Bezpečnost IT a vývoj informačních systémů

Milada Hrabalová
Otakar Fišer

Hutnická zaměstnanecká pojišťovna (HZP),
Jeremenkova 11, 703 00 Ostrava-Vítkovice, ČR,
milada.hrabalova@hzp.cz, fiser@hzp.cz

Abstrakt

Příspěvek se zabývá zkušenostmi Hutnické zaměstnanecké pojišťovny (dále HZP) se zaváděním procesu řízené bezpečnosti IT a uvádí platné české normy pro tuto oblast. Předkládá seznam a stručný vysvětlující text k dokumentům, které organizace musí v souladu s normami vypracovat a problémy, se kterými se přitom může setkat.

Druhá část příspěvku je věnována rozboru normy ČSN ISO/IEC 17799 [1] z hlediska vývoje informačních systémů. To může být vodítkem pro organizace, které řízenou bezpečnost zavedenou nemají a přesto by chtěly vyvíjet bezpečné informační systémy.

1. POLITIKA BEZPEČNOSTI IT A NORMY

Pro zavádění bezpečnosti IT platí v ČR dvě základní normy:

- ČSN ISO/IEC TR 13335 [2] je vydána v češtině a má pět částí
    1. Pojetí a modely bezpečnosti IT
    2. Řízení a plánování bezpečnosti IT
    3. Techniky pro řízení bezpečnosti IT
    4. Výběr ochranných opatření
    5. Ochranná opatření pro externí spojení
- ČSN ISO/IEC 17799 [1] byla schválena ČNI (Českým normalizačním institutem) jako ČSN k přímému použití originálu a tudíž je oficiálně pouze v anglickém jazyce.

Kromě toho existují normy k některým konkrétním oblastem, jako např.:

- ČSN ISO/IEC 15408 - Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT
- ČSN ISO/IEC 10181 - Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů
- ČSN ISO/IEC 11770 - Informační technologie - Bezpečnostní techniky - Správa klíčů

2. ZAVÁDĚNÍ ŘÍZENÉ BEZPEČNOSTI

Hutnická zaměstnanecká pojišťovna se začala systematicky věnovat bezpečnosti IT v roce 2003. Již před tímto rokem se bezpečností IT zabývala, ale jednalo se o řešení izolovaných problémů (antivir, firewall atd.) a řešil je v naprosté většině případů odbor informatiky. Jenže bezpečnost IT je věcí všech zaměstnanců organizace a k tomu jsme chtěli dojít.

Vybrali jsme dodavatele, firmu Pro IT, která nás uvedla do problematiky bezpečnosti IT, provedla analýzu rizik a pomohla s vyhotovením některých potřebných dokumentů. Během práce jsme se také naučili, jak pokračovat samostatně dále.

2.1. Analýza rizik a vypracování dokumentů

Analýza rizik trvala nejdéle. Při ní jsme museli být dodavateli nápomocni a odpovídat na jeho otázky co vše vlastníme a provozujeme, jak si čeho ceníme a co by se stalo, kdyby některá ze služeb byla nedostupná.

V průběhu sběru podkladů pro analýzu rizik jsme vyhotovili dokument Politika bezpečnosti HZP, jako doplnění strategie Hutnické zaměstnanecké pojišťovny o bezpečnost a deklaraci vůle managementu HZP ohledně bezpečnosti.

Dodavatelem byly vypracovány kromě analýzy rizik i dokumenty: Politika bezpečnosti IT HZP, Systémová bezpečnostní politika ICT/IS, Plán bezpečnosti, Havarijní plán oddělení IT, Směrnice pro interní audit a Struktura školení bezpečnosti IT.

Analýza rizik a struktura dokumentů vycházela z norem, především z ISO/IEC TR 13335 [2] a s přihlédnutím k ISO/IEC 17799 [1]. Veškeré práce dodavatele trvaly zhruba čtyři měsíce.

