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

Softwarové noviny 2-5/2002. Seriál čtyř článků je pojat jako volné povídání na téma komplexního a systémového přístupu k řešení zajištění bezpečnosti informací v organizaci v souladu s doporučeními ČSN ISO/IEC 17799:2000 a s nejlepšími praktikami, jaké se v obdobných případech používají ve světě i v unás.

INFORMAČNÍ BEZPEČNOST

Ing. Marián Svetlík:
Od ukončení vysokoškolského studia výpočetní techniky pracoval v různých oblastech výzkumu, vývoje a aplikací IT. Od roku 1992 se zabýval kriminalistickou a forenzní analýzou počítačů a sítí. Do roku 2000 vedl pracoviště počítačové expertizy Kriminalistického ústavu Praha. V současné době je vedoucím konzultantem společnosti Risk Analysis Consultants, s r. o.

CAST I.

Informační bezpečnost je pojmem, který je skloňován stále častěji. Mílovými kroky kráčíme k informační společnosti, společnosti, kde hodnota informací začíná mít stále větší váhu, kde si začínáme postupně uvědomovat, co vlastně reálně znamená ono často (ne)skloňované slovní spojení "know-how", kde na vlastní kůži často cítíme, jak citlivé, důležité a zneužitelné jsou osobní informace, kde život firmy často stojí a padá na důvěrnosti informací, s nimiž pracuje.
Na první pohled by se zdálo, že to s bezpečností informací nemůže být tak zlé. Ze všech stran se na nás řítí záplava reklam na kvalitu a vysokou technologickou úroveň bezpečnostních a zabezpečovacích systémů, špičkovou úroveň a prakticky neprolomitelné šifrovací algoritmy, elektronický podpis, PKI, čipové karty, biometrické autentizační a přístupové systémy,...
Je to dost? Který systém si vybrat a za kolik? Zachrání (ochrání) naše informace dobrá šifra? Můžeme klidně spát, když zavedeme do firmy (úřadu) PKI? Budou potom naše informace bezpečné? Kde se mají hledat odpovědi na tyto a jim podobné otázky?
S podobnými problémy jme se potýkali a potýkáme stále častěji. Pokusme se nalézt odpověď na základní otázku: Co je to informační bezpečnost?

1. Informace

Začneme od začátku a zkusíme si nejdříve vysvětlit, co vlastně představují ta dvě slova - *informační bezpečnost*. Úmyslně jsem pro název seriálu použil slovné spojení v tomto pořadí, protože nejdříve budeme hovořit o **informacích** a potom o jejich **bezpečnosti**.
Všechno, kolem čeho se vlastně točí celá problematika, jsou informace. Rozvoj výpočetní techniky v nás už automaticky vyvolává asociaci, že informace je něco, co se zpracovává na počítačích, co se ukládá na jejich discích, co se přenáší po síťových linkách a co "putuje" po Internetových dálnicích. Na tyto informace útočí hackeři, viry, zabezpečujeme je firewally, šiframi, podepisujeme elektronickými podpisy a chráníme přístupovými právy.
Máme informační systémy (v tomto kontextu výpočetní systémy), s rozvojem informačních (opět rozuměj počítačových) systémů se mluví o informační dálnici a informační společnosti. Všechny tyto pojmy v nás vyvolávají dojem, že k nám informace přišly s rozvojem počítačů, že to jsou ty "jedničky" a "nuly", kterých jsou plné disky a které se "prohánějí" po Internetu.
Informace je však pojem mnohem širší. Na tomto místě by se dalo nalistovat několik naučných slovníků a podat několik učených definic. Já použiji raději příklad fiktivní společnosti, jejíž činnost je závislá na informacích:
Naše smyšlená společnost se kromě jiného zabývá konstrukcí strojních zařízení. A protože to umí, nebylo pro ní problém najít si výhodného zahraničního partnera, který je schopen dobře ocenit práci konstruktérů. Partner je bohužel až v Brazílií. Práce na společných projektech však vyžaduje operativní spolupráci a nejvýhodnější by byla společná práce konstrukční kanceláře s výrobou. Brazílie je však trochu z ruky, a proto se spojení realizuje pomocí Internetu.
České know-how ve spojení s technologiemi, které jsou pro oblast činnosti naší společnosti příhodné právě v Brazílii, přináší oběma subjektům efektivitu v podnikatelských záměrech. Na rozdíl od Brazilských partnerů je však naše společnost mnohem zranitelnější právě na poli informační bezpečnosti, protože to, co právě informace jí přinášejí největší zisky. Informace a jejich bezpečný přenos na druhou stranu zeměkoule je to, co má v tomto partnerském vztahu pro naši společnost klíčovou hodnotu.
Takový je hrubý nástin situace v naší "příkladné" společnosti. Při letmém pohledu by se mohlo zdát, že opět přece mluvím o počítačích a informacích, které jsou přenášeny Internetem a že pouze potvrzuji to, že bezpečnost informací je vlastně

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

bezpečností informačního (v tomto kontextu počítačového) systému a informačních technologií (v tomto kontextu technologií určených pro zpracování informací). Pravda to je pouze částečná. Aby se dalo mluvit o informacích, je potřeba si nejdříve stanovit o jaké informace se vlastně jedná, jakou cenu ty které informace pro naší společnost mají a v jaké podobě a kde všude a jakým způsobem se s nimi pracuje. Až potom si můžeme udělat představu, co to pro naší společnost znamená, když se řekne pojem bezpečný informační systém. V naší fiktivní společnosti to tedy budou informace, které nejprve vznikají v hlavách konstruktérů, pak jejich poznámky, výpočty v bloku nebo na kouscích papírů rozprostřených po stole v kanceláři (nebo doma), první náčrty (nejspíše už v CADu), geneze a zdroje vývoje, které jsou uloženy na discích v systému ale i v knihovnách a archívech, data, která jsou přenášena po vnitřní síti, související dokumentace a korespondence (poštovní i elektronická), archív společnosti, ale i “soukromý archív” konstruktéra, internetová komunikace. Zmínit musíme i tu část, která patří vlastně už do působnosti brazilského partnera, protože i tam se informace zpracovávají, důležitá je i jeho důvěryhodnost apod.

Informace jsou tedy pojmem mnohem širším. Nejsou to pouze bity a bajty v počítačích. Pro naši společnost totiž není rozhodující, v jaké podobě nebo na jakém nosiči se informace nacházejí, pro ni je důležitá informace samotná. Ta má hodnotu. Ano, s rozvojem výpočetní techniky je častěji informace prezentována v podobě počítačových dat, ale není to její jediná podoba. Rovněž to nejsou jen osobní počítače, které umožňují, abychom s informacemi pracovali a aby informace mohly být použitelné nebo zneužitelné.

2. Informační systémy

Asi by se dala opět najít učená a možná i vhodná definice informačního systému, obecně však platí, že je to systém, který slouží k získání, ukládání, zpracování a poskytování informací. Úmyslně se nezmiňuji o tom, jak jsou informace reprezentovány, protože pro společnost mají hodnotu nezávisle na tom, zda jsou uloženy v paměti počítače nebo konstruktéra.

Z hlediska pohledu naší fiktivní společnosti je tedy informačním systémem vše, co je schopno pracovat s informacemi určité hodnoty. Informačním systémem je také vše, co informace zpracovává v průběhu jejích životního cyklu - od vzniku až do doby, kdy pro společnost ztrácejí hodnotu, a to nezávisle na tom, v jaké podobě se zrovna informace nacházejí.

S drobnou nadsázkou by se tedy dalo říct, že i konstruktér jako takový je součástí informačního systému naší společnosti (a to součástí podstatnou!), ale i všichni ostatní zaměstnanci se jistou mírou na informačním systému podílí. Odborná knihovna nebo archiv je také jeho součástí a konec konců i budova, ve které se archiv nachází, má podíl na tom, že informace, které archiv obsahuje, nejsou volně k dispozici, ale jsou chráněny (alespoň proti povětrnostním

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

RAC®

WHITE PAPER

V020611

V této souvislosti je velice zajímavý a poučný pohled do Ottova naučného slovníku. Koncem předminulého století je **informace** definovaná jako **poučení, zpráva**. Informační systém sice ve slovníku nenajdeme, ale je tam **informační kancelář**, která je popisována jako instituce, zejména bankovní, jejímž cílem bylo získávání a poskytování informací o tom, čemu se dnes říká bonita klientů. Jiné, zejména soukromé informační kanceláře, se zabývaly získáváním a poskytováním informací i jiného charakteru, a to někdy za značnou úplatu. Obecně ale jejich posláním bylo získávat, zpracovávat a poskytovat informace. Kreditem takových kanceláří byla zejména serióznost a důvěrnost zjištěných informací.
No řekněte, v čem se to liší od našich informačních systémů? Pouze a jenom v objemech a v technologiích zpracování. Hodnoty zůstávají stejné: serióznost a důvěrnost.

vlivům).
Závěr z výše uvedeného je jednoduchý: v kontextu informační bezpečnosti je pojem **informace** chápán jako jakákoliv informace v jakékoliv podobě nebo formě, která má pro společnost (organizaci) hodnotu a **informačním systémem** je systém, který tyto informace získává, zpracovává uchovává a poskytuje, opět nezávisle na tom, jakým způsobem (ve smyslu technologickém) je tento informační systém realizován.
Protože však informační technologie (v tomto smyslu počítačové) přebírají stále větší roli v procesu zpracování informací, jejich pozice v komplexu informačních systémů je stále větší, vážnější. Je to nejenom proto, že rostou paměťové kapacity a výpočetní výkony, ale výrazně se rozšiřuje i spektrum aplikací a oblasti uplatnění, zpracovávají se informace mnohdy neobvyklého charakteru a formy, počítačové/digitální technologie začínají postupně nahrazovat mnohé "klasické" postupy, jevy a předměty, na které jsme byly mnohdy desetiletí a i staletí zvyklí.
Jenom jako příklad uvedu klasický telefon pana Bella, který se 120 let prakticky principiálně nezměnil až do doby, kdy jsme začali telefonovat přes Internet (a i to jenom jako "vedlejší" produkt zdokonalujícího se způsobu komunikace) nebo používat GSM technologie. Přemýšlejme, k čemu má GSM blíže. K telefonu, nebo k počítači? Internetu netrvalo snad ani 10 let a už začíná přebírat funkce dalších "klasických" technologií (televize, rádio, pošta, banka, ...)

3. Informační společnost

Na tomto místě je vhodné zdánlivě trochu odbočit od tématu. Kdysi dávno (předesílám, že to bylo v polovině devadesátých let) jsem byl tázán, jaké technologie nejvýznamnějším způsobem ovlivnily lidskou komunikaci. Já vybral tři:

- již zmiňovaný **telefon** pana Bella z druhé poloviny předminulého století,

- **počítač** z poloviny minulého století,

- **hudební CD**.

