Risk Analysis Consultants, s.r.o
Národní 9, 110 00 Praha 1, CZ

tel. +420 2 2207 5340
fax +420 2 2422 8273
rac@rac.cz, www.rac.cz

INFORMATION SECURITY EXPERTS

WHITE PAPER

Odpovědnost je dobré vnímat i ctít

Bezpečnost informací malé a střední podniky zanedbávají a podceňují

Marián Svetlík,
vedoucí konzultant
Risk Analysis Consultants, Praha

Když se mluví o bezpečnosti informací, zejména zpracovaných informačními technologiemi, hovoří se o tom, jak zajistit jejich důvěrnost, integritu a dostupnost. Zdůraznění těchto tří základních atributů bezpečnosti je velice důležité. Jejich nedostatečné zajištění totiž může způsobit každé firmě nenahraditelnou škodu.

Aby bylo vůbec možné hovořit o hrozících škodách z nezabezpečených informačních systémů (IS), je třeba jednoznačně vyjasnit, jaké místo mají prostředky informačních technologií (IT) v našich podnikatelských aktivitách. V prvé řadě je třeba stanovit klíčové podnikatelské procesy. Od těch se pak odvíjí i požadavky na bezpečnost (důvěrnost, integritu a dostupnost) informačních technologií a systémů, které tyto klíčové procesy podporují.

Podle předmětu podnikání mohou být IT/IS základními výrobními prostředky, například v e-businessu nebo v činnosti konstrukční kanceláře, která používá výhradně CAD. Většinou fungují IT/IS ve firmách jako prostředky podpůrné k základním podnikatelským procesům (účetní systémy, ale i např. mzdové, personální, skladové, controlling, managerské IS (MIS), systémy řízení výroby apod).

Společnost, jejíž podnikatelskou činností je poskytování logistických služeb nebo distribuce zboží, bude zřejmě výrazně závislá na kvalitě a bezpečnosti IS, který zajišťuje evidenci zákazníků a skladového hospodářství. Personální agentura podnikající přes Internet bude naopak závislá na kvalitě a bezpečnosti personálního evidenčního systému a na kvalitě a bezpečnosti internetového připojení.

Zajištění dostatečné bezpečnosti informací

Zajištění dostatečné bezpečnosti informací není jednoduchým procesem. Co se pod těmi čtyřmi slovy skrývá?

a) Informace - obecně jde o jakékoliv informace, které mají z hlediska podnikání pro uživatele nějakou cenu a jejich nedostatečná bezpečnost může způsobit firmě škody. Z tohoto pohledu je jedno, v jaké podobě se informace vyskytují, zda jsou na papíře, na paměťových médiích počítačů, nebo jenom jako vědomosti v hlavách pracovníků. O bezpečnosti informací v IS se mluví proto, že IT/IS se stávají nedílnou součástí procesu zpracování informací a postupně v něm sehrávají stále větší roli.

b) Bezpečnost - představuje zajištění tří základních parametrů, a to důvěrnosti, integrity a dostupnosti.

c) Dostatečnost - je další z klíčových pojmů. Jde o určení, jaká bezpečnostní opatření nebo technologie jsou ještě postačující k tomu, aby bylo možné odpovědně říci, že informace jsou bezpečné. Nebo naopak, že se na jejich zajištění neplýtvá zbytečně prostředky tam, kde to není potřeba. Při určování dostatečnosti se vy-chází z velikosti škod, které by mohlo nedostatečné zabezpečení informací firmě způsobit a z posouzení toho, jaké hrozby vlastně

V020611

informacím hrozí (kdo by mohl mít na informacích zájem, jakým způsobem by je bylo možné zneužít apod.).

d) Zajištění - jde o proces, spočívající v zjištění aktuálního stavu (analýza bezpečnosti informací), přijímání vhodných bezpečnostních opatření (implementace bezpečnosti informací), kontrole jejich účinnosti a dodržování (audit bezpečnosti informací) a přizpůsobování se novým podmínkám (revize bezpečnosti informací).

Zajištění dostatečné bezpečnosti informací je vyvážený systematický proces, který lze parametrizovat kvalitativně, kvantitativně i časově.

Z mnoha výše uvedených pojmů je třeba vysvětlit pojem bezpečnostní opatření. Jeho objasnění pomůže při stanovení pozice a vážnosti, kterou by bezpečnost informací ve firmě měla mít.

Přísně diferencovaný úkol

Každý z nás určitě stál před problémem zabezpečit byt. Při výběru způsobu zajištění se určitě vychází z toho, co v tom bytě je a jakou to má pro koho hodnotu (nejenom přímou materiální, ale i nemateriální). Nestačí ale pouze instalovat vhodné zámky nebo závory, je nutné např. naučit všechny obyvatele bytu je používat a zavést odpovídající „bezpečnostní režim. Zabezpečení bytu je tedy komplex technických a netechnických bezpečnostních opatření a pravděpodobně těch netechnických bude často i víc.