2.2. Bezpečnostní management

V určité etapě práce bylo nutné jmenovat bezpečnostní management, aby pokračoval v práci na místě, kde ji ukončil dodavatel:

- Bezpečnostní manažer – je v HZP pracovník informatiky částí své pracovní náplně a v této činnosti je přímo podřízen řediteli organizace. Toto řešení bylo zvoleno proto, že jsme považovali za zbytečné v organizaci naší velikosti mít pro bezpečnost IT zaměstnance na plný úvazek.
- Fórum bezpečnosti – zahrnuje zástupce důležitých útvarů, řídí manažera bezpečnosti a schází se čtvrtletně nebo nad aktuálním problémem.
- Auditor bezpečnosti – kontroluje stav bezpečnosti IT, dodržování bezpečnostních směrnic. Musí být nezávislý, nezúčastněný na administraci bezpečnosti.

Bylo nutné pojmenovat vlastníky procesů a dat, správce systému a aplikací.

2.3. Bezpečnostní dokumenty

Dokumenty vypracované dodavatelem nebylo možno použít přímo jako vnitřní předpisy HZP. V mnohých případech bylo navrženo variantní řešení, na mnohá řešení jsme nebyli vybaveni personálně ani finančně, ale hlavním důvodem bylo dokumenty přepsat do jazyka, srozumitelného i zaměstnancům mimo informatiku.

Například *Systémová bezpečnostní politika ICT/IS* byla příliš obsáhlá (cca 70 stran) a na mnohých místech příliš odborná na to, aby ji četli všichni zaměstnanci. Byla tedy rozdělena do tří částí. Dokumenty byly vypracovávány jeden po druhém v průběhu několika měsíců. Již teď je zřejmé, že je v brzké době nutná jejich revize a aktualizace.

V současné době existují v HZP tyto vnitřní předpisy:

- Politika bezpečnosti HZP – v ní je řešena bezpečnost celková včetně fyzické, personální atd.
- Politika bezpečnosti IT – týká se pouze IT a je postavena v obecné rovině.
- Příručka bezpečnosti IT (v normě zvaná *Politika bezpečnosti systému IT*, dodavatel ji nazval *Systémová bezpečnostní politika ICT/IS*), kde jsou již podrobně rozepsána požadovaná ochranná opatření. Je rozdělena do:
    - obecné části, se kterou musí být seznámeni všichni zaměstnanci

    - speciální části, určené pro specialisty IT a bezpečnostní management
    - Politiky bezpečnosti IT pro dodavatele, která obsahuje vše, co musí dodavatel naší organizace splňovat, čím se musí řídit a co musí mít uvedeno ve smlouvě
- Plán bezpečnosti IT – plán organizace, co je třeba podniknout v oblasti bezpečnosti IT v nejbližším roce.
- Havarijní plán – příprava na havárii, jmenování havarijních čet a popis kroků, které je po havárii nutno podniknout.
- Školení bezpečnosti IT – určení zodpovědnosti za školení bezpečnosti IT, termíny a rozsah školení pro různé skupiny zaměstnanců.

2.4. Prosazování bezpečnosti

Postupným vytvořením a přijetím příslušných vnitřních předpisů skončila jednodušší část práce. Složitější je nyní dostat bezpečnost do povědomí všech zaměstnanců tak, aby zásady bezpečnosti nebyly brány jako zbytečná práce navíc a také aby zaměstnanci uvedeným zásadám dobře porozuměli a řídili se jimi v praxi. Je těžké docílit toho, aby si všichni uvědomili, že informace jsou cenné, a že se je nelze sdělovat neoprávněným osobám.

3. VÝVOJ INFORMAČNÍCH SYSTÉMŮ A BEZPEČNOST

Každý vyvíjený systém musí v HZP splňovat požadavky, které jsou pro tento účel vymezeny v Příručce bezpečnosti IT ve speciální části. Případný dodavatel informačního systému (dále jen IS) je o svých povinnostech informován v dokumentu Politika bezpečnosti IT pro dodavatele a stvrzuje svůj souhlas s naplňováním této politiky ve smlouvě.

Jsou však organizace, které podobné vnitřní předpisy nemají. V nich většinou není kladen na bezpečnost IT takový důraz a vývojář má volnou ruku pro svou tvořivost. Pokud ale vývojář takovéto předpisy nemá k dispozici, ale přesto by chtěl, aby vyvíjená aplikace byla pokud možno bezpečná, může se řídit vlastním rozumem a tím, co kde najde na webu nebo v odborné literatuře. V takovém případě je ale velké nebezpečí, že na něco zapomene.

