STANDARD ISO/IEC 27001 A OBLAST VÝVOJE A POŘIZOVÁNÍ SOFTWARE

Ladislav Beránek
Jihočeská universita v Českých Budějovicích, beranek@pf.jcu.cz

ABSTRAKT:
Příspěvek popisuje stručně zavádění systémů řízení bezpečnosti informací (ISMS) dle ISO 27001 se zaměřením na metriky v oblasti vývoje a pořizování software. Vzhledem k tomu, že při zavádění se ISMS jedná o nastavení řídicích procesů, je důležitou otázku stanovení bezpečnostních metrik pro měření účinnosti a efektivnosti procesů a přijatých opatření. Příspěvek se zaměřil na metriky pro oblast vývoje a pořizování software, protože v této oblasti se, podle zkušeností autora, většina firem a i kontrol soustředí na jednou opatření a to je oddělení vývojového a provozního prostředí. Cílem příspěvku bylo připomenout nutnost zavedení procesů a zejména metrik v celém rozsahu dané části standardu týkajícího se vývoje a pořizování programového vybavení.

KLÍČOVÁ SLOVA:
bezpečnostní metriky, bezpečnost informací, ISO 27001, ISMS

1. ÚVOD

Jedinou cestou, jak zajistit účinnosti bezpečnosti informací a přesvědčit se o efektivnosti vkládaných prostředků do oblasti bezpečnosti, je zavedení standardních řídicích procesů. Pro zavedení a provozování systému řízení bezpečnosti informací (ISMS) v organizacích včetně příslušných opatření je určen i standard ISO 27001. Systém řízení dle tohoto standardu je v souladu i s dalšími standardy systémů řízení (jako ISO 9001 a ISO 14001). Stejně tak jako systémy managementu jakosti, systémy managementu prostředí nebo systémy bezpečnosti a ochrany zdraví při práci, také systém řízení bezpečnosti informací dle ISO 27001 v sobě zahrnuje management, politiku, organizaci i pravidelné přezkoumávání, tzv. PDCA model [1].

2. ZAVEDENÍ SYSTÉMU INFORMAČNÍ BEZPEČNOSTI DLE ISO 27001

Zavedení a provozování efektivního systému řízení informační bezpečnosti zahrnuje celý řetězec kroků. V rámci těchto kroků je zapotřebí řešit následující oblasti.

Rozsah ISMS. Nejdříve je zapotřebí stanovit, v jakém rozsahu má být ISMS budováno. Systém sebou totiž přináší také nároky na celkové řízení, řídící dokumentaci a tvorbu záznamů. To má dopad na všechny pracovníky od ostrahy po vrcholový management. Implementovat ISMS znamená primárně rozhodnout o jeho rozsahu a způsobu zavedení do stávajících procesů organizace. Představuje také nároky na zdroje organizace.

Integrace systémů řízení. Pokud má organizace již zavedené jiné systémy řízení (např. ISO9001, ISO14001), pak je třeba ISMS zavádět v souladu s nimi. Je třeba vytvořit integrovaný systém řízení, neprovozovat několik systémů odděleně.

Řízení rizik. Důležité je především určit, jaká úroveň rizika je přijatelná v organizaci pro různá aktiva. S tím souvisí i výběr metodiky pro hodnocení rizik (CRAMM, OCTAVE, FRAP a další).

Bezpečnostní kultura organizace. Musí se zjistit, zda kultura v organizaci podporuje ISMS. Například jaké změny ve firmě znamená zavedení ISMS, zda je potřeba provést změnu kultury tak, aby vzniklo silné povědomí o otázkách bezpečnosti.

Metriky. Měření toho, zda zavedený systém řízení informační bezpečnosti funguje, je jednou z podmínek, které jsou nutné pro certifikaci. Při stanovování metrik může pomoci například dokument PD 3003:2002 „Are you ready for BS7799 Part 2 Audit" [3], který poskytuje celou řadu praktických návodů, jak zhodnotit ISMS a jeho efektivnost. (dokument vydává Britský normalizační institut.)

Certifikace. Cílem zavedení ISMS je většinou certifikace tohoto systému. Nicméně je přínosné zavést a provozovat ISMS i bez cíle bezprostřední certifikace.