Myslím si totiž, že hudební CD bylo prvním praktickým a reálním prostředkem, s nímž digitální technologie v širokém měřítku pronikla do běžného života lidí. Od digitálního zvuku již byl jenom malý krůček ke všem ostatním současným vymoženostem - DVD, GSM komunikace, Internetové telefonie, rádia a televize. To byl podle mého názoru ten zásadní a praktický průlom, který digitální (a tím vlastně výpočetní) techniku "protlačil" do běžného života společnosti, aniž by lidé zaznamenali, že se jim vlastně do "obýváku" stěhují počítače.
Dnes bych určitě k výše zmíněným prostředkům přidal Internet, který v době, kdy jsem vybíral ty předchozí, právě nabíral na dechu. Ale jeho obrovský rozmach a popularita byly umožněny kromě jiného i tím, že byl a je čím dál tím víc schopen poskytovat širokému spektru uživatelů informace v podobě, která je jim mnohem bližší, než jsou (nebo byly) strohá textová rozhraní unixových prostředí.
Důležitý jev, který v poslední době můžeme pozorovat, je také opětovný návrat k centralizovanému ukládání, zpracování a správě informací. Je to způsobeno zejména technologickými pokroky jak v oblasti ukládání dat, tak v oblasti zvyšujících se výkonů jejich zpracování. Možná to v době statisíců velice výkonných PC vypadá nepravděpodobně, ale je to podle mého názoru tak. A paradoxně se o to zasluhuje i Internet a neustále se zdokonalující síťové technologie a služby. Internetový boom znamenal ze začátku obrovský informační chaos, informace byly všude, každý se snažil zpřístupnit vše, co se dalo. Dnes už se začíná postupně tento chaos "uklidňovat" a informace se začínají "seskupovat", centralizovat. Ovšem díky technologickému pokroku na mnohem vyšší úrovni jakéhosi spirálovitého vývoje a také v mnohem větších objemech. Internetový boom byl z pohledu informací jako "velký třesk" při vzniku vesmíru. Najednou byly informace všude ve velkém objemu ale také ve velkém

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

chaosu. Postupně je "přitažlivé síly" zájmů a obchodu začínají seskupovat, velký zmatek se začíná postupně "ukládat".
Již nyní nás informace obklopují prakticky všude. Je jich spousta, jsou až nepředstavitelně propojeny a ještě více se propojují. Žijeme v domnění, že ty naše soukromé, privátní, máme pod kontrolou, že víme, kam je ukládáme, komu je svěřujeme, kdo k nim může a kdo zase nemůže. Mělo by to tak být, protože "naše" informace, neboli naše osobní data, jsou tím nejcennějším, co máme. Propojenost informačního světa přináší ve vztahu k soukromí (nejenom tomu osobnímu, ale i firemnímu a státnímu) nový problém. Stává se stále těžším rozlišit, kde přesně je hranice mezi tím "mým" a okolním světem.

Zatím poslední „2001 CSI/FBI Computer Crime and Security Survey" zaznamenal opět výrazný nárůst jak v počtu útoků na bezpečnost informací, tak ve výši způsobených škod. Popravdě to není nic neočekávaného. Zajímavé na tom však je konstatování, které je uvedeno hned na druhé straně a které se pokusím přetlumočit:

„Zajímavé je, že všechny tyto útoky se uskutečnily navzdory širokému uplatnění bezpečnostních technologií: 95% organizací mělo firewally, 61% IDS, 90% aspoň nějaký systém řízení přístupu, 42% digitální ID atd. Technologie zřejmě nepracují jak by se čekalo."

Podobná situace vládne i na mnohem menším poli firemních informačních systémů. Krásné opojení z toho, kolik různých a pro organizaci důležitých informací se dá na disky počítačů uložit, nahrazuje snaha o jejich třídění, klasifikaci a snaha o praktickou správu, údržbu a efektivní zpracování. Opět se začíná ukazovat, že i když jsou dnes disky s kapacitou nad 30GB běžnými, jsou v klasickém počítači pro běžnou práci nepotřebné. Zdá se, že stačí několik málo GB pro operační systém a základní uživatelské aplikace (i to jenom proto, aby mohly běžet rychleji z lokálního disku) a to ostatní, tedy veškerá důležitá data, je stejně uloženo někde na sdílených síťových prostředcích.Je to způsobeno tím, že je téměř vždy naše práce dílo kolektivní a tudíž s informacemi, se kterými pracujeme teď, pracoval před chvílí někdo jiný a za chvíli ještě někdo další...
Tyto úvahy, zdánlivě nesouvisející s tématem informační bezpečnosti, nebyly zbytečné. Když mluvíme o informačních systémech, musíme si totiž uvědomit, že přes tendenci k centralizaci v ukládání a zpracování informací, ke které se postupně vracíme, existuje stále větší a neustále se zvětšující kapacitní a výpočetní potenciál, který je rozptýlen v "prostoru". Není to jenom zahálející výpočetní výkon osobních počítačů. Už jenom chvíli a nastane reálné (nejenom v projektech a v reklamních ukázkách) a úplné propojení technologií (telefony, počítače, Internet, televize, kino, lékař, zaměstnání, ...).
Tak, jak se neustále zvyšují objemy zpracovávaných dat, roste jejich hodnota, a tím i požadavky na jejich bezpečnost. A tak přirozeně rostou nároky na bezpečnostní technologie, které ji mají zajistit. K tomu je zapotřebí neustále vyšších technologických výkonů. Výkonné počítače potřebují nejen běžní uživatelé pro zabezpečení svých dat, ale i ti, kteří se snaží tyto bezpečnostní technologie překonat. Technologický kolotoč se tak uzavírá a stává se nikdy nekončící spirálou, vedoucí k nekonečnému zápasu o spolehlivé technologie k zajištění bezpečnosti informací. Kde je míra, která nám říká, že už dost, že naše informace přece nemají ani hodnotu technologií, které je mají ochraňovat?
Z tohoto zorného úhlu by se asi zdálo, že problém bezpečnosti informací nemá konečné řešení. Už teď je ale zřejmé, že technologiemi to asi nevyhrajeme. Firewally mají své slabiny, s růstem jejich složitosti roste i počet chyb, které jsou do systémů zaneseny a které jsou podrobovány neustálým útokům.Abychom zajistili své informace šifrou, potřebujeme znásobit výpočetní výkon (jinak nás bude on-line šifra zdržovat). Tento vysoký výkon však lze výhodně využít i k jejímu prolomení.
Nedejbůh, aby nastala doba, kdy z důvodů bezpečné práce s informacemi, budeme většinu pracovní doby zadávat hesla, strkat někam nějaké karty či "kovové knoflíky", tisknout otisky palců, mžourat do digitálních kamer a nechávat si on-line měřit průměr hlavy a vzdálenost uší...

4. Bezpečnost informací

Když opustíme obecné úvahy o informačních systémech a informační společnosti a vrátíme se k naší konstrukční kanceláři spolupracující se svým brazilským partnerem, můžeme si z pohledu

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

RAC®

WHITE PAPER

bezpečnosti položit hned několik otázek. Jak dobře máme zajištěnu tu část informací, která je jenom naše? Jak bezpečná je ta část informací, kterou sdílíme s partnerem? Kdo všechno s našimi informacemi může přijít do styku a jak jsou tyto subjekty spolehlivé? Můžeme si položit i další otázky. Dá se zajistit, aby systém, který spravuje naše informace, byl spolehlivý a bezpečný? Kolik musíme investovat do bezpečnostních technologií abychom si mohli říci, že to je dost?

Jestliže si uvědomíme důležitost informací, asi je zřejmé, že pro zajištění výše uvedeného již nevystačíme s empirickým přístupem. Není to podceňování zkušeností jednotlivců - odborníků, ale objektivní jev, protože obecné povědomí o přístupu k bezpečnosti informací existovat v potřebném rozsahu ani nemůže. Informační společnost a informační propojenost světa totiž neexistuje tak dlouho, aby se takové povědomí stihlo vytvořit a dostat do obecného povědomí. Když hoří, hasíme vodou a proti zlodějům zamykáme. To je zkušenost, která je v každém z nás, je obecná a vypěstovaná během staletí. Ale informace? Začínáme chápat, že mají hodnotu, ale co to je, ty informace? Nedá se to chytit. Jsou ještě v mém počítači, nebo už tam nejsou? Jak to vlastně vypadá? Kudy to teče? Co to je ta informační dálnice? Musíme přiznat, že tu a tam něco víme, ale obecným povědomím se to nazvat nedá. Proto ani empirický přístup k jejich zabezpečení nestačí. Naše obecné bezpečnostní povědomí donedávna vystačilo s tím, čemu se říká objektová, fyzická a případně personální bezpečnost. To jsou oblasti, které jsou nám známé a které jsou schopny zajistit bezpečnost všeho, na co jsme schopni si "sáhnout". Vystačili jme si s tím, protože i informace, které měly pro nás, pro organizaci, firmu, společnost hodnotu, nám byly předkládány a zprostředkovávány v materializované podobě. Zejména ve formě dokumentů a písemností. To se potom jednoduše propojila ochrana a bezpečnost fyzických aktiv (např. peněz, zlata, unikátních výrobků) s know-how (např. konstrukční a projektové dokumentace, smlouvy apod.), protože všechna tato aktiva měla hodnotu pouze v materializované podobě. Ještě v nedávné minulosti jsme to, co reprezentuje naše materiální hodnoty - peníze - měli prakticky všichni pěkně pod kontrolou. Své bankovky jme měli po výplatě uložené v zásuvce, ti pořádnější je měli roztříděné do obálek podle jednotlivých účelů použití (měsíční nájem, jídlo, oblečení, ...). Ti bohatší měli své peníze uloženy ve spořitelně a prakticky věděli, že tam peníze leží ve velkém a bezpečném trezoru. Jak je to dnes? Kde vlastně jsou naše peníze? V platební kartě ani v elektronické peněžence je nenajdeme, tam je pouze informace o našem účtu. A co je vlastně náš účet? Pouze informace o tom, za jakou hodnotu si můžeme koupit zboží. Dnes již v bance peníze v materiální podobě prakticky nenajdeme (a tady nemíním v žádném případě parafrázovat určitá "specifika" našeho bankovnictví doufejme že již nedávných let).

Vezměte si třeba předplacené služby mobilních operátorů. Když si pomocí bankomatu a své platební karty dobiji kredit v mobilu, mám fiktivní představu o tom, že v něm mám svých 500.- Kč, za které mohu telefonovat. Zavolám a najednou tam už mám pouze 450.- Kč. Co se stalo? Fyzicky žádné peníze nikam nepřibyly, nikam neputovaly. To se jenom vyměnily nějaké informace mezi mnou, "cizím" bankomatem, zúčtovacím karetním systémem, mou bankou a GSM operátorem. Kde teď jsou mé peníze? Kdo je vlastně má pod kontrolou? Kde je hranice "mého", na které si mohu sáhnout a dát ruku do ohně za to, že je to pod mou kontrolou?

Situace se dnes změnila podstatně. Nejenom fakticky, ale i de-iure. Přijetím zákona o elektronickém podpisu se do elektronické podoby začínají dostávat i takové pojmy, jako jsou smlouvy, doklady, cenné papíry, akcie, peníze... Už si nevystačíme se systémem pevných trezorů, mříží, patentních klíčů a bezpečnostních agentur, které hlídají přístup do objektu a nestačí jíž ani přísné dodržování pravidel spisové

Bezpečnost informací je charakterizována jako zachování:

a) důvěrnosti – zajištění toho, že informace je dostupná pouze osobám s autorizovaným přístupem,
b) integrity - zabezpečení správnosti a kompletnosti informací a metod zpracování,
c) dostupnosti – zajištění toho, že informace a s nimi spjatá aktiva jsou dostupné autorizovaným uživatelům podle jejich potřeby.

Information Security Management – Interpretace standardu BS 7799 pro české prostředí,
© BSI, © RAC, Praha, 2000, str. 5

V020611

služby. Všechno to je i nadále potřebné, ale již nepostačující.
Teorie bezpečnosti informací popisuje tři základní atributy, které je nezbytné pro zabezpečení informací zajistit. Je to **důvěrnost, dostupnost a integrita** informací. Jednoduše řečeno to znamená, správné informace dostupné pouze v nezbytně nutném rozsahu, vždy a jenom tehdy, když to je potřebné. To vše musíme mít pod kontrolou. Dá se to zajistit?
Dá, ale abychom si příště mohli říct jak na to, musíme si k tomu jasně stanovit výchozí pravidla. Pokusím se o to shrnutím výše uvedeného:
1. Základní otázkou bezpečnosti informací je určení jejich hodnoty. Obecně je nám všem jasné, že informace pro nás mají neustále větší hodnotu. Taková všeobecná proklamace však není pro stanovení míry jejich ochrany postačující. Je potřebné použít přesnější metody stanovení jejich hodnoty a není při tom vůbec rozhodující, zda ta hodnota bude vyjádřena pomocí násobků nějaké měnové jednotky nebo jiným způsobem.
2. Nelze zajistit absolutní informační bezpečnost. Míra bezpečnosti a také rozsah a nákladnost bezpečnostních opatření musí vždy odpovídat hodnotě informací, které jsou chráněny.
3. O bezpečnosti informací se většinou nerozhoduje na pracovištích informatiky. Tato pracoviště jsou pracoviště provozní. Jejich úkolem je zajistit, aby informační systémy fungovaly v souladu s podnikatelskými záměry organizace. Jestliže je v zájmu organizace i ochrana informací, tak pracoviště informatiky odpovídá za to, že ta bezpečnostní pravidla, která jsou realizována prostředky IT, budou fungovat v souladu se záměrem organizace. Ale základní záměry v oblasti bezpečnosti informací se nestanovují na úrovni pracoviště informatiky, ale mnohem výše. Jestliže jsou informace klíčovými hodnotami organizace, tak o bezpečnostních principech (říká se tomu bezpečnostní politika organizace) se rozhoduje na úrovni vrcholového managementu.
4. Informační bezpečnost nelze zajistit pouze technickými prostředky. Už jsme si řekli, že informace a informační systémy nejsou pouze počítače a výpočetní systémy. Tyto technické prostředky jsou pouze nástroji pro zpracování informací. Nejdůležitější součástí informačních systémů vždy byl, je a bude člověk. Proto i zajištění bezpečnosti informací je vždy uceleným komplexem organizačních, personálních, technických a jiných opatření, která se navzájem doplňují a vyvažují v závislosti od toho, jakou hodnotu chráněné informace mají.

Přirozeně, že těch základních výchozích pravidel by se dalo vyjmenovat asi víc. Pro úvod by to však stačilo, protože uvedené čtyři body jsou v tuto chvíli těmi základními, které vyvracejí v mnoha organizacích zavedené nesprávné nahlížení na informační bezpečnost.
Příště si řekneme už konkrétní postupy, jak by měla být v organizaci na základě současných nejlepších zkušeností systematicky zajištěna bezpečnost informací.

ČÁST II.

5. Stavíme bezpečný informační systém

Závěr předcházející části našeho povídání o informační bezpečnosti byl postaven na negativních závěrech - definicích. Řekli jsme si, jak informační bezpečnost zajistit nelze. V této části k problému přistoupíme z té pozitivní stránky a budeme si povídat o tom, jakým způsobem je toto možné zajistit na odpovídající úrovni.
Dřív, než se do toho pustíme, si musíme vyjasnit pravděpodobně nejdůležitější závěr, který se dá z těch minulých vyvodit. Překotným vývojem informačních technologií se **bezpečnost informací stává samostatným oborem**. To není nic překvapujícího - samostatné bezpečnostní útvary a bezpečnostní management známe již dávno. Problém je pouze v tom, že se většinou jedná přímo o oblast bezpečnosti fyzické, případně personální, a ve výjimečných případech o bezpečnostní útvary, starající se výlučně o utajované skutečnosti. Tyto útvary a jednotlivci si časem vybudovali určité "výsadní" postavení v organizaci. Potud je všechno v pořádku a tak, jak má být.
Situace se ale dosti zásadně změnila a skalní zastánci pevných trezorů, mříží a silných chlapů z bezpečnostních agentur neustále problematiku informační bezpečnosti potlačují, bagatelizují a přesouvají na někoho jiného - většinou na pracoviště IT. Nechci samozřejmě generalizovat, jen zobecňuji své zkušenosti. Navíc jsem přesvědčen, že všichni, nebo alespoň většina správců systémů a vedoucích IT, mi dají za pravdu.
S trochou nadsázky si dovolím tvrdit, že nikoliv v blízké budoucnosti, ale již teď jsou informace a jejich bezpečnost mnohem důležitější, než bezpečnost fyzická. Ono to tak možná na první pohled nevypadá,

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

protože v novinách se tak často nedočteme, kolik desítek a stovek miliónu už uteklo různými počítačovými podvody a machinacemi. Zato téměř denně čteme o násilných vloupáních. Odhalit násilnou trestnou činnost je mnohem jednodušší. Vylomené dveře, rozbitá okna, vykradená klenotnictví a loupežná přepadení v bankách jsou totiž vidět na první pohled, k tomu není potřeba ani základní vzdělání (tím se v žádném případě nechci dotknout naší policie, ta přece nezjišťuje ty první impulsy - ty se k ní dostávají až na základě oznámení poškozeného a také rozhodně nechci bagatelizovat tragické následky na zdraví a životech lidí, kteří jsou touto násilnou trestnou činností dotčeni).

6. První krok - kdo

Jak jsem již uvedl, informační bezpečnost je samostatným oborem a v této části si povíme, jak by se mělo postupovat, aby byla bezpečnost informací zajištěna. Papírově by mělo být zajištění informační bezpečnosti záležitostí managementu organizace (viz. 3. bod v závěrech minulého dílu). Proč o tom tedy mluvím tady, v časopise určeném ryze počítačovým odborníkům? Přes veškerou "systémovou" nesprávnost jsou to většinou správci sítí, administrátoři a vedoucí IT, kteří bezpečnost informací reálně zajišťují a prosazují. Jednoduše proto, že informatice rozumí trochu víc a také proto, že si jsou vědomi vysoké míry zranitelnosti informací, které jsou za pomoci IS/IT zpracovávány. Sami také asi nejvíce cítí nesamospasitelnost bezpečnostních technologií a rozsah problematiky informační bezpečnosti . Ale začíná to být na ně moc jak po stránce časové (o pracovní době této skupiny lidí si povídat nemusíme), tak zejména po stránce jejich omezených kompetencí.
Proč se tedy s touto problematikou obracím právě na tu nevytíženější skupinu? Jak to už ve světě chodí, problémy mohou vyřešit nejlépe ti, koho nejvíce pálí. Informatici jsou touto problematikou "postiženi" nejvíce a proto by právě tato skupina měla vědět, jak prosadit, aby se informační bezpečnost dostala na to místo v systému řízení organizace, které ji z hlediska její současné, a nepochybně i budoucí důležitosti, náleží. Naštěstí to nejsou vždy jen informatici. Existují i předvídaví vrcholoví manažeři, kteří si jsou vědomi, že v informacích jsou ukryté jejich současné, ale zejména budoucí hodnoty. A jestli mám být upřímný, nejsou to většinou - jak by se možná zdálo - finančníci, ale zejména předvídaví a progresivní kormidelníci průmyslu. Není jich bohužel mnoho (ani tolik, kolik je u nás prosperujících podniků). Takže, informatici, čtěte dál. Možná najdete argumenty, které vám pomohou v dobré věci - zajištění bezpečnosti informací a přenesení odpovědnosti za ni na úroveň, která ji právem náleží.

7. Druhý krok - co a proč

Než si řekneme jak informace chránit, uděláme ještě jednu důležitou, ba přímo zásadní, odbočku. **Bez toho, abychom věděli které informace chránit a proč jsou pro nás důležité, postrádá každé další rozhodování o způsobu ochrany jakýkoliv smysl.** V každé organizaci jsou systémy důležité, méně důležité, pomocné a podpůrné. Každý z těchto systémů zpracovává určitý druh informací, které jsou z hlediska základních podnikatelských záměrů organizace rozdělitelné do několika skupin podle toho, jakou měrou se na těchto záměrech účastní. Některé informace mají tudíž hodnotu zásadní a pro organizaci vysokou, jiné zase nejsou tak podstatné. Ale ani samotná vysoká hodnota informací (i když se nám ji podaří nějakým známým nebo empirickým způsobem vyčíslit) ještě nemusí znamenat vysoké investice do jejich ochrany. Přes vysokou hodnotu pro konkrétní organizaci se informace mohou vyznačovat nízkou zranitelností. Pro okolí jsou prostě nezajímavé a je vysoce nepravděpodobné, že by se někdo pokoušel je nějakým způsobem napadnout. Proč tedy investovat neúměrně vysoké částky do jejich ochrany?
Hodnocení informací je jedním z výchozích kroků při úvahách o zajištění jejich bezpečnosti. Již na první pohled to není problematika jednoduchá. Zasluhuje si delší povídání, a proto se jí budu podrobněji věnovat v následující části seriálu. Tady jenom stručně základní východiska:
a) Účel z hlediska základních podnikatelských záměrů organizace. Již jsem se o tom krátce zmiňoval.
b) Pořizovací hodnota IS/IT. Nejedná se však pouze o hodnotu HW a SW, ale celého komplexu, který s provozem informačních systémů souvisí. Mnohdy jsou s pořízením IS spojeny různé stavební úpravy, příprava zvláštních nebo dodatečných prostor, další technologická zařízení, klimatizace, zajištění bezprašnosti ve výrobních prostorách, pořízení komunikačních prvků a služeb apod. Neméně důležitou součástí při stanovení hodnoty informací jsou samotná data, kdy jedněmi z hodnotících faktorů jsou náklady na jejich získání/nákup nebo jejich vlastní pořízení.