Jako vodítko úplnosti jeho řešení zabezpečení IS je možno použít normy, pro daný účel je vhodnější ČSN ISO/IEC 17799 [1]. Touto normou se budeme v dalším textu zabývat. Níže uvedený text slouží pouze jako jakási orientace v textu normy, na podrobný popis je norma příliš obsáhlá a místa ve sborníku málo.

Norma ČSN ISO/IEC 17799 [1] byla schválena ČNI (Českým normalizačním institutem) jako ČSN k přímému použití originálu a je oficiálně pouze v anglickém jazyce. To způsobuje nedostupnost pro některé méně zdatné angličtináře a také nejednoznačnost některých pojmů; lépe řečeno každý uživatel si je přeloží poněkud jinak. V dalším textu budu uvádět názvy kapitol i v původním znění.

3.1. Kapitoly normy ČSN ISO/IEC 17799 [1]

Norma ČSN ISO/IEC 17799 [1] se skládá z následujících kapitol:

1. Scope (Předmět normy)
2. Terms and definition (Termíny a definice)
3. Security policy (Bezpečnostní politika)
4. Organizational security (Organizační bezpečnost)
5. Asset classification and control (Klasifikace a řízení aktiv)
6. Personnel security (Personální bezpečnost)
7. Physical and environmental security (Fyzická bezpečnost a bezpečnost prostředí)
8. Communications and operations management (Řízení komunikací a provozu)
9. Access control (Řízení přístupu)
10. Systems development and maintenance (Vývoj a údržba systémů)

11. Business continuity management (Řízení kontinuity činností)
12. Compliance (Zajištění souladu)

Nejpodrobněji se vývoji a údržbě systémů věnuje kapitola 10., ale i v předcházejících kapitolách je možno najít metodiku pro bezpečný vývoj IS.

3.2. Řízení komunikací, provozu a přístupu

V části 8.1.5 Separation of development and operational facilities (Oddělení vývojových a provozních prostředků) je uvedeno, že je nutné oddělovat vývojové prostředí pro vývoj a testování od prostředí provozního, jaký je k tomu důvod a co je třeba dodržet. Myslím, že důvody jsou každému zřejmé – vývojové a testovací činnosti mohou způsobit nechtěnou modifikaci dat nebo systémového prostředí a mohou zapříčinit nestabilitu nebo poruchy systému. Oddělení provozu a vývoje je nutné také z důvodu utajení informací, obsažených v provozní databázi. Všem je nám to jasné, málokde je to striktně dodržováno.

V části 8.1.6 External facilities management (Řízení externích prostředků) jsou uvedeny zásady pro zpracování dat externím dodavatelem (outsorcing činností). Je nutno určit, které aplikace jsou příliš citlivé na tento způsob zpracování, monitorovat relevantní činnosti, určit postup při zjištění bezpečnostního incidentu atd.

Část 8.2 System planning and acceptance (Plánování a akceptace systému) hovoří o plánování kapacit a sestavení akceptačních kritérií před započetím práce na IS a část 8.3 Protection against malicious software (Ochrana před škodlivým SW) uvádí nutnost implementovat kontroly na odhalení škodlivého SW.

V části 8.4 Housekeeping (Vnitřní správa – administrace IS) se dozvíte blíže o:

- zálohování – záloha a údaje o záloze včetně způsobu obnovení dat musí být uložena na vzdáleném místě, data musí být stejně chráněná jako v hlavním sídle, obnovovací postupy musí být pravidelně prověřované a testované.
- auditních záznamech operátorů – protokoly o časech spuštění a vypnutí systému, o systémových chybách a opravných krocích včetně identifikace osoby, která činnost vykonala.
- protokolu chyb – určení jasných pravidel, týkajících se zpracování oznámených chyb.

Část 8.6.3 Information handling procedures (Postupy pro nakládání s informacemi) upozorňuje na nutnost zavést postupy pro zacházení s informacemi v souladu s jejich klasifikací. Týká se to označování, omezení přístupu, kontroly úplnosti vstupních dat, správnosti ukončení procesu a kontroly správnosti výstupu.

Část 8.7 Exchanges of information and software (Výměny informací a SW) popisuje, jak předejít ztrátě nebo modifikaci informací při elektronické výměně informací. Blíže se zabývá např. e-mailem, webovými aplikacemi včetně elektronického obchodování, FTP.

