Kapitola 6

Systém řízení bezpečnosti informací

Po prostudování kapitoly budete umět:

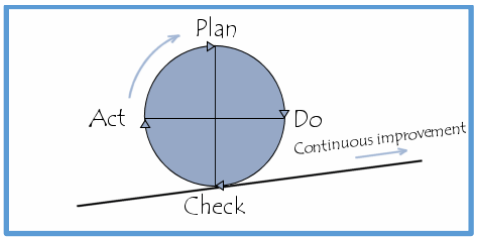
- vysvětlit účel cyklu PDCA;
- rozpoznat, proč je nutné při realizaci bezpečnosti informačního systému postupovat dle požadavků ISMS;
- základy řízení rizik;
- pojmy ITIL, COBIT, Prince 2;
  vysvětlit, proč je nutné při realizaci bezpečnosti informačního systému postupovat dle doporučení ČSN norem řady 27000.

Klíčová slova:

PDCA, ISMS, ČSN normy, řízení rizik, Prince 2

6.1 Procesní řízení bezpečnosti v cyklu PDCA

Principem celého ISMS (Information Security Management System), tedy systému řízení bezpečnosti informací je tzv. PDCA model (Demingův model), který je zobrazen na obrázku č. 6.1.



Obrázek 6.1 Demingův model

Vlastní implementace systému řízení bezpečnosti informací zahrnuje především návrh a implementaci procesů, které vedou k řízení bezpečnosti informací, kontroly způsobu jejich implementace a neustálého udržování a zlepšování (PDCA).

Postupů a metodik, jak implementaci zvládnout existuje několik, v případě informačních systémů lze v souladu PDCA postupovat podle osvědčeného postupu.

Plan – ustavení ISMS:

- Strategie informační bezpečnosti
- Management rizik
- Návrh bezpečnostní politiky, systémových směrnic, plánu řízení kontinuity činností
- Bezpečnostní plán a plán implementace ISMS

Do – zavádění a provozování ISMS:

- Implementace procesů a postupů dle bezpečnostního plánu a plánu implementace ISMS
- Zavedení postupů kontrol
- Školení
- Provoz

Check – monitorování a přezkoumání ISMS:

- Před-certifikační audit
- Penetrační testy
- Testy procesů
- Testy techniky

- Testy metodami sociálního inženýrství
- Další testy dle plánu implementace

Act – udržování a zlepšování

6.2 Normy řady ČSN ISO/IEC 27000

Spolu s rozvojem šifrové ochrany informací hrají stále důležitější roli standardizační činnosti mezinárodních i státních organizací. Přijímané normy a standardy dávají doporučení a stanovují principy a postupy vývoje, testování a ověřování parametrů i podmínky provozu šifrovacích zařízení i celých informačních systémů s integrovanou bezpečnostní nadstavbou. Zároveň jsou nezbytnou součástí při hodnocení bezpečnostních parametrů realizovaných komponent a systémů. Cílem bezpečnostních norem je též unifikace vytvářených produktů i celých systémů. Zvláštní zřetel je nyní dáván na standardizaci procesního řízení v oblasti bezpečnosti.

Normy ČSN ISO/IEC řady 27000 lze považovat za nejvhodnější technický normativní systém v oblasti bezpečnosti informací.

ČSN ISO/IEC 27000 je určena pro obecný úvod do ISMS a pro uvedení předmětů jednotlivých norem této řady. ČSN ISO/IEC 27000 poskytuje slovník, formálně definující většinu pojmů používaných v řadě norem ČSN ISO/IEC 27000, a popisuje rozsah a cíle pro každou normu této řady.

Norma ČSN ISO/IEC 27002:2014. Tato mezinárodní norma specifikuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací v rámci kontextu organizace. Tato mezinárodní norma také zahrnuje požadavky na posuzování a ošetření rizik bezpečnosti informací, přizpůsobené potřebám organizace. Požadavky této mezinárodní normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností.

Norma ČSN ISO/IEC 27002:2014. Tato mezinárodní norma poskytuje směrnice pro organizační normy bezpečnosti informací a postupy pro řízení bezpečnosti informací, včetně výběru, implementace a řízení opatření, s přihlédnutím k prostředí rizik bezpečnosti informací organizace. Je určena pro použití organizacemi, které mají v úmyslu:

a) vybrat opatření v rámci procesu zavádění systému řízení bezpečnosti informací založeném na normě ISO/IEC 27001 - ISMS;
b) zavést obecně uznávaná opatření bezpečnosti informací;

c) vypracovat vlastní směrnice k řízení bezpečnosti informací.

Zatímco tato norma poskytuje návod pro širokou škálu opatření v oblasti bezpečnosti informací, která se běžně uplatňují v mnoha různých organizacích, zbývající normy v řadě norem ČSN ISO/IEC 27000 poskytují doplňující doporučení či požadavky týkající se dalších aspektů celkového procesu řízení bezpečnosti informací.

6.3 Nastavení maturity bezpečnosti informačního systému

Pro řízení bezpečnostních procesů v informačním systému je vhodné postupovat podle metodologie CoBiT 5 (Control Objectives for Information and related Technology) – Řídící cíle pro oblast informačních a s nimi propojených technologií, definující kromě základních bodů řízení i tzv. modely zralosti (maturity models) pro jednotlivé bezpečnostní procesy.

Na základě analyzovaných informací o informačním systému podniku, jakož i rozboru vnitřní bezpečnostní dokumentace podniku lze zařadit daný informační systém, resp. celý podnik do příslušné úrovně bezpečnostní zralosti (tzv. enterprise maturity level of security).

Interní benchmark ilustruje stav informačního systému s hodnotami získanými počáteční analýzou v porovnání s tím, do jaké míry (procentuálně) plní požadavky normy ČSN ISO/IEC 27002:2014 ve srovnání s jejími cílovými hodnotami požadovanými pro příslušnou úroveň bezpečnostní zralosti. Od této úrovně zralosti podniku se odvíjí i výše uvedená, navrhovaná bezpečnostní opatření.

6.4 Řízení rizik

Proces řízení rizik v podniku těsně navazuje na výsledky analýzy rizik. Na základě těchto výsledků musí podnik připravit bezpečnostní projekt. V tomto projektu se řízení rizik zaměřuje na dvě úrovně rizik projektu:

- Koncepční úroveň – kdy jsou řešeny hlavní úkoly a formulují se priority bezpečnostních opatření. Zároveň je třeba skloubit tento projekt v rámci řízení projektů s projekty již realizovanými.

- Projektová úroveň – zvážení hlavních projektových rizik, které mohou být interního i externího charakteru. Musí být vytvořen soupis evidovaných rizik a stanoveny možnosti podniku při realizaci návazných opatření z hlediska finančního, personálního aj. pokrytí. V tomto případě je nezbytné posoudit, zda jsou veškerá identifikovaná rizika přijatelná či nepřijatelná. V případě nepřijatelných rizik musí být projekt upraven tak, aby, byl nastaven proces eliminace těchto rizik

6.5 Audit bezpečnosti

Účelem auditu bezpečnosti informačního systému je posouzení vhodnosti a úplnosti provozovaných bezpečnostních opatření, tj. zda funkční a technická specifikace navržených a provozovaných bezpečnostních řešení poskytuje předpoklady, že řