1. díl: Jak začít?

Informační bezpečnost v praxi

Petr Nádeníček

Témata týkající se zajištění dostatečné úrovně informační bezpečnosti organizace patří mezi často diskutovaná. Bohužel se tak děje spíše na „teoretické“ úrovni. Prosazení konkrétních bezpečnostních opatření a procesů do praxe pak ve valné většině případů selhává. Většinou se řeší pouze zabezpečení samotných informačních technologií, ale neméně důležitá opatření v oblasti organizační bezpečnosti se ztrácí ve zmatcích hierarchie organizace.

Pokud přihlédneme k aktuálnímu prostředí, které je silně ovlivněno trvající ekonomickou krizí, nemůžeme přehlédnout její vliv na zajištění informační bezpečnosti. I když ještě na začátku tohoto roku renomované expertní autority předpokládaly, že změněná ekonomická situace nebude mít na segment ICT bezpečnosti žádný negativní vliv a predikovaly jeho pokračující růst, dnes již většina expertů jasně vidí, že se znatelné škrty v rozpočtech organizací nevyhnuly ani jemu. Nic na tomto faktu nezměnily ani logické argumentace bezpečnostních odborníků postavené na oprávněně předpokládaných nárůstech specifických hrozeb, jako jsou například nespokojení nebo propuštění zaměstnanci, a z nich vyplývajících rizik. Překlad těchto argumentů do jazyka finančních částek, kterým mluví většina členů vrcholných manažerů organizací, asi není tak jednoduchá...

Z pohledu bezpečnostního konzultanta, který v tuzemských firmách a organizacích pomáhá identifikovat stávající stav zabezpečení, navrhovat vhodná protiopatření směrovaná proti nejvýznamnějším hrozbám, implementovat je a ověřovat jejich účinnost, je vliv ekonomické krize patrný mimo jiné i v nastavení priorit samotných bezpečnostních projektů. Jednoduše řečeno, pokud vůbec organizace bezpečnost nějak aktivně řeší, vede ji úbytek prostředků k realizaci spíše jen nezbytných bezpečnostních opatření, případně těch, které nevyžadují velké investice nebo přinášejí „okamžitý viditelný efekt“.

V tomto a následujících dvou článcích se zamyslíme nad tím, jak v současné situaci při řešení informační bezpečnosti postupovat, kterým úskalím věnovat pozornost a jak se s nimi vypořádat. Řekneme si, jak identifikovat aktuální stav bezpečnosti, jak definovat vhodná opatření, jak je uvést do života a jak ověřit jejich fungování. Pokusíme se při tom udržet kontext s prostředím „běžné české firmy“ střední velikosti a upozornit na kritická místa podmiňující úspěšnost našeho snažení.

S čím začít

Dejme tomu, že jsme ve firmě, jejíž osvícené vedení došlo k závěru, že je třeba systematicky řešit problematiku informační bezpečnosti, a to nejlépe v duchu implementace ISMS (information security management system – systém řízení informační bezpečnosti).

Zde musíme bohužel podotknout, že výše uvedený předpoklad je v praxi spíše výjimkou než pravidlem. V praxi tato iniciativa daleko častěji vychází z nižších úrovní managementu, případně přímo z řad pracovníků IT oddělení, a u členů vedení je pak s obtížemi prosazována. Smutnou realitou většiny organizací je, že informační bezpečnost se začíná řešit až v okamžiku, kdy došlo k nějakému „průšvihu“, který se v horším případě citelně projevil na jejím mediálním obrazu (viz nedávný incident s únikem osobních údajů klientů z nedostatečně zabezpečené webové aplikace jedné nejmenované pojišťovny). Účinná (ne jen formální) podpora vedení aktivitám informační bezpečnosti je

přitom klíčovou, ne-li nezbytnou podmínkou úspěšného zavedení bezpečnosti do prostředí organizace. Nedůslednost v oblasti bezpečnosti může vést až k porušování platné legislativy, která v řadě případů zabezpečení určitých informací přímo nebo nepřímo vyžaduje (např. zákon č. 101/2000 Sb., o ochraně osobních údajů), obchodních smluv (ochrana obchodního tajemství) apod.

Pokud je vůle pro řešení bezpečnosti, což zahrnuje i uvolnění nezbytných interních kapacit a samozřejmě také určitého objemu finančních prostředků, první činnosti by měly směřovat k identifikaci aktuálního stavu informační bezpečnosti organizace. Tato identifikace bývá zpravidla provedena formou bezpečnostní analýzy s různou hloubkou záběru, která může být dále doplněna o dílčí specifické prověrky technického, procesního nebo jiného rázu.

Běžně prováděné bezpečnostní analýzy vycházejí nejčastěji ze standardů, jako ISO/IEC TR 13335, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408 (Common Criteria) apod. V individuálních případech mohou být použity také jiné standardy, jako je například americký SOX, případně zohledněna i jiná hlediska, jako jsou například IT procesy podle ITIL, COBIT apod. Většinou neuděláme chybu, pokud se alespoň rámcově držíme základních oblastí bezpečnosti tak, jak je definuje norma ISO/IEC 27002:

- bezpečnostní politika,
- organizace bezpečnosti,
- klasifikace a řízení aktiv,
- personální bezpečnost,
- fyzická bezpečnost a bezpečnost prostředí,
- řízení komunikací a provozu,
- řízení přístupu,
- nákup, vývoj a údržba informačního systému,
- zvládání bezpečnostních incidentů,
- řízení kontinuity činností organizace,
- soulad s požadavky.

Rozčlenění na výše uvedené oblasti nám při provádění analýzy pomáhá udržet přehled a nezapomenout na nic podstatného. Co se týče jejich konkrétního obsahu, inspirujeme se zpravidla normou ISO/IEC 27002, která tvoří de facto katalog použitelných bezpečnostních opatření v daných oblastech.
V praxi můžeme v závislosti na potřebné hloubce záběru aplikovat tři základní typy bezpečnostní analýzy:

Bezpečnostní screening organizace

Jedná se o přehledový typ analýzy, která směřuje k poměrně rychlé identifikaci aktuálního stavu a definici hlavních bezpečnostních problémů, na které je třeba se v organizaci zaměřit. Její použití je vhodné zejména v menších firmách a v organizacích, kde dosud s bezpečností nemají žádné zkušenosti. Je založena na ucelené sadě dílčích auditů, kontrol a testů, které sice nejdou příliš do hloubky, ale jsou cíleny na nejčastěji se vyskytující typické problémy, což se logicky promítá i do menší časové, případně finanční náročnosti analýzy. Vhodnými pomůckami při realizaci jsou mimo jiné předem zpracované dotazníky, checklisty, automatizované testy technického zabezpečení informačního systému apod. Úspěšné provedení analýzy je také do značné míry závislé na míře podpory a aktivní spolupráce ze strany zodpovědných pracovníků organizace.

Analýza současného stavu informační bezpečnosti organizace

Tento typ analýzy přináší organizaci o něco detailnější pohled na slabá místa v jejím zabezpečení. Výstupem ale bývá kromě přehledu identifikovaných nedostatků i návrh doporučení na jejich odstranění, který je využitelný při plánování dalších kroků budování bezpečnosti. Přístup k provádění analýzy je podobný jako u formální analýzy rizik s tím rozdílem, že je vynechána, nebo velmi zjednodušena fáze identifikace aktiv organizace a formulace rizik. Směřuje se přímo k nalezení a popisu bezpečnostních nedostatků v rámci jednotlivých oblastí bezpečnosti. V rámci analýzy jsou využity jak vhodné technické testy cílené na identifikaci stavu technického zabezpečení informačního systému, tak interview s odpovědnými zaměstnanci, studium interní dokumentace a další aktivity směřující k identifikaci stavu organizační bezpečnosti a bezpečnosti v rámci jednotlivých obchodních a podpůrných procesů organizace. V porovnání s bezpečnostním screeningem je analýza současného stavu daleko více komplexní, ale logicky také časově a finančně náročnější. U malých a středních organizací může být použita jako víceméně plnohodnotná náhrada formální analýzy rizik.

Analýza rizik organizace

Analýza rizik představuje klasický formální přístup k posouzení aktuálního stavu bezpečnosti informačního systému organizace. Cílem je pomocí různých nástrojů a metod identifikovat jednotlivá aktiva informačního systému organizace a nalézt slabá místa informačního systému, tyto poznatky pak shrnout do definice konkrétních rizik a navrhnout managementu, či jiným odpovědným složkám, vhodná protiopatření. Ta mohou být zpracována přímo ve formě implementačního plánu a tvořit podklad pro další budování bezpečnosti v organizaci. Analýza by měla zahrnovat různé pohledy na organizační, administrativní, fyzickou, počítačovou a personální oblast bezpečnosti, které

Inzerce

Odborný seminář

Více informací na
www.controlling.cz

Controller-Institut
Controlling Finance Management

7.-8. 12. 2009, Brno

Finanční řízení pro neekonomy

...aneb podnikové finance v kostce

- Finanční výkazy a vazby mezi nimi
- Způsoby financování společnosti
- Pracovní kapitál, význam, využití
- Cena peněz, cenné papíry
- Investice - hodnocení efektivnosti
- Finanční analýza

Controller-Institut, Contrast Consulting Praha spol. s r.o.

Italská 26
120 00 Praha 2
Tel.: 224 314 410
www.controlling.cz
info@controlling.cz

mohou být dány také vnitřními požadavky organizace, legislativou apod. V rámci analýzy mohou být využívány různé metody sběru informací, jako jsou interview a workshopy s odpovědnými zaměstnanci organizace, technické prověrky sítí, audity dílčích systémů apod.