V020611

c) Možné následky, způsobené bezpečnostními incidenty. Již minule jsme si řekli, že bezpečnost informací je zachování jejich důvěrnosti, integrity a dostupnosti. Každé narušení těchto atributů bezpečnosti je označováno jako bezpečnostní incident. Ten jako takový způsobí organizaci určité následky, jejichž míra se stanovuje různými způsoby a metodami. Ohodnocují se ale nejenom náklady na odstranění následků (například náklady na pořízení nových dat při jejich zničení), ale i další možné dopady na organizaci, mezi nimiž je například ztráta konkurenčních výhod, ztráta důvěry, narušení pracovní morálky a mnoho dalších.

d) Míra ohrožení informací. Pod tímto pojmem se skrývá nejenom posouzení možnosti jejich zneužití, zcizení vlastními zaměstnanci nebo průnik z Internetu. Při detailní analýze se jedná o celý komplex faktorů, které mohou působit jako hrozba na bezpečnost informací. Opět jen pro příklad: vliv možných výpadků nebo nestability napájecích napětí, selhání technických prvků, chyby v programovém vybavení, úmyslné nebo nedbalostní chování apod. Další skupinou pro hodnocení informací a míry jejich bezpečnosti jsou samotné důvody, které nás nutí k tomu, abychom se nad jejich bezpečností vážně zamýšleli. Tím podstatným je opět jejich úloha při realizaci podnikatelských záměrů. Souvisí s tím ale i řada dalších faktorů. Aby organizace byla lukrativní pro potenciální klienty (nebo pro potenciálního investora), musí splňovat určité kvalitativní parametry. A tady se nemusí vždy jednat pouze o přesnost a kvalitu výrobků, ale i o celkový image, přičemž už jenom přístup k hodnotám (a informace takovými hodnotami nepochybně jsou) může být důležitým kritériem. Způsob ochrany informací má jednoznačně vliv na důvěryhodnost organizace (tady jsou zářným příkladem například finanční instituce). V neposlední míře má na podnikatelský úspěch vliv i taková skutečnost, jakou je dodržování interních, místních, oborových, ale zejména obecně závazných právních norem. Mám na mysli zejména zákon o ochraně utajovaných skutečností, osobních údajů nebo autorský zákon a mnohé další.. Všechna tato kritéria mají přímou souvislost s bezpečností informací.

Už z uvedených východisek je zřejmé, že jenom samotné zhodnocení nebo ocenění informací není úplně triviální záležitostí. Přirozeně - dá se využít a také se využívá empirických zkušeností a názorů na výše uvedené východiskové parametry. Obecně se však komplexního posouzení nedá dosáhnout pouze na základě místních praktických zkušeností.

8. Třetí krok - jak

Velkým štěstím je, že i podle mých vlastních praktických zkušeností je “komunita počítačových fandů - informatiků” skupinou lidí, kteří nejenom pro bezpečnost informací dělají prakticky vše, co je v jejich možnostech. Oni vědí, nebo alespoň tuší, kde má jejich systém slabiny. Vědí, nebo tuší, jak by se ten který problém dal technicky řešit Minimálně však vědí, že nějaké slabiny jsou a že to lze řešit. Když se však pokusím situaci zobecnit, dostaneme se k několika základním problémům, které brzdí prosazování bezpečnosti informací u nás:

a) Informatika (až na výjimky) **není základním výrobním prostředkem organizace**. Odtud pramení i vztah vedení organizace k problémům bezpečnosti informací, které jsou s pracovišti informatiky zcela nesprávně spojovány. Už jenom těch peněz, co stojí samotné pořízení informačních technologií - a to nemluvím o provozu. A pak má ještě něco zbýt na bezpečnost?

b) Bezpečnost se řeší, až když hoří. Tento problém vyplývá z toho prvního. Když už jsem zmínil dodržování autorského zákona - jen si uvědomme, kolik je ještě organizací, které netrápí používání nelegálního softwaru. Přitom za použití i jednoho “obyčejného” ZIPu nebo Windows Commanderu riskují nepodmíněné tresty odnětí svobody (většinou pro statutární zástupce) a to všechno pro relativně malé částky. Když přijde na lámání chleba a vyskytne se nějaký dobrák, který je udá, jsou ochotni (a hlavně schopni) ihned vyvinout žhavé aktivity, aby se s majitelem autorských práv rychle a hlavně pro sebe bezbolestně vyrovnali.

c) Bezpečnost se řeší jenom když je k tomu vedení organizace dotlačeno. Ty páky jsou různé. Jednou z nejsilnějších jsou zákonem stanovené požadavky. Bohužel až na výjimky bankovního tajemství, utajovaných skutečností a osobních údajů vlastně žádná podstatná, zákonem požadovaná bezpečnostní kritéria stanovena nejsou. Co je ale ze zákona pro některé (většinu) organizace povinné, je účetní audit, součástí kterého je vyjádření auditora k bezpečnosti nebo důvěryhodnosti IS (bohužel pouze účetního). Negativní výrok auditora je příklad té druhé páky, která částečně tlačí vedení k řešení bezpečnosti informací. Jaký je však kvalitativní rozdíl mezi prací, kterou dělat musím a prací, kterou dělám z vlastního přesvědčení, nemusím zdůrazňovat.

d) Informatici mají sklon řešit bezpečnost výlučně technickými prostředky. Je to zcela přirozené, protože

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

V020611

to je jejich profese. Je to ale také proto, že ze své pozice ani nemají jinou možnost a prostředky, jak komplexněji informační bezpečnost prosazovat.
Samotný způsob řešení bezpečnosti informací je již naznačen v předcházejícím problému. V podstatě se jedná o přechod od intuitivního způsobu řešení bezpečnosti ke způsobu systémovému. V úvodu této části jsem uvedl, že informatici povětšinou dělají pro bezpečnost vše, co je v jejich možnostech. Je to ale dost? Je to to správné? Nakolik jsou investice do technologií, které ve své snaze o zlepšení bezpečnosti požadují, opodstatněné? Jak dlouhé heslo použít, jak často jej měnit? A mají se nasadit silná hesla na celou organizaci, nebo jenom někde a když, tak kde?
Podobných příkladů se dá nalézt nespočetně. Intuitivně cítíme, že bezpečnost lze zvýšit přijetím různých opatření, ale mnohem hůř se dá zdůvodňovat kterých a v jakém rozsahu. Z druhé strany platí to, o čem jsme si povídali v minulém díle, a to že informační bezpečnost je pojmem mnohem širším, než se na ní pohlíží v současnosti, a že ji nelze zajistit pouze technologiemi.
Abych co nejvíce přiblížil systémový přístup k řešení informační bezpečnosti použiji příklad, který by mohl problematiku popsat názorněji. Předem na sebe beru riziko, že tento příklad pokulhává, neboť je řeč o úplně jiných souvislostech a jde pouze o přiblížení základního principu. Chci totiž přirovnat řízení bezpečnosti informací k procesu zajištění kvality (např. podle ISO 9000), který je u nás již delší dobu znám, je populárnější, ale bohužel v mnoha případech i zprofanovaný. Každopádně zavedení systému řízení kvality ještě neznamená, že podnik bude vyrábět kvalitně. Jsou v něm ale vytvořeny předpoklady, že kvalita výroby je systematicky sledována a řízena, tudíž se dá předpokládat , že i výroba takového podniku bude kvalitnější.
V tomto pohledu je to s bezpečností informací podobné. Systematický přístup k řízení bezpečnosti znamená, že organizace má nastartované komplexní systémové postupy a procesy, které vytvářejí všechny předpoklady k udržení bezpečnosti informací na odpovídající úrovni. Neznamená to přirozeně, že se už nevyskytnou bezpečnostní incidenty, a že nedojde ke škodám nebo ztrátám. Znamená to ale, že organizace ví zcela přesně, kde má slabiny, a podniká adekvátní kroky k jejich odstranění. Navíc je připravena v případě výskytu bezpečnostního incidentu reagovat na něj způsobem, který minimalizuje možné dopady na její chod a je tudíž v dané chvíli tím neoptimálnějším.

9. Čtvrtý krok - certifikace?

Použil jsem přirovnání k certifikaci podle ISO 9000. Nemusíte se bát, že by v nejbližší době zachvátilo naši zemi “šílenství” honby za certifikáty na bezpečnost informací. Ne že by nebylo podle čeho (od roku 2000 je v platnosti velice dobře napsaná a použitelná norma **ISO/IEC 17799:2000**), ale v oblasti bezpečnosti informací jsou mírně řečeno trhliny nejenom u organizací samotných, ale i v procesu budování obecně použitelného certifikačního schématu. Jedna věc je ale získání mezinárodně uznávaného certifikátu (přitom tuto snahu mnoha organizací vůbec nebagatelizuji), druhá je reálný přínos v zavádění systémového přístupu k řízení bezpečnosti informací. Ideální stav by přirozeně byl, kdyby to šlo spojit, ale současná situace je taková, jaká je.
Certifikace u nás v republice zatím nejsou a ani nemám indicie, kdy by být mohly. V tomto ohledu nás může pouze uspokojit , že ani jinde ve světě není situace výrazně jiná. Momentální absence certifikačního schématu není ovšem v principu na závadu, protože samotný proces zavádění systémového přístupu řízení bezpečnosti informací není žádná procházka růžovým sadem. Ten, kdo poctivě absolvoval certifikaci podle ISO 9000, mi dá za pravdu, že ani příprava není jednoduchá, natož samotná implementace systému. Jde o to, aby se systematický přístup nejenom nastartoval, ale aby se také dostal do reálného života organizace - aby se stal součástí vnitrofiremní kultury. Ze stávajících zkušeností mohu říct, že to není proces krátkodobý, spíše naopak. Z tohoto pohledu tedy nic nebrání jej nastartovat již teď a než se situace s certifikacemi pohne dopředu, můžete mít kus cesty za sebou a být na ni již připraveni. A jsem přesvědčen, že se nemusíte bát přípravy na něco, co pak při případné certifikaci bude vypadat jinak.
Vývoj v oblasti IT jde dopředu sice výrazně, ale v samotných principech řízení bezpečnosti nebudou tyto změny nijak podstatné.
Znovu připomínám, že celý problém není o certifikaci, ale o bezpečnosti samotné. Vraťme se tedy k tomu, kde se zaváděním systematického přístupu k bezpečnosti informací prakticky začít.

10. Ryba smrdí od hlavy

... říká jedno přísloví. Možná trochu tvrdé, ale bohužel vystihující obecnou situaci. Pokud potřebujeme do organizace něco

systematicky zavádět (zdůrazňuji možná již poněkolikáté, že do celé organizace), musíme začít od samotného vedení. Tím nemám na mysli, aby si vedení sedlo a sahalo si do svědomí, zda a jak bude dodržovat bezpečnostní pravidla (stejně je v praxi spíše nedodržuje) nebo jak implementovat PKI (tady už si vůbec nedělám iluze, že by průměrný vrcholový manažer vůbec věděl, co to je). Vedení je v organizaci zejména od toho, aby vydávalo strategická rozhodnutí. Zavádění systému řízení bezpečnosti informací (tj. přechod od intuitivního k systémovému řešení bezpečnosti) je rozhodnutím strategickým. Bez něj celá snaha nemá velkou šanci na úspěch a na každém kroku bude narážet na nespočetné množství vnitropodnikových kompetenčních, finančních, organizačních a jiných bariér. Z druhé strany od vedení vlastně ani nic jiného nepožadujeme. Ale pozor, platí to pouze tehdy, jestliže se jedná o vedení, které si za svým strategickým rozhodnutím umí i stát!

