„Súčasťou technológií by malo byť čoraz viac subtechnológií, ktoré riešia problematiku spamu, ako napríklad Sender ID alebo technológia filtrovania. Ich cieľom je, aby používateľovi prichádzala len tá pošta, ktorú si vyžiadal“, uvádza Gabriel Fedorko.

Phishing je jedna z najnebezpečnejších praktík, pretože odchytáva veľmi citlivé údaje, ako heslá a čokoľvek iné, čo človek zadáva na internete. *„Riešeniu tohto problému sa bude venovať spomínaný Internet Explorer 7.0, pretože je to vstupná brána k využívaniu bankových služieb v on-line prostredí alebo nakupovaniu cez internet, kde však treba zadať číslo kreditnej karty,“* dodáva Fedorko.

Keď na prihlásenie treba viac ako len meno a heslo

„Častokrát útok neprichádza z vonkajšieho prostredia – internetu, ale priamo zvnútra spoločnosti. Môže k tomu napr. dôjsť tak, že sa nepoužíva šifrovaná komunikácia na prístup k citlivým dátam, alebo zamestnanec spoločnosti prezradí niekomu svoje prístupové meno a heslo,“ tvrdí Ján Schwarz.

Aby firmy zabránili takémuto bezpečnostnému riziku, implementuje sa dodatočná autentifikácia, teda nepoužíva sa na prístup len meno a heslo, vyžaduje sa aj digitálny certifikát. Aplikácie, ktoré natívne nepodporujú šifrovanú komunikáciu, sú zabezpečené protokolom IPSec, ktorý je súčasťou Microsoft Windows. V praxi to znamená, že ak sa aj niekto dozvie prístupové meno a heslo do aplikácie, nemožno sa prihlásiť, ak nemá platný certifikát – čiže privátny a verejný kľúč. Administrátor certifikačnej autority prideľuje privátne a verejné kľúče jednotlivým používateľom a nastavuje pravidlá, kde má daný používateľ prístup. Každý certifikát má časovo obmedzenú platnosť a musí sa obnovovať. Pri podozrení na zneužitie prístupu do firemnej infraštruktúry alebo k aplikáciám stačí, aby administrátor daný certifikát zrušil. Celá PKI infraštruktúra je postavená na certifikačnej autorite Microsoft. Distribúciu a publikovanie verejných kľúčov zabezpečuje Microsoft Active Directory.

V snahe o ďalšie zvýšenie bezpečnosti možno toto riešenie rozšíriť o Secure ID alebo Smart karty.

Prístup cez šifrovaný VPN kanál do firemnej infraštruktúry prináša znížený komfort, pretože používatelia musia mať aspoň čiastočnú znalosť IT, aby si vedeli vyžiadať certifikát, naimportovať, kontrolovať jeho platnosť a pod. Okrem toho je dosť problematické zabezpečiť tento spôsob komunikácie z internetových kaviarní, hot spotov alebo z miesta, ktoré je už chránené firewallom.

Efektívnejším ako VPN prístup a hlavne pre používateľa pohodlnejším riešením je využiť vlastnosti produktu Microsoft ISA Server na prístup do firemnej infraštruktúry. Pri použití Microsoft ISA Server ako vstupnej brány k firemným informáciám netreba vytvárať šifrovaný VPN kanál a stále možno použiť dodatočnú autentifikáciu používateľa.

Bezpečnostný dizajn postavený na PKI infraštruktúre, Active Directory a produkte Microsoft ISA Server je implementovaný napr. v spoločnostiach Neumann Aluminium Fliesspresswerk Slovakia, s.r.o. (spracovávanie a výroba kovov a umelých hmôt v Žarnovici), Slovenské národné múzeum a Antalis a.s. (bývalý závod Smoza, veľkoobchod s papierom). Na jednom z celoeurópskych mítingov spoločnosti Antalis bol tento dizajn zabezpečenia prezentovaný ostatným pobočkám v Európe. Všetky pobočky tejto firmy naň budú, pravdepodobne, v blízkom čase migrovať. *„Nie je to preto, že by toto riešenie bolo pekné, ale preto, že práve slovenská pobočka nemala od leta 2003 problémy s bezpečnosťou ani s komfortom používateľov – zamestnancov pri zabezpečenom prístupe k firemnému systému. Ďalej bolo toto riešenie pripravené na požiadavky, ktoré vznikli v priebehu rokov 2003 až 2005,“* uvádza Schwarz.

Dôležitosť bezpečnosti narastá

Vo svete IKT existujú v súčasnosti mnohé úlohy a problémy, pričom bezpečnosť informačných systémov je trvalo na jednom z popredných miest záujmu výrobcov aj používateľov IKT. Realita súčasného podnikateľského prostredia núti zaoberať sa touto problematikou bankové, poisťovacie či štátne organizácie aj priemyselné podniky. Informačná spoločnosť už vo svojom názve predznamenáva, čo bude v najbližšej budúcnosti jej podstatou. Informácie. Zaručenie ich bezpečnosti a dôveryhodnosti je výzvou pre celý trh IKT.

Spracované podľa materiálov spoločnosti Omnipublic.

-tog-