Část 9. Access control (Řízení přístupu) uvádí nutnost kontroly přístupu k informacím a popisuje zásady pro: registraci uživatele, řízení přístupových práv, řízení uživatelských hesel, kontrolu přístupu do sítě, do operačních systémů, do aplikací, monitorování přístupu a použití systému.

3.3. Vývoj a údržba systémů

Část 10. Systems development and maintenance (Vývoj a údržba systémů) se přímo zabývá vývojem a údržbou systémů. Všechny bezpečnostní požadavky na IS včetně uvedení nouzových opatření musí být zahrnuty již do fáze projektování. Norma je v této části rozčleněna do oddílů:

10.1 Security requirements of systems (Bezpečnostní požadavky na systémy) – uvádí, co má být provedeno v rámci analýzy,

10.2 Security in application systems (Bezpečnost v aplikacích) popisuje:

- způsob validace vstupních dat - formální kontroly na rozsah, chybné znaky a kompletnost, pravidelná kontrola obsahu klíčových položek pro udržení integrity databází, způsob reakce na chyby,
- řízení vnitřních procesů - funkce přidej a smaž, řízení spouštění programů ve správném pořadí, programy na zotavení po chybách,
- autentizace zpráv - na odhalování neoprávněných změn nebo poškození obsahu),
- ověřování platnosti výstupních dat (kontrola smyslu, kontrola, zda jsou zpracovány všechny údaje, určení zodpovědnosti.

10.3 Cryptographic controls (Kryptografická opatření) se zabývá oblastmi:

- politika použití kryptografických kontrol - rozhodnutí, zda vůbec použít kryptografii, způsob obnovy zašifrovaných informací v případě poškození nebo ztráty klíčů, určení zodpovědnosti,
- obecný popis šifrování, digitálního podpisu a služby pro nepopiratelnost,
- řízení klíčů – ochrana klíčů, použití norem, postupů a metod pro řízení klíčů (způsob generování klíčů, certifikátů, distribuce klíčů, jejich ukládání, změny a aktualizace, zrušení, obnova, archivace, skartace, platnost).

10.4 Security of system files (Bezpečnost systémových souborů)

- řízení přístupu k OS a implementovanému SW - povolení pro aktualizaci, aktualizovat až po úspěšném testu, uchovat protokol o všech aktualizacích, uchovávat předešlé verze programů,
- ochrana dat při testování - použití anonymizovaných dat pro testy,
- řízení přístupu do knihovny zdrojových programů – zdrojové texty programů by měly být pro každou aplikaci v jiné knihovně, omezený přístup ke zdrojovým textům.

10.5 Security in development and support processes (Bezpečnost vývojových a podpůrných procesů). Tato část obsahuje popis postupu řízení změn, technické posouzení změn OS, omezení změn SW balíků, skryté kanály a trojský kód, vyvíjení SW mimo organizaci (vyvíjení SW třetí stranou je podrobněji popsáno v části 4.2 Security of third party access - Bezpečnost přístupu třetí strany).

4. ZÁVĚR

V současné době se již žádná organizace, která používá výpočetní a komunikační techniku, neobejde bez alespoň dílčích bezpečnostních opatření. Od určité velikosti organizace je vhodnější řešit bezpečnost IT komplexně, v souladu s normami. Osvědčily se nám následující zásady:

- Nestačí politiku bezpečnosti vytvořit a deklarovat, hlavní je dostat ji do povědomí zaměstnanců, aby se bezpečnostní chování dostalo do praxe. To znamená: školení, kontrola, sankce.
- Není dobré soustředit se pouze na technická opatření. Pokud potenciální útočník zjistí, že se přes ně nedostane, zvolí jednodušší cestu zevnitř organizace.
- Nasazovat bezpečnostní opatření na již existující systém je složitější než bezpečnost budovat už od analýzy nového systému. Na to je třeba myslet, při projektování nového IS.
- Je vhodné vybírat dodavatele s vlastní bezpečnostní politikou nebo jej smluvně zavázat k dodržování vaší.

5. LITERATURA

[1] ČSN ISO/IEC 17799:2000 – Informační technologie – Soubor postupů pro řízení informační bezpečnosti
[2] ČSN ISO/IEC TR 13335:1997 - 2000 – Informační technologie – Směrnice pro řízení bezpečnosti IT.