Je hned jasné, že tak jednoduché to nebude. Dobré vedení totiž nedělá strategická rozhodnutí jen tak, na základě hezkých očí nebo úmyslů. Nestačí je jen přesvědčit o pěkné a určitě i celkem jasné a správné myšlence systematizace přístupu k bezpečnosti informací. Celá legrace totiž i něco (lépe řečeno nemálo) stojí a bude to znamenat i určité změny v systému a organizaci práce uvnitř i navenek organizace. Proto už jenom samotná příprava podkladů pro takové strategické rozhodnutí zabere mnoho sil.

Opět malá praktická odbočka. Celkem se zdá, že při rozhodování tohoto, řekněme strategického druhu, je základním nebo podstatným kritériem přímá finanční náročnost projektu. Není to zcela pravda. Často jsou mnohem důležitějším kritériem právě nároky na personální a zejména organizační změny, které si realizace takového projektu vynutí. Nákup, byť drahé technologie, sebou totiž nese mnohem méně reálné řídící a organizační práce, než mnohdy zdánlivě nepatrné nebo nepodstatné organizační změny. Technologie se koupí a implementuje, kdežto při organizačních změnách je nutné intenzivněji pracovat s lidmi a někdy i pozměnit jejich zaběhlé návyky. Co víc, hrozí riziko, že bude nutné změnit i návyky nás samotných. Z tohoto pohledu mohou být v konečném důsledku drobné organizační změny mnohem náročnější a obtížněji realizovatelné, než zajištění určité "vyšší" částky na nákup technologie nebo služby. Tato odbočka není opět v žádném případě myšlena ironicky. Je to prostě tak a je nutné s tím počítat při jakékoliv snaze prosadit něco, co se netýká pouze mě samotného, ale zasahuje to do okruhu více lidí. Koneckonců, vždy jde vlastně o lidi. Již jsem to s nadsázkou zmínil i v souvislosti s bezpečností informací - člověk je nejdůležitější součástí informačního systému!

11. Strategické rozhodnutí formou "Bezpečnostní politiky"

Abychom dali tomuto důležitému a z pohledu našeho cíle zásadnímu kroku konkrétní podobu, pojmenujeme jej podle doporučení ISO/IEC 17799 "Politikou". Možná to není příliš vhodný název, ale když se odpoutáme od asociací s politikařením, vystihuje celkem správně charakteristiku onoho

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

V020611

strategického rozhodnutí. Politika je něco jako programový dokument. Neobsahuje způsoby a prostředky (ty se časem a vývojem mohou měnit), ale cíle a důvody. Proto je tím příhodným dokumentem, vhodným ke schválení vrcholovým vedením organizace. Jak by konkrétně měla taková politika vypadat? Je to dobré vědět, protože ji bude potřebné připravit. Na vedení organizace je, aby ji schválilo, to ji připravovat nebude. Již v této fázi musíme mít zcela jasno, jak systémové řízení informací vypadá a jakých oblastí se Bezpečnostní politika bude dotýkat. Dejme tedy obecnému povídání o komplexnosti a složitosti problematiky bezpečnosti informací konkrétní systematickou podobu.

Podle doporučení ISO/IEC 17799 se v bezpečnostní politice definují cíle organizace při zajištění bezpečnosti informací v následujících základních oblastech:

a) Organizace bezpečnosti - definování vhodných organizačních a řídících struktur, rolí a odpovědností pracovníků organizace.

b) Klasifikace a kontrola aktiv - provedení "inventury" a klasifikace toho, co vlastně bude předmětem ochrany.

c) Personální bezpečnost - definování cílů v oblasti zajištění a zvyšování bezpečnostního povědomí pracovníků.

d) Fyzická bezpečnost - cíle v oblasti předcházení neautorizovaného přístupu do citlivých prostor a k citlivým informačním prostředkům organizace.

e) Řízení provozu - zajištění správného a bezpečného provozu prostředků IT/IS

f) Řízení přístupu - zajištění takového přístupu k informacím organizace, který odpovídá podnikatelským záměrům.

g) Vývoj a údržba systému - stanovení bezpečnostních pravidel pro údržbu a zejména další rozvoj systému.

h) Řízení kontinuity - minimalizace výpadků a škod způsobených bezpečnostními incidenty

i) Soulad s požadavky - zajištění dodržování právních norem, smluvních a bezpečnostních požadavků.

Není cílem vysvětlovat podrobněji strukturu normy. Důležité je to, že už ze základní struktury je jasné, že na bezpečnost informací má vliv mnoho různorodých faktorů a jestli ji chceme zajistit komplexně není to jen o technologiích a zdaleka to není práce jen pro pracoviště IT. Proto zdůrazňuji důležitost Bezpečnostní politiky a nezbytnost jejího schválení (rozuměj přijetí, ztotožnění se) vedením organizace.

Za předpokladu, že se nám povedlo úspěšně absolvovat přijetí Bezpečnostní politiky, máme jednu z nejtěžších etap přechodu od intuitivního k systémovému řešení bezpečnosti za sebou. Zbývají nám ještě dvě - rozpracování politiky do konkrétních realizačních kroků a tou poslední je jejich implementace.

Při naplňování cílů definovaných v Bezpečnostní politice narazíme opět už po několikáté na problém, jaká bezpečnostní opatření jsou právě pro nás ta vhodná a dostačující. Už víme, že uvažované spektrum možných opatření se v Bezpečnostní politice výrazně rozšířilo - od technických prostředků IT/IS na organizační, personální, řídící, právní atd. Už víme, že o vhodnosti bezpečnostních opatření rozhoduje hodnota chráněné informace (aktivum) a míra jejího ohrožení. Jak pro realizaci bezpečnostní politiky vybírat ta správná, vhodná, účinná a bezpečnostně i ekonomicky efektivní opatření si povíme v další části.

ČÁST III.

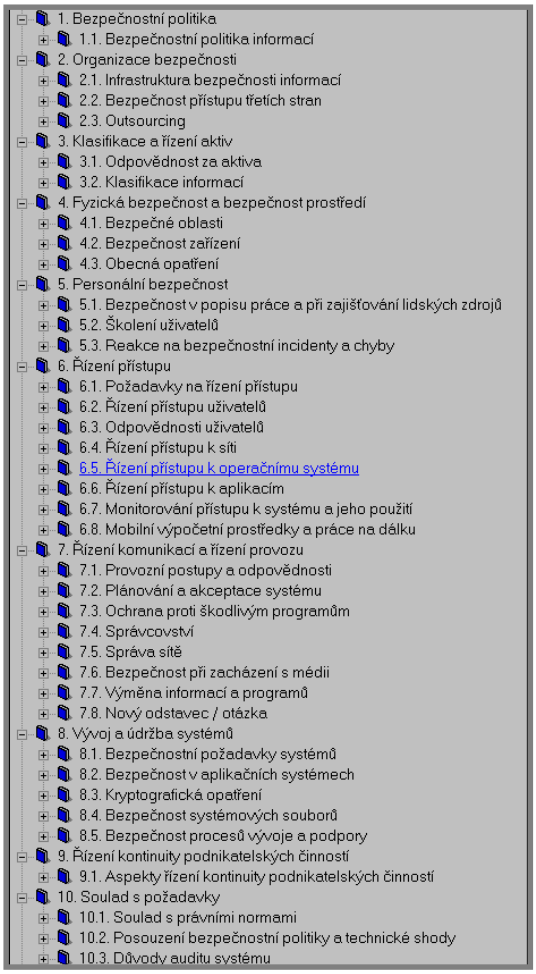
V minulém povídání jsme si povídali o tom, že základním krokem k dosažení bezpečnosti informací je stanovení klíčových bezpečnostních cílů, které chceme v organizaci dosáhnout. Vyjasnili jsme si, že optimálním způsobem je definování bezpečnostní politiky a její schválení nejlépe vrcholovým managementem. Také je nám jasné, čeho všeho by se taková bezpečnostní politika měla týkat. Teď už jenom zbývá vyřešit, jak bezpečnostní cíle, které jsou v bezpečnostní politice krásně stanoveny, dosáhnout, zrealizovat.

12. Přehledová analýza

Abychom mohli začít něco smysluplně budovat, měli bychom zjistit, jak na tom s bezpečností informací vlastně jsme. Donedávna to byl docela problém, každý posuzoval bezpečnost podle svého (nejčastěj podle toho, jak intenzivně bylo používané šifrování). Nebylo zřejmé, podle čeho vlastně posuzovat, zda bezpečnost informací je dobrá, dostatečná, odpovídající situaci nebo požadavkům. Navíc nebylo žádného srovnání.

Velice často jsem se setkával s otázkou klientů: "Jsme na tom s bezpečností informací hůř než jinde (ve světě)?" Intuitivně se odpovědět dá, ale k objektivnosti mají takové závěry daleko. I to byl jeden z významných důvodů, proč již minule zmiňovaná norma ISO/IEC 17799 nalezla tak rychle místo v systému zajištění bezpečnosti informací. Popisuje totiž ty nejlepší zkušenosti a doporučení, jak by měla být bezpečnost zajištěna. Stala se jakýmsi prvním "pevným" srovnávacím bodem -

etalonem. Navíc není rigidní, naopak, základním pravidlem je posouzení oprávněnosti jednotlivých bezpečnostních požadavků v daných konkrétních podmínkách a případně stanovení požadavků nových nebo



dodatečných. Takže to není šablona, ale spíše návod, ke kterému je nutné přistoupit s rozumem a tvůrčí invencí.
Zjištění aktuálního stavu v zabezpečení informací je nesmírně důležité. Je to jako poznání základů, na kterých chceme založit stavbu. Způsobů, jak zjistit aktuální stav je několik, doporučenou metodou je takzvaná "Gap" analýza (analýza nedostatků, rozporů s doporučeními). Tady je právě výhodné použít ISO/IEC 17799 jako to správné doporučení, jako srovnávací platformu, která nám stanoví základní východiska pro zjištění míry bezpečnosti informací.
Pro ilustraci rozsahu takové analýzy je na obrázku uvedena základní struktura požadavků, které jsou při Gap analýze podle zmíněné normy posuzovány.
Na tomto místě není podstatné, jakým způsobem se taková přehledová analýza provádí. Důležité je si uvědomit její účel - před zahájením systematických prací v oblasti zajištění bezpečnosti informací je zjištění aktuálního stavu prvním krokem k úspěchu.