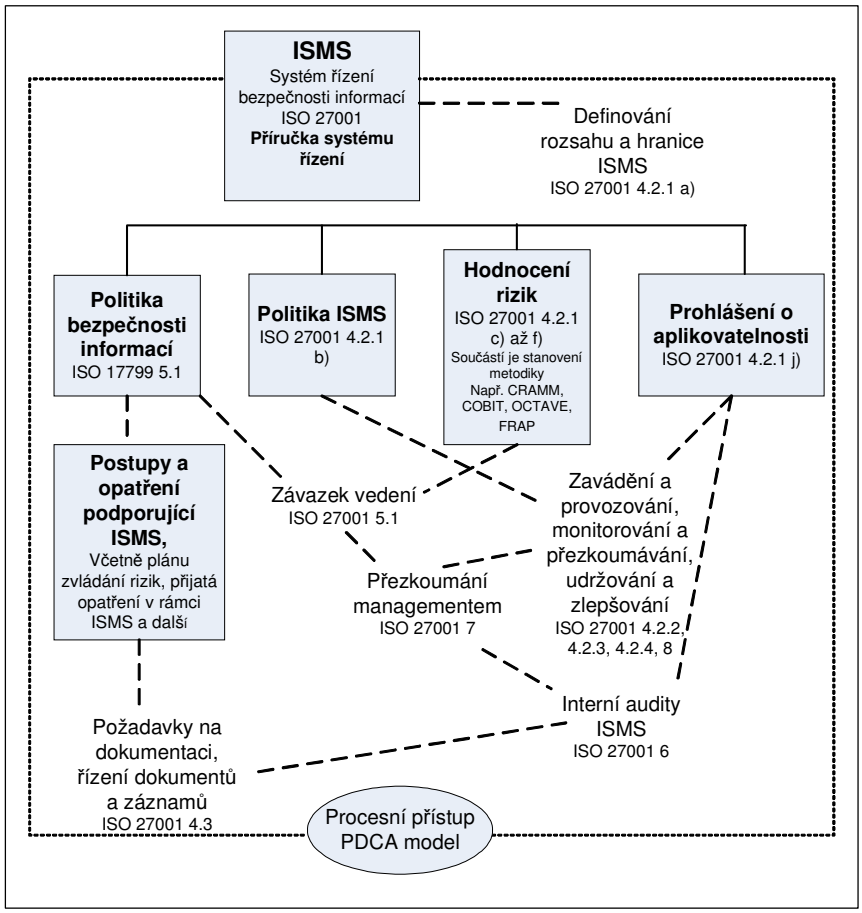
2.1 Nejčastější chyby při zavádění ISMS

Zavádění ISMS v organizacích není krátkodobý proces. Vyskytují se i problémy, které je nutno překonat. Nejčastěji se jedná o:

- podcenění ceny podnikových informací i dalších aktiv,
- spoléhání pouze na technické řešení (firewall, antiviry, aj.), kdy management podniku rozumí spíše problematice fyzické bezpečnosti, ale nevidí následky špatné informační bezpečnosti,
- nezvládnutí provozních aspektů bezpečnosti, zejména neprovádění dostatečných opatření a nedostatečná kontrola,
- přidělení neškolených pracovníků na udržování bezpečnosti,
- nepřidělení dostatečných zdrojů na odstranění nedostatků po certifikaci,
- nedostatečné nastavení procesů a špatné metriky,
- a další.

Všechny tyto nedostatky vypovídají o chybách v příslušných řídicích procesech a o nízké efektivitě manažerského řízení v oblasti bezpečnosti informací. V rámci zavedení nebo zlepšování ISMS musí být tyto nedostatky odstraněny.

Jedná se zejména o důsledné respektování systémového přístupu ke kvalitě návrhu informačních systémů [6] a postupu návrhu IS podle doporučených metod.



Obrázek 1: Základní dokumenty ISMS a jejich souvislosti

3. METRIKY PRO VYHODNOCENÍ RIZIK

Metrika je definována jako přesně vymezený finanční či nefinanční ukazatel nebo hodnotící kritérium, které je používáno k hodnocení úrovně efektivnosti konkrétní oblasti řízení podnikového výkonu a jeho efektivní podpory prostředky IS/ICT. Metrika by měla být konzistentní a její sledování by nemělo být náročné na zdroje. Skupinu metrik sdružených za určitým cílem (tzn. vztahujících se ke konkrétní oblasti, procesu či projektu) nazýváme "portfolio metrik".