Řada lidí má v souvislosti s „analýzou rizik“ zafixovaný pojem CRAMM (CCTA Risk Analysis and Management Method), který představuje mimo jiné metodiku a nástroj pro provádění analýzy rizik. Není však určitě pravda, že by analýza rizik musela být prováděna pomocí CRAMMu, a to ani ve většině velkých organizací. Použití CRAMMu je značně finančně náročné (zakoupení licence, proškolení metodiků atd.). Pokud vezmeme v úvahu, že už samotná vstupní data zadávaná do CRAMMu mohou být často zatížena značnou odchylkou od skutečnosti, což se v důsledku musí projevit na výsledcích analýzy, postrádá ve většině případů jeho nasazení smysl. Kvalitní analýza rizik může být provedena i bez CRAMMu, například pomocí metodiky postavené na základech normy ISO/IEC TR 13335 a normách ISO/IEC 2700x. Daleko více záleží na zkušenostech konzultantů a jejich schopnosti identifikovat nedostatky a formulovat samotná rizika.

Všechny výše uvedené typy analýz mohou být provedeny jak vlastními zaměstnanci dané organizace, tak externími konzultanty. Snaha „ušetřit“ finanční prostředky tím, že si analýzu provedeme sami, však může mít určité negativní aspekty, je to například:

- provozní slepota interních zaměstnanců,
- snaha o záměrné účelové přehlížení určitých nedostatků interními zaměstnanci,
- nesnadné vyčíslení interních nákladů, které mohou být v důsledku větší než přímá finanční investice do externích konzultantů,
- určitý nadhled, nezaujatost a širší zkušenosti externích konzultantů.

Na druhé straně je třeba podotknout, že v případě, kdy máme k dispozici vlastní kvalitní konzultanty, kteří jsou schopni se vystříhat výše uvedených, případně dalších úskalí, může být jejich nasazení výhodnější v hlubší znalosti místních poměrů, které externí konzultanti pravděpodobně nebudou schopni v takové míře dosáhnout. Také je třeba říci, že pokud svěřujeme analýzu do rukou externího dodavatele, měli bychom mít určitou důvěru v něj i ve schopnosti jeho konzultantů. Pokud dodavatele již neznáme z předchozích projektů, je vhodné mít k dispozici důvěryhodné reference, případně si například nechat předložit ukázky výstupů analýzy apod. Většinou je také výhodné, pokud má dodavatel předchozí zkušenosti z obdobné organizace nebo odvětví.

Jednou z mnoha otázek, které často řešíme při plánování analýzy, je hloubka zkoumání technického zabezpečení informačního systému organizace. Pokud organizace provozuje pouze „běžný“ informační systém, tj. klasická firemní síť s uživatelskými stanicemi, servery a dalšími zařízeními, se standardními aplikacemi apod., postačí zběžné technické testy zmiňované v rámci výše uváděných typů analýz (raději si ale vždy ověřte, že jsou v nabídce konkrétního dodavatele obsaženy). Pokud organizace provozuje aplikace, které jsou pro její fungování životně důležité nebo jinak kritické (např. obsahují vysoce citlivé informace), případně pokud má o technickém zabezpečení svého informačního systému odůvodněné pochybnosti (např. při plném outsourcingu provozu IT) apod., je opodstatněné provést před vlastní analýzou komplexní penetrační testy, případně další technické audity. Zjištěné nedostatky pak mohou být zahrnuty do následné analýzy.

Jen analyzovat nestačí...

Závěrem je třeba zdůraznit, že samotné provedení analýzy k úspěšnému nastartování řešení informační bezpečnosti v organizaci nestačí. Pokud nejsou výsledky komunikovány v rámci celého vedení, případně v dalších relevantních strukturách organizace, může být v nejhorším případě jediným výsledkem analýzy „zpráva v šuplíku“. Vhodným způsobem, jak tomuto předejít, je v prvé řadě zapojení daných lidí přímo v rámci analýzy (úvodní vysvětlení proč se analýza provádí, dožádání potřebných informací v jejich působnosti, spolupráce při stanovení úrovní hrozeb apod. v průběhu). Dále je vhodné uspořádat závěrečnou prezentaci výsledků analýzy a navrhovaných opatření formou workshopu, kde jsou všechny opatření důkladně vysvětlena a zdůvodněna v kontextu celé organizace. V praxi se bohužel často stává, že organizace úspěšně implementuje navržená opatření spadající do oblasti technické bezpečnosti (toho se většinou úspěšně chopí samotné IT oddělení), ale není už schopna správně uchopit opatření v oblasti organizační bezpečnosti (vytvoření rolí, zavedení vlastnictví aktiv, přidělení zodpovědností, definice a údržba formální bezpečnostní politiky apod.). Omezovat se pouze na technickou bezpečnost je však jen částečným řešením. Hlavně je třeba nastartovat bezpečnostní procesy, které by měly zajistit udržování a kontinuální zlepšování úrovně informační bezpečnosti organizace. ■

Tolik k fázi identifikace aktuálního stavu bezpečnosti. Příště se podíváme na návrh bezpečnostních opatření...

Autor působí jako IT security consultant společnosti AEC, člena skupiny Cleverlance.