13. Zpětná vazba

Jestliže chceme systematicky přistoupit k řešení bezpečnosti informací, musíme jednoznačně stanovit po každém kroku míru a sílu zpětných vazeb. Nejedná se o nic jiného než o určení toho, jakým způsobem ovlivňují poznatky, které zjistíme v každém následujícím kroku předpoklady, ze kterých jsme vycházeli.
V případě přehledové analýzy se jedná o mechanizmus, který nám umožní provést korekce celkové bezpečnostní politiky organizace na základě výsledků přehledové analýzy.
V praxi se jedná o to, že když necháváme vrcholové vedení organizace schválit dokument, který se nazývá "Bezpečnostní politika", musíme si být vědomi (a nejenom my, ale hlavně i samotné vedení) toho, že to není dokument neměnný, ale živý.
Dokument, který musí neustále odrážet aktuální situaci. Je jen přirozené, že např. taková přehledová analýza může přinést nové poznatky, které by bylo vhodné do politiky začlenit.
Použití zpětné vazby je zjevně velice důležité. Mimo jiného z toho vyplývají i požadavky na takové věci, jako je např. rozsah bezpečnostní politiky. Dobře všichni víme, že vedení se nebude neustále zabývat dokumentem, který rozsahem přesahuje objem, který je ochotno čas od času číst (a schvalovat). I z toho vyplývají požadavky na rozsah bezpečnostní politiky. Někdy se dokonce doporučuje, aby měla jen několik stránek (2-3).
Má to hned několik výhod:
a) vedení organizace by nemělo být "zatěžko" se dokumentem v případě potřeby opětovně zabývat a aktualizovat jej;
b) v krátkém a výstižném dokumentu je politika popsána natolik globálně, že ani nebude vyžadovat časté aktualizace;
c) takový dokument může být veřejný, může to být veřejné prohlášení organizace o tom, jak důležitá je pro ní informační bezpečnost.
Princip zpětné vazby je důležité realizovat v průběhu celého procesu zajištění bezpečnosti. Reálně to znamená, že každý krok, dokument, předpis, metoda, postup by měl mít stanoveno, co ovlivňuje jeho platnost a měly by být stanoveny příčinné nebo časové podmínky, které vyvolávají nutnost jeho revize a aktualizace.
Abych byl ještě konkrétnější a odpoutal se od řeči předpisů. Představme si, že na základě dalších analýz zjistíme, že například pro zabezpečení konstrukční dokumentace podniku budeme potřebovat nasadit (kromě jiného) k ověření přístupu k systému "silné" heslo (např. náhodná kombinace 12 alfanu-

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

merických znaků s vynucenou změnou každý měsíc). Abychom ale zajistili spolehlivost zabezpečení musíme určit, jak dlouho takový požadavek bude platný nebo kritéria, která vedou k jeho nasazení. Situace se totiž může měnit hned v několika směrech. Může se ukázat, že příliš silné heslo vede k tomu, že lidé si jej začnou psát na papírky, že bezpečnost konstrukční dokumentace postupně ztratí v organizaci na prioritě, nebo se objeví nové slabiny operačního nebo aplikačního systému a silné heslo, které určitě způsobuje nemálo komplikací, ztratí smysl.
Dobře nastavená pravidla zpětné vazby mají velký vliv na účinnost a efektivnost veškeré naší snahy o zajištění bezpečnosti informací. Nejenom ve vztahu ke globálním předpisům, jako je bezpečnostní politika, ale i ke konkrétním technickým bezpečnostním opatřením.

14. Analýza rizik

Dostáváme se k podstatnému kroku zavádění systematického přístupu k zajištění bezpečnosti informací. Kroku, který nám dá odpověď na otázku, která opatření je vhodné použít k tomu, abychom bezpečnost informací zajistili cíleně, dostatečně a také ekonomicky efektivně. Analýza rizik informačních systémů je poměrně složitý systém, který asi není podstatné podrobně popisovat.
Pro správné pochopení podstaty si však vyjasníme základní pojmy, se kterými jste se možná již setkali a které se budou dále vyskytovat:
a) aktivum je to, co je předmětem chráněného zájmu. To nejcennější, co chráníme, jsou zřejmě data a služby nebo procesy, které jsou informačním systémem poskytovány nebo zpracovávány. Je to to, proč si vlastně IS pořizujeme. Data a služby jsou tedy zpravidla těmi nejcennějšími aktivy. Přirozeně, že existují i další aktiva, jako jsou například aplikační programy, operační systémy, hardware, komunikace, podpůrná zařízení (klimatizace servrovny, záložní zdroje apod.)
b) hodnota aktiva je pojem, který charakterizuje důležitost aktiva pro organizaci. Může být vyjádřena mnoha způsoby, např. finančně. Toto vyjádření se používá v metodikách analýzy rizik, používaných zejména na americkém kontinentu. V Evropě je zvykem používat vyjádření spíše relativní, protože ne vše se dá penězi vyjádřit. Co je ale důležité a společné pro oba způsoby vyjádření hodnoty aktiv je to, že charakterizují to, co se stane, když aktivum nebude k dispozici, bude prozrazeno nebo pozměněno. V principu je pak jedno, zda míra takového dopadu je vyjádřena penězi nebo nějakým jiným číslem.
c) hrozba je pojem, který charakterizuje nebezpečí, které může působit na náš informační systém. Při analýze rizik je nutné zvažovat velice různorodé druhy hrozeb. Jenom pro příklad toho, nakolik komplexně se při analýze rizik posuzují jednotlivé druhy hrozeb, uvedu namátkově několik jejich druhů: falšování uživatelské identity zaměstnanci, smluvními partnery nebo cizími osobami (falešné přihlášení se do systému), viry, několik způsobů manipulace s komunikačnímu kanály (odposlech, selhání, ...), technické závady, selhání napájení, zneužití systémových prostředků, chyby v programech, provozní chyby, chyby v obsluze, servisní chyby, požár, přírodní katastrofa, terorizmus, nedostatek personálu, poškození vodou, krádež, ...
d) dopad je druh následku, který může způsobit uplatnění určité hrozby. Obecně je dopad charakterizován porušením jednoho ze tří základních atributů bezpečnosti informací - dostupnosti, integrity a důvěrnosti. Míra dopadu (a tím narušení uvedených atributů) je různá a tím i stupnice pro hodnocení může být značně rozsáhlá.
e) riziko charakterizuje pravděpodobnost výskytu porušení základních atributů bezpečnosti informací. Opět může být vyjádřeno jako pravděpodobnostní veličina nebo jako nějaká odpovídající hodnota (například akceptovatelné, malé, střední, velké, kritické)
Aby analýza nebyla tak jednoduchá, do hry vstupují mnohé další vazby. Jako příklad jenom uvedu, že ne všechny hrozby mohou působit na všechna aktiva, některé hrozby působí jenom na určitá aktiva, určité hrozby mohou vyvolat jenom některé specifické dopady apod. Takže situace se nám pomalu komplikuje.
Postup analýzy rizik může být následující. V první fázi se namodeluje struktura a závislosti jednotlivých aktiv a určí se jejich hodnota. V další fázi se posuzují jednotlivé hrozby a míra jejich možných dopadů na jednotlivá informační aktiva organizace. V poslední fázi se určuje riziko, jako určitá funkce hodnoty aktiva, hodnoty hrozby a míry dopadu. Výsledkem je podrobný přehled rizik působení určitých hrozeb na určitá aktiva organizace.

15. Řízení rizik

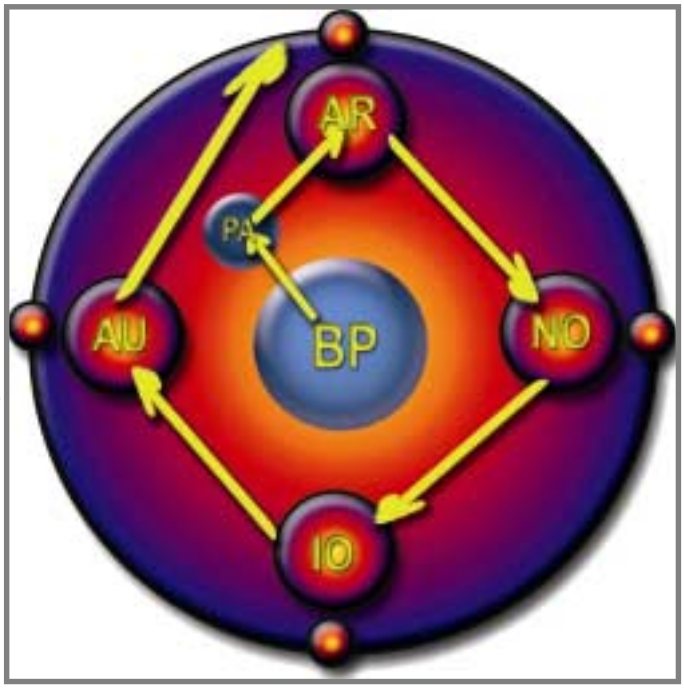
Zjištění rizik je však pro zajištění bezpečnosti informací málo. To důležité, co by mělo být výstupem analýzy rizik, je právě

V020611

návrh bezpečnostních opatření, která se snaží zjištěná rizika eliminovat. **Tady je tedy ta základní odpověď na otázky účelnosti, dostatečnosti a efektivnosti bezpečnostních opatření.**
Primárním pravidlem výběru bezpečnostních opatření je skutečnost, že nelze zajistit absolutní bezpečnost.
Než začneme vybírat opatření, musíme udělat v organizaci zásadní rozhodnutí o míře rizika, která bude pro nás akceptovatelná. Jestliže některá rizika, která jsme analýzou rizik definovali, jsou nižší, než je námi akceptovatelná míra, nebudeme se jimi primárně zabývat. Tím jsme vlastně již vyloučili potenciálně značnou skupinu opatření, které by z hlediska organizace bylo vlastně zbytečné zavádět.
To je první a podstatní přínos analýzy rizik - **zabývat se pouze těmi riziky, která jsou neakceptovatelná**.
V dalším kroku řízení rizik si musíme uvědomit, že opatření, která připadají do úvahy, mají různou míru účinnosti a různou nákladnost. Nezapomínejme při tom, že jsme si stanovili akceptovatelnou míru rizika a nebylo by příliš efektivní, vybírat na jeho eliminaci opatření, která třeba několikanásobně převyšují svojí účinností potřebnou hranici.
Navíc je potřebné zvažovat skutečnost, že k eliminaci určitého rizika na akceptovatelnou úroveň lze obecně vždy použít několik opatření. Mnohé z nich navíc nepůsobí pouze na jedno riziko, ale na několik rizik současně a je možné takovým způsobem vytvořit synergický efekt, kdy k eliminaci určitého rizika postačují dvě jednoduchá opatření místo jednoho nákladného.
Druhým podstatným přínosem analýzy rizik je, že pro jejich eliminaci jsme schopni vybrat a navrhnout **pouze taková opatření, která mají dostatečnou (tj. odpovídající riziku) účinnost k tomu, aby je snižovala na akceptovatelnou úroveň, co největší záběr napříč riziky a co nejmenší náklady na realizaci.**
Asi zjevnou podmínkou takového řešení je existence systematizované základny opatření, které lze pro eliminaci rizik použít, včetně toho, že všechna taková opatření jsou ohodnocena z hlediska nákladnosti, účinnosti a šířky záběru.
Jakého jsou charakteru ta opatření, která spadají do úvahy? Když si je promítneme do struktury požadavků na bezpečnost, které stanovuje doporučení v normě ISO/IEC 17799 uvidíme, že mohou být organizačního, personálního, technického a programového charakteru. Obecně platí, že opatření organizačního charakteru jsou nejlevnější, opatření personálního zase nejúčinnější.