Metriky pro vyhodnocení rizik kvantifikují aktiva, systémové prostředky a informační zdroje, dále kvantifikují hrozby a zranitelnosti a mohou kvantifikovat i přijatá opatření. Kombinací těchto prvků na základě různých přístupů a za použití různých nástrojů (CRAMM, RA2, FRAP apod.) nakonec získáme model rizika, pomocí něhož se můžeme rozhodovat co s různými riziky ohrožujícími naše aktiva dále dělat. Můžeme rizika přijmout, pokud bychom například museli přijmout opatření, jehož cena by byla příliš vysoká, můžeme přenést riziko, například přenesením dané činnosti, na jiný subjekt a nebo můžeme přijmout nějaké opatření ke snížení daného rizika. Řízení rizik znamená proaktivní přístup. Mnoho zranitelností je známých a protože známe své systémy, můžeme tyto zranitelnosti do jisté míry měřit a řídit.

Na druhé straně možné hrozby, které mohou ovlivnit negativně naše systémy obsahují větší míru nejistoty v tom smyslu, že vnější prostředí obsahuje takové aktéry hrozeb, které organizace nemůže přímo ovládat. Může se jednat i o fyzické hrozby, jako jsou požáry, záplavy apod. Při snižování stupně zranitelnosti musíme uvážit i takové věci, jako doba

potřebná pro odstranění dané zranitelnosti, technologické trendy, a tak dále. Měření pravděpodobnosti hrozby úspěšného útoku na systém je extrémně obtížné. Přijatá opatření mohou snížit zranitelnosti a zmírnit jisté hrozby při ochraně jednoho nebo více aktiv. K tomu, abychom mohli změřit efektivnost přijatých opatření, musíme definovat a přijmout určité bezpečnostní metriky.

Aktivům přiřazujeme při výpočtu rizika určitou hodnotu: ta se odvozuje zejména na základě představy o ztrátě daného aktiva, jeho nesprávného použití, ztrátě jeho důvěrnosti, přerušení služby nebo nutnosti náhrady příslušného aktiva. Také identita je takové aktivum a můžeme na něj vztáhnout všechny uvedené souvislosti řízení rizik IS/IT a můžeme je posuzovat z hlediska společnosti, správce identit nebo z hlediska uživatele a z dalších hledisek.

Pro hodnocení zavedených procesů v rámci tvorby ISMS musíme zavést metriky, umožňující měření toho, zda daný proces probíhá správně a zda opatření jsou správně implementována. Příklad takových metrik uvádí tabulka 1.

Proces / Skupina opatření	**Metrika**	**Cílová hodnota**	**Reporting**
Zvládání rizik a implementace bezpečnostních opatření	Celkový počet bezpečnostních incidentů a událostí		Měsíčně
	Počty incidentů podle závažnosti		Čtvrtletně
	Počty incidentů s původem „interní“ a původem „externí“		Čtvrtletně
	Počty incidentů IT a ostatních		Čtvrtletně
	Součet času stráveného řešením bezpečnostních incidentů		Čtvrtletně
	Součet přímých nákladů bezpečnostních incidentů		Čtvrtletně
	Počet porušení SLA IT		Čtvrtletně
	Procento porušených SLA IT		Čtvrtletně
Zlepšování ISMS	Počet zjištění při interních auditech		Ročně
Zálohování	Procento úspěšného obnovení dat ze záloh	95%	Čtvrtletně
Školení	Procento zaměstnanců, kteří neabsolvovali školení o bezpečnosti informací	5%	Čtvrtletně
Plánování kontinuity	Interval mezi revizemi plánů kontinuity	24 měsíců	Ročně
Interní audity	Interval mezi interními audity stejné oblasti	12 měsíců	Ročně

Tabulka 1: Příklady metrik procesů ISMS

4. OBLAST VÝVOJE A POŘÍZENÍ SOFTWARE - METRIKY

Zejména aplikační programy a informace v nich zpracovávané představují aktiva organizace, které mají největší hodnotu.pro danou organizaci. Může se jednat o ERP systémy, datové sklady, systémy pro HR, různé zákaznické systémy a další. Tyto systémy na druhé straně reprezentují místa potenciální zranitelnosti. Vektory hrozeb vůči aplikacím jsou stejně

důležité jako vektory hrozeb počítačovým sítím, i když hrozby aplikacím nejsou tak přehledné, protože různých aplikací existuje celá řada s různou úrovní zabezpečení. Většina útoků je také směřována proti aplikacím, protože ty představují, jak již bylo uvedeno, nejcennější aktiva organizací.