Velice podobná situace je i v případě bezpečnosti informací, která je také komplexem technických a netechnických bezpečnostních opatření. Navíc ta technická opatření nejsou výlučně jenom charakteru, který odpovídá náplně práce lidí z oddělení IT, ale zahrnují i fyzické zabezpečení prostředků IT, kontrolu vstupu do prostor, bezpečnostní kvalifikace zaměstnanců aj. Vyplývá z toho, že zajištění bezpečnosti informací není záležitostí informatiků. Skupina (oddělení) informatiky plní provozní úkoly, stará se o to, aby IT/IS fungovaly správně a bezpečně. Ale jaké bezpečnostní parametry mají IT/IS splňovat, to je záležitostí vedení firmy, Vedení musí určit, které systémy jsou pro ni jak důležité, jakou mají pro firmu hodnotu. Na informaticích je pak, aby bezpečnostní opatření odpovídající důležitosti jednotlivých systémů zabezpečili.

Záběr bezpečnostních opatření je však mnohem širší. Kromě prostředků IT je bezpečnost informací zajišťována i dalšími opatřeními - fyzickou bezpečností, školením a vzděláváním, organizací a řízením apod. V komplexu je cílem zajištění dostatečné bezpečnosti informací vytvořit příznivou vnitrofiremní bezpečnostní kulturu. Ponechat problematiku bezpečnosti informací pouze na informaticích není správné řešení.

Nastartování systémových mechanizmů uvnitř firmy, které postupně působí k příznivé bezpečnostní kultuře firmy, se nazývá zaváděním systému řízení bezpečnosti informací (ISMS - Information Security Management Systém). Co všechno je doporučeno pro to udělat, je detailně popsáno v ČSN ISO/IEC 17799:2000 a v BS 7799:2000 (část1. a 2.)

Velká a malá bezpečnost

Bezpečnost informací je důležitá jak pro velké tak i pro malé firmy. Selhání bezpečnosti může mít katastrofální následky pro firmu nezávisle na její velikosti. Rozdíl je pouze v tom, jaké hodnoty se v IT/IS skrývají a od toho se dá odvodit i způsob, použitá metoda a míra nákladnosti celého procesu zajištění bezpečnosti.

Podle tuzemských zkušeností, které se potvrzují i celosvětovými odhady,

Risk Analysis Consultants, s.r.o
Národní 9, 110 00 Praha 1, CZ

tel. +420 2 2207 5340
fax +420 2 2422 8273
rac@rac.cz, www.rac.cz

INFORMATION SECURITY EXPERTS

RAC®

WHITE PAPER

V020611

Risk Analysis Consultants, s.r.o
Národní 9, 110 00 Praha 1, CZ

tel. +420 2 2207 5340
fax +420 2 2422 8273
rac@rac.cz, www.rac.cz

INFORMATION SECURITY EXPERTS

WHITE PAPER

se náklady na zajištění bezpečnosti informací a IS pohybují řádově kolem nebo pod 10% z celkových nákladů na provoz a zpracování informací ve firmě. Přirozeně, že když se bezpečnosti několik let nikdo systematicky nevěnoval, tyto neproinvestované náklady se kumulují a pak je i nastartování a zavádění procesu zajištění bezpečnosti informací úměrně dražší. Jestliže navíc důležité bezpečnostní požadavky, které vycházejí z provedených analýz, vyžadují určitá konkrétní bezpečnostní opatření může dojít k situaci, kdy je pro zajištění dostatečné bezpečnosti informací nutné část nebo celý IS předělat znovu nebo zakoupit systém nový, jiný.

Závěr na začátek

Problematika zajištění bezpečnosti informací je značně rozsáhlá a masovým rozšířením a nasazením IT/IS se dostává do popředí obecného zájmu. Z množství důležitých poznatků shrňme pouze několik:

- zajištění bezpečnosti informací je komplexní a systémový proces, cílem kterého je nastartovat a udržet vnitrofiremní bezpečnostní kulturu na úrovni, která vytváří předpoklady pro dostatečnou bezpečnost informací ve firmě;

- bezpečnosti informací je samostatným multidisciplinárním oborem, který není součástí pracovní náplně oddělení/pracovišť informatiky;

- bezpečností informací je nanejvýš vhodné se zabývat co nejdříve, nejlépe už ve fázi výběru nebo tvorby IS;

- v oblasti bezpečnosti informací je vhodné vyslechnout si na problém více nezávislých názorů, nejenom názor dodavatele, protože zajištění bezpečnosti není obecně levná záležitost.

V020611