16. Ještě jednou zpětná vazba

Důležitost zpětné vazby jsem už jednou zdůrazňoval. Po zdárném absolvování analýzy rizik, zodpovědném výběru bezpečnostních opatření a jejich implementaci je nejvhodnější doba k tomu, abychom si prověřili, zda naše práce byla úspěšná. K tomu slouží audit bezpečnosti.



Nejspíše by se dalo najít mnoho dalších účelů, ke kterým lze audit využít, ale tím primárním je právě uzavření "zpětnovazebné smyčky". Zajištění bezpečnosti informací totiž není lineární proces, který by měl svůj začátek v bezpečnostní politice a konec v implementaci opatření. Je to nekonečný proces, který lze nejjednodušeji popsat obrázkem. Začínáme bezpečnostní politikou (BP), pokračujeme přehledovou analýzou (PA), pak následuje analýza rizik (AR), návrh opatření (NO), jejich implementace (IO) a cyklus se uzavírá auditem (AU). Pak už následuje uzavřený cyklus pouze s tím rozdílem, že jestliže ve fázi zavádění systému řízení bezpečnosti informací jsou všechny kroky provedeny v plném rozsahu (proto i náklady na ně jsou vyšší) a v dalších cyklech se provádí pouze rozdílové analýzy (to jsou ty malé satelity po obvodu obrázku).
Při každém z uvedených kroků nesmíme zapomínat na to, co již bylo uvedeno u zpětné vazby v úvodu. **Jakákoliv naše činnost totiž ovlivňuje nejenom kroky násle-**

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

dující, ale má vliv i na východiska, která se novými poznatky mohou měnit, korigovat.

17. Kdy se to vyplatí?

To co bylo výše řečeno silně zavání teorií a na první pohled není zřejmé, k čemu to všechno vlastně je. V případě relativně a jednoduchých systémů je takový model analýzy rizik zbytečně složitý, ale jakmile se dostaneme na počty aktiv řádově několik desítek, už nelze empiricky postihnout všechny vztahy a vazby mezi aktivy, hrozbami, dopady a opatřeními. Právě tady končí efektivnost empirického přístupu k bezpečnosti informací a vyvstává nutnost použít některý ze systematických přístupů.
Při úvahách o tom, kdy je efektivní přejít na systematické řízení bezpečnosti informací, je odpověď jednoduchá - vždy! Otázkou pouze zůstává, jakým způsobem, jaký systém, program si zvolit, aby odpovídal důležitosti a rozsahu IS organizace.
Pro volbu způsobu zavádění systému řízení bezpečnosti informací může posloužit srovnání podílu nákladů na bezpečnost v poměru k celkovým nákladům na provoz informačního systému. Podle našich i mezinárodních zkušeností se náklady na bezpečnost při nesystémovém způsobu řízení (za předpokladu zajištění dostatečné úrovně bezpečnosti) pohybují až do 20% celkových nákladů. Většinou ale není bezpečnost zajištěna a bezpečnostní náklady jsou u mnoha organizací minimální. O to horší je situace v případech porušení bezpečnosti, kdy následky mnohonásobně převyšují jakékoliv náklady a mnohdy jsou pro organizaci tragické (už jsem o tom mluvil v první části s odkazem na “2001 CSI/FBI Computer Crime and Security Survey”). Při rutinním provozu systematického řízení bezpečnosti informací náklady na klesají až na 3 - 5 % celkových provozních nákladů.
Důležitá je zkušenost o míře nákladů na samotné zavedení systému řízení bezpečnosti informací. Přirozeně, že když se do bezpečnosti neinvestuje průběžně, deficit bezpečnosti se kumuluje a pak jsou prvotní náklady značné. Průměrné informace hovoří o částce 25 - 50% z celkových ročních provozních nákladů v průběhu jednoho až tří let (podle složitosti systému). Pak si už relativně jednoduše můžeme spočíst, kolik nás zavedení systematického přístupu k řízení bezpečnosti bude stát a kdy se nám to v nákladech vrátí.
Příklad (hodně zjednodušený): při ročních provozních nákladech 100 tis., předpokladu “nesystematických” ročních investic do bezpečnosti 15 tis. (vysoká požadovaná míra bezpečnosti) a nákladů na zavedení systematického přístupu 30 tis. na dva roky je předpoklad návratnosti 5 let, přičemž další náklady na bezpečnost mohou klesnout pod 5% celkových provozních nákladů.
Navíc získáme výhodu toho, že bezpečnost informací budeme mít pod kontrolou! Implementace systému řízení bezpečnosti informací není levnou záležitostí. Předchozí úvahy o nákladech jsou výrazně ovlivněny i tím, ve které fázi životního cyklu informačního systému se začneme systematicky jeho bezpečností zabývat. Asi nemusím zdůrazňovat, že čím dřív, tím lépe a levněji. Zajištění bezpečnosti informací je obecně záležitost preventivní. Z tohoto pohledu je přirozené, že investice do bezpečnosti si nemůže dovolit každý v takovém rozsahu, jaký by si zasluhovala. Je to skutečně pouze otázka peněz?
V případě, že pozice organizace je výslovně regionální, tak asi ano. Současná podnikatelská atmosféra u nás asi na bezpečnost informací nehledí tolik, kolik by si to tato problematika zasloužila. Je to škoda, protože čím později, tím se to bude hůř dohánět. Z druhé strany je to pochopitelné, většina má spoustu jiných starostí.
Nový rozměr nabývá bezpečnost informací, když se začínáme rozhlížet za hranice. Tam je konkurence mnohonásobně vyšší a každé plus, které může pomoct, je dobré. V těchto případech může být návratnost investic do bezpečnosti informací mnohonásobně vyšší. Mezinárodní srovnávací norma k tomu existuje a není v podstatě nic jednodušší, než ji aplikovat. Snaha o co nejlepší uplatnění v mezinárodním měřítku (a EU nám klepe na dveře) může být tím dalším impulsem, který může management společnosti zvažovat při rozhodování, zda, kdy a jak k systémovému zajištění bezpečnosti informací přistoupit.

ČÁST IV

18. Dost bylo předpisů?

Předminule jsem proces zajištěni bezpečnosti informací přirovnával k systému zajištění kvality (podle ISO 9000). Každý, kdo to absolvoval ví, že značnou část procesu tvoří objemem nemalá dokumentace, na všechno jsou vytvořeny předpisy a postupy, všechno je dokumentováno. I pro systematické zvládání bezpečnosti informací je charakteristická tvorba rozsáhlé bezpečnostní dokumentace. Od již zmiňo-

vané bezpečnostní politiky, přes směrnice pro výkon personální práce, fyzického zajištění IS, postupy pro přidělování uživatelských oprávnění, pro zálohování, havarijní plány a spousta dalších.
Normy, politiky, směrnice, analýzy, metodiky - je to vůbec k něčemu? Jen jsme se zbavili různých nesmyslných předpisů a oběžníků, které nám dlouhá léta otravovali život a které stejně téměř nikdo nečetl, už vám vnucuji zase nějaké "papíry", které zase nikdo nebude číst...
Ti z vás, kdo děláte v podnicích se zahraničním vlastníkem (a zejména americkým) asi víte o čem mluvím. Pro takový systém řízení je typické, že veškerá činnost každého zaměstnance je popsána, každý má přesně vymezené pracovní místo a pracovní povinnosti. Není moc prostoru na iniciativu ba naopak, iniciativa se většinou přímo nevyžaduje, záměrem je maximální zvyšování produktivity každého jednotlivce. Někdy je tento systém doveden do takového extrému, že kdyby jste si v levném americkém motelu sami nahodili jističe, které se vám povedlo nedopatřením vyhodit kávovarem a které jsou navíc přímo ve vašem pokoji za dveřmi, koukali by na vás divně (možná proto, že jste tím připravili místního údržbáře o pracovní úkon, který si on na předepsaném tiskopisu CX-251 denně vykazuje). Druhý extrém je, když zaměstnanci rámcově ví, co se od nich čeká a zbytek je ponechán na jejich iniciativě. Obecně nelze říci, že ten či onen přístup je lepší nebo horší. V mnohém to závisí od předmětu podnikání, způsobu řízeni, kvalitě personálu, ... Ať tak či onak, jsou určité oblasti, které přímo vyžadují formální zakotvení v systému činnosti organizace. Jenom pro příklad uvedu mojí nedávnou diskusi o účelnosti plánů obnovy funkčnosti IS. V rozhovoru s představiteli pobočky jedné banky, která byla postižena povodněmi, jsme dospěli k zajímavému závěru: první, co se zachraňovalo, byly právě zmiňované plány. Ty byly vyneseny ze sklepa, kde byl archiv, do nejvyšších pater. Pak se již postupovalo, aniž by někdo do těch plánů nakoukl. Když se pak vyhodnocovala činnost pobočky při povodních bylo zjištěno, že IS byl obnovován přesně v souladu a podle havarijních plánů. Že by ty plány byly zbytečné? Vůbec ne, rychlé obnovení takového systému není hračka a povedlo se to jen díky pravidelným aktualizacím havarijních plánů a díky proškolování. Proto všichni kompetentní zaměstnanci věděli co mají dělat a plány jako takové vlastně ani nepotřebovali.
Zmíněný příklad je o tom, že vypracování bezpečnostní dokumentace je pouze jedním z nezbytných kroků k zajištění bezpečnosti informací. V konečném důsledku není podstatné, jak podrobnou a rozsáhlou dokumentaci máte zpracovanou, důležité je, aby každý zaměstnanec znal své místo, práva a povinnosti ve vztahu k bezpečnosti informací a jednal podle toho. Bezpečnost informací není o tom, kolika centimetrovou dokumentaci předložíte řediteli, akcionářům nebo auditorům. Je to o tom, aby dokumentace byla natolik systematická a dostatečná, aby se podle ní zaměstnanci naučili odpovídajícím způsobem k informačním aktivům organizace chovat. Aby rozumnou mírou zapadla do úrovně vnitrofiremní kultury, byla dostatečně komplexní a účinná.

19. Když bezpečnost selže

Nemalou roli v zajištění bezpečnosti informací má jasné rozdělení kompetencí. Nejasné vymezení činností jednotlivých odpovědných pracovníků může vést ke katastrofálním následkům. Není nic horšího, než když se v kritické situaci dohadují

	Akceptovatelné riziko	Příklad
1.	**Škody, které incidenty mohou způsobit, jsou „přijatelné".**	Můžeme se rozhodnout nenasazovat antivirové prostředky na personální systém, protože je dostatečně oddělen od ostatní sítě, je pravidelně zálohován, dublován v papírové podobě a personál je kvalitně proškolen právě ve vztahu k virové problematice. Navíc tento systém není pro nás kritický co do požadavku na funkčnost v reálném čase a tudíž škody způsobené případnou virovou infekcí lze považovat za minimální.
2.	**Náklady pro eliminaci rizika jsou v současnosti příliš vysoké.**	V daný moment může být neúnosně nákladné přejít z důvodů požadavků na silnější autentizaci z Windows95/98 na Windows2000 Nejenom z hlediska nákladů na upgrade operačního systému, ale zejména z hlediska nákladů na inovaci počítačů
3.	**Pravděpodobnost výskytu incidentu je velmi nízká.**	Bylo by neefektivní vynakládat prostředky na zabránění vzniku incidentu. Typickými málo pravděpodobnými bezpečnostními incidenty mohou být živelné pohromy (požár, povodeň), teroristický útok, vandalství, pád letadla apod.

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

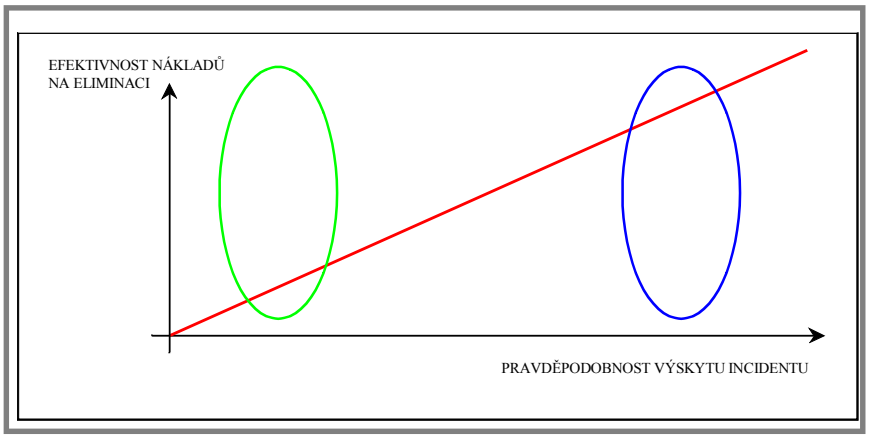
dostatečně vysoce postavení funkcionáři, co je nejlepší právě udělat a každý si prosazuje svou pravdu silou své pozice nebo svého platu.

Kritické situace jsou těmi nejlepšími zatěžkávacími zkouškami, které prověřují celý systém. Je nám už jasné, že přes veškerou snahu a investice nelze zajistit absolutně bezpečný informační systém, že vždy bude existovat určité zbytkové riziko. O akceptovatelné míře rizika, které jsme se rozhodli neřešit, jsme nakonec mluvili v minulé části.

Když jsme se už jednou s plným vědomím rozhodli, že určitá rizika budeme akceptovat, jsme si tím vědomi, že bezpečnostní incidenty nastat mohou, ale my se s tím smíříme. Příklad takových akceptovatelných rizik je uveden v tabulce

Důležité a podstatné je to, že po dobře provedené analýze rizik víme docela přesně, jaké druhy nebo skupiny bezpečnostních incidentů můžeme potenciálně očekávat. Víme dokonce, do které z výše uvedených skupin spadají a můžeme se na ně odpovídajícím způsobem připravit. Celý systém řízení bezpečnosti informací tak můžeme doplnit o důležitou kapitolu, která se jmenuje **reakce na bezpečnostní incidenty.**

Část bezpečnostní dokumentace, který se zabývá reakcemi na bezpečnostní incidenty, bývá velice často opomíjena. Vychází ze skutečnosti, že **když už z různých důvodů nemůžeme rizika eliminovat, je nutné se připravit tak, aby dopady z případných bezpečnostních incidentů byly minimální.** Pro dokreslení situace lze použít graf. V modrém oválu je část pod červenou linkou oblastí, kde jsou rizika pokryta bezpečnostními opatřeními a část nad linkou je nepokryta. V zeleném oválu se poměr pokrytých a nepokrytých rizik obrací. Tam je efektivní použít plánování reakcí na bezpečnostní incidenty.



Dobrým příkladem plánování reakcí na bezpečnostní incidenty může být oblast **plánování obnovy funkčnosti IS**. I havárie (např. požár) je z pohledu teorie bezpečnosti informací vlastně “jen” bezpečnostní incident, u kterého dochází ke skokové absolutní ztrátě minimálně jednoho ze základních bezpečnostních atributů - dostupnosti informací. Proto se někdy mluví také o havarijním plánování.

Kdybychom se podívali do literatury (která je u nás zatím bohužel k sehnání pouze v originálu - většinou v angličtině) která se cíleně oblastí havarijních plánů zabývá, zjistili bychom, že východiskem pro dobrý havarijní plán (připusťme na chvíli, že plán obnovy funkčnosti IS = havarijní plán) je provedení tzv. analýzy dopadů na podnikatelské procesy (**Business Impact Analysis - BIA**). BIA je analýza, výsledkem které je, velice zjednodušeně řečeno, pořadí důležitosti a požadavky na lhůty obnovy jednotlivých IS. Je to nalezení takové časové hranice, kdy nedostupnost některého z IS způsobí neakceptovatelné (velmi výrazné nebo až katastrofické) dopady na podnikatelské záměry organizace. **Cílem havarijních plánů je pak nalézt způsob, jak obnovit alespoň v minimálním přijatelném rozsahu funkčnost IS v pořadí jejich priority a s náklady, které nepřevýší škody, které by jejich nefunkčností hrozily**.

Stačí si jenom na chvíli představit, že potřebujete proto, aby vaše organizace po požáru vůbec “přežila”, zprovoznit alespoň některé důležité IS do tří dnů. Nemálo toho jste právě vy, kdo celou informatiku v organizaci stavěl na nohy a ví, kde který kabel vede a kde jsou které instalačky a zálohy, na zasloužené dovolené někde na neurčitém místě “pod širákem”. Bez podrobného postupu zprovoznění klíčových IS to prostě možné není. V takových případech musí být předem stanoveno, kde se bude provizorně IS uvádět do provozu, kde a jakým způsobem se sežene náhradní HW, jak se provizorně natáhnou sítě, jak se budou instalovat systémy a aplikace a obnovovat ze záloh data. Ale nejenom to, musí být odzkoušena a natrénována i časová posloupnost jednotlivých kroků, protože v kritických případech a při časovém presu je každá hodina tápání, prostojů nebo pokusů výraznou ztrátou.

V020611

Jistě také chápete, že tohle už není jen záležitost informatiky, ale musí se na tom podílet prakticky každý a tedy bez toho, aby to bylo naplánováno, koordinováno a hlavně i schváleno vedením organizace, to asi už nepůjde. A ještě jednou zopakuji, že snad nejdůležitějším faktorem je jasné (myslím tím i vedením organizace odsouhlasené) vyjasnění si kompetencí.
O plánování obnovy funkčnosti by se dalo mluvit dlouho. Mnohem častěji než s haváriemi se ale v praxi setkáváme s menšími a mnohdy neméně nebezpečnými bezpečnostními incidenty. I tady obecně platí stejné pravidlo: musíme být na incidenty předem připraveni. Dobře provedená analýza rizik nám k tomu vytváří všechny základní předpoklady.

20. Turecké hospodářství a závěr

Za svojí praxi jsem se setkal již s mnoha přímo absurdními situacemi. Např. když pracovník byl kárně stíhán za to, že se mu v průběhu několika přestaveb jeho počítače někde ztratila redukce z 9 na 25 pinový sériový port. Jenom na popsaném papíře a poštovném se při řešení tohoto případu prodělalo víc. V žádném případě nenavádím k benevolenci nebo nepořádku, právě naopak. Když jsem vzpomněl ztracenou redukci, je to jednoznačně vzniklá škoda, která si **jako každá jiná** zaslouží vyřešení (ale vzhledem k její marginální výši pouze z principiálního hlediska a způsobem, odpovídajícím její výši a konkrétní situaci).
Při provádění auditu plánů obnovy funkčnosti IS jsem se prakticky vždy setkal u klientů s udivenou reakcí na otázku, zda mezi prostředky, které budou při procesu obnovy IS potřebovat, mají i kameru nebo alespoň fotoaparát. Co to má prý s IS společného!
Mnoho. Mohu zodpovědně prohlásit, že prakticky nikdo si tuto souvislost neuvědomuje. Ztracenou redukci každý automaticky vyhodnotí jako škodu, ale málokdo si už dá do souvislosti bezpečnostní incident (a je jedno, zda to je zavirování počítače, technická závada pevného disku nebo průnik hackera z Internetu do interní sítě) s pojmem škoda. Škody přitom vznikají, a nemalé. Jen si spočtěte, co vám to dá práce, než odvirujete jeden počítač. A v případě, že to nejde, musíte reinstalovat systém, aplikace, obnovovat data, navíc zkontrolovat, zda se vir nerozšířil do celé sítě. Než to uděláte, dotyčný nešťastník, co počítač zaviroval, nedělá a kouká vám pod ruky. Minimálně hodina jeho i vaší práce. Spočetl si někdo, co stojí organizaci jen dvě hodiny na mzdách? (Já vím, že by se dalo říct, že při výši vaší mzdy to snad ani nestojí za řeč.) A vy přitom jednoznačně víte, že dotyčný si zavirování počítače způsobil sám.
Byl to jenom banální případ zavirovaného počítače. Velice často jsou bezpečnostní incidenty mnohem závažnější a způsobují mnohem větší škody. Přesto je nikdo neřeší a jaksi "automaticky se odepisují" s konstatováním, že v IS se to přece stává. (To jenom Bill Gates naučil celý svět, že restartování počítače patří k samozřejmosti jeho fungování a když teď W2k už tolik nepadají, považuje se to ne za samozřejmost, ale velký úspěch tvůrců!)
Řešení bezpečnostních incidentů má podle všech stávajících doporučených postupů následující základní kroky:
a) odhalení incidentu (jsme vůbec schopni odhalit incident a odhalit jej včas?)
b) zamezení incidentu (jak rychle a dobře jsme schopni incident zastavit?)
c) obnovení funkčnosti (jsme schopni obnovit funkčnost systému po incidentu a jak rychle a spolehlivě?)
d) ponaučení se (jsme schopni analyzovat příčiny incidentu a přijmout taková opatření, aby se už neopakoval?)
Ponaučení se z incidentu však nemůže být pouze technického rázu (nemůže to být jenom zajištění pravidelné aktualizace antivirového prostředku na zavirovaném počítači). Každý bezpečnostní incident musí být zadokumentován dvojím způsobem:
a) z pohledu technického, aby se mohla přijat technická opatření k zamezení jeho opakování,
b) z pohledu procesního, aby bylo možné právně prokázat příčiny a původce jeho vzniku.
Jen tak je potom možné se snažit původce postihovat a škodu případně vymáhat. Na první pohled se to zdá být téměř nerealizovatelné. Ale jenom na první pohled.
Prostředky a metody k takovému postupu jsou už dlouho známé. Jestliže stávající systém a existující mechanizmy jsou schopny postihovat takovou absurditu, o jaké jsem se zmínil v úvodu, určitě stojí za to nasadit prostředky a metody, které odpovídají charakteru a povaze problematiky informačních technologií a jsou tím schopny postihnout i situace, na které je stávající systém "klasického účtování" neuzpůsoben. Protože už teď platí, že HW a SW sice mají svojí (účetní) hodnotu, ale informace jsou a v krátké budoucnosti ještě více budou klíčovým aktivem celé společnosti.
Začněme si už konečně uvědomovat, že informace mají nenahraditelnou hodnotu a učme se je chránit.

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