Společnosti mohou aplikační software vyvinout vlastními silami nebo nechat tento software vyvinout na zakázku. Software, které je vyvíjeno bez věnování dostatečné pozornosti bezpečnostním problémům, může být z hlediska bezpečnosti problematické. Při vývoji software musí být postupováno s ohledem na určité obecné principy. Měření relativní bezpečnosti aplikačního kódu není snadné. Ani bezpečnostní průmysl se zatím neshodl na tom, co to znamená budovat „bezpečnou aplikaci“. Ačkoli se definice se mění, existují přinejmenším tři potenciální způsoby, jak měřit aplikační bezpečnost (viz tabulky): počítáním vzdáleně a lokálně využitelných vad bez znalosti kódu (metriky bez předběžných znalostí), počítáním návrhových a realizačních vad kódu (bezpečnostní metriky kódu), a vytvořením indikátorů kvalitativních rizik při používání váženého vyhodnocovacího systému (metriky a indikátory kvality procesů).

Vzhledem k tomu, že ISO 27001 požaduje, aby bylo zaveden proces pro udržování bezpečnosti programů a informací aplikačních systémů (odstavec A.12.5 standardu), je nutné, aby dané procesy byly příslušným způsobem měřeny. Příklad některých metrik jsou uvedeny dále, týkají se zejména procesů spojených s odstavcem standardu ISO/IEC 27001 A.12.5.

Tabulka 2 uvádí příklad metrik, které je možné využít při hodnocení procesů dle A.12.5.1 oddělení vývojového a produkčního systému.

Metrika	Účel	Zdroje
Počet změn provozního software	Měří počet změn, které musí programátoři provést v produkčním systému, ale standardním postupem přes vývojové a testovací prostředí.	Ruční sledování
Počet výjimek	Měří počet změn, které musí programátoři provést přímo v produkčním systému	Ruční sledování
Počet neautorizovaných změn	Měří počet neautorizovaných změn	Systémové zápisy

Tabulka 2: Příklad bezpečnostních metrik pro hodnocení změn v produkčních systémů

Tabulka 3 uvádí příklad metrik pro hodnocení aplikačního softwaru bez předběžných znalostí. Zpravidla se provádí automatické testování.

Metrika	Účel	Zdroje
Počet závad	Identifikovatelné vady vzniklé v důsledku chyb při realizačních nebo při návrhu	Testovací nástroje
Počet zjištěných zranitelností v aplikaci (počet), který může být dále specifikován podle kritičnosti, typu chyby apod.	Měří počet zranitelností, které může potenciální útočník nalézt bez předběžných znalostí	Ohodnocení zranitelností bezpečnostním konzultantem

Tabulka 3: Bezpečnostní metriky pro hodnocení aplikací bez předběžných znalostí

Tento typ testování bez předběžných znalostí je typický zejména pro webové aplikace, ale použití je samozřejmě širší. Pro testování se nejčastěji používají automatizované nástroje (Nessus apod.) nebo testy prováděné bezpečnostními konzultanty. Cíl testování je najít zranitelnosti, které mohou být využity k porušení integrity, důvěrnosti nebo dostupnosti. Příkladem takových chyb může být:

- SQL injection: manipulace se vstupními hodnotami webových formulářů k obejití bezpečnostních prvků databáze, která dovolí přístup k citlivým informacím,
- Command injection: Provádění nativních příkazů operačního systému na webovém
- serveru,
- Parametr tampering: změna polí předložených webových formulářů způsobující změnu stavu aplikace,
- Cross-site scripting: Změna vstupních údajů způsobí, že následující uživatelé mohou
- vykonat příkazy JavaScriptu s cílem zmocnit se session nebo zachycení dat,
- Buffer overflow: Přeplnění bufferu na straně serveru s cílem donutit server k ukončení činnosti nebo ho vzdáleně převzít.

Na základě testování je zpracovaná zpráva o výsledcích, která uvede počet závad a bezpečnostních nedostatků a může je seřadit podle kritičnosti.

Další typ metrik spojených s informačními systémy vyvíjenými nebo nakupovanými jsou metriky spojené s využitím systémů:

Metrika	Účel	Zdroje
Riziko spojené s obchodními činnostmi	Jednoduchý vzorec pro vyjádření obchodní dopad a kritičnosti zranitelností identifikovaných v bezpečnostních hodnocení	Bezpečnostní hodnocení
Indikátory shody	Vytváří skóre pro klasifikaci aplikace nebo skupin aplikací podle celkového bezpečnostního stavu	Dotazníky

Tabulka 4: Procesně kvalitativní metriky a indikátory

O tyto metriky se může jednat již ve stadiu ranějšího stadia životního cyklu aplikace. Jedná se zejména o:

- Kontroly návrhu
- Ohodnocení návrhu architektury
- Případná kontrola kódu, zejména v případě dokončení vývoje určitých citlivých funkcí a bezpečnostních mechanismů
- Penetrační testy

Při tomto typu hodnocení je vhodné používat přístup řízení rizik, tj. vyhodnocovat riziko a hodnotit jeho úroveň z hlediska možnosti nebo nutnosti jeho snížení.

Další skupina metrik se vztahuje na bezpečnost kódu. Zde uvádím jenom několik příkladů, protože podrobnější popis by přesáhl rámec příspěvku. Více např. v [4], [5] a v dalších.

Metrika	Účel	Zdroje
Stanovená četnost pro vyvíjené aplikace v procentech	Měřítko, jak často jsou aplikovány bezpečnostní principy při vývoji software v průběhu jeho životního cyklu	Ruční sledování Počet řádků kódu (LOC)
Závady a nedostatky na tisíc řádků kódu (KLOC)	Charakterizuje dopad poměr bezpečnostních závad v vyvíjeném kódu	Software pro analýzu kódu
Hustota zranitelností (počet zranitelností na jednotku kódu)	Charakterizuje dopad poměr bezpečnostních závad ve vyvíjeném kódu	Software pro analýzu kódu

Tabulka 5: Příklad metrik týkajících se bezpečnosti vyvíjených aplikací

5. ZÁVĚR

V oblasti bezpečnosti informací přišlo použití metrik na řadu zejména se zaváděním systémů řízení bezpečnosti informací dle ISO 27001, kde jednou z fází modelu PDCA je monitorování a přezkoumávání. U této fáze je jedním z požadavků měřit účinnost zavedených opatření pro ověření toho, zda byly naplněny požadavky na bezpečnost. V příspěvku byly zmíněny některé metriky pro oblast vývoje a pořizování software. Také pro tuto oblast musí být zavedeny procesy a musí být definovány vhodné metriky pro sledování účinností těchto procesů. Nejčastěji je u firem určitým způsobem zvládáno oddělení vývojového a provozního prostředí a provozovány příslušné procesy, často je ale na další procesy týkající se této oblasti standardu ISO/IEC 27001 zapomínáno. Příspěvek měl připomenout i nutnost zavedení procesů a zejména metrik v celém rozsahu standardu.

6. LITERATURA:

[1] Standardy ISO/IEC 27001
[2] Standard BS/ISO/IE 17799
[3] PD 3003:2002, Are you ready for BS7799 Part 2 Audit, British Standard Institution 2002
[4] M. Howard, J. Pincus, and J.Wing, "Measuring Relative Attak Surfaces," 2003, [cit. 4.3.2008]. Dostupné na: http://www.cs.cmu.edu/~wing/publications/Howard-Wing03.pdf
[5] P. Manadhata and J.M. Wing, "Measuring a System's Attack Surface," 2004, [cit. 4.3.2008]. Dostupné na: http://reports-archive.adm.cs.cmu.edu/anon/2004/CMU-CS-04-102.pdf (1/2008)
[6] B. Lacko, Systémový přístup k jakosti softwaru, Sborník konference Tvorba software 2004, VŠB-TU Ostrava 2004, 129-138

ABSTRACT:

The paper describes briefly the establishing of the information security management system according ISO/IEC 27001. Introduction and operation of efficient information security management system includes whole chain of steps. In terms of these steps it is necessary to establish some processes. The important question is the correct definition of metrics for measurement of effectiveness of established processes and accepted measures. The paper describes some practical metrics from ISMS operating but it deals primarily with the metrics from the domain of software development and acquisition. From the author's experience organizations often concentrate only on the measure of the separation of development environment from the production environment. The aim of the paper was to remind the necessity to establish processes and metrics in the entire scope of relevant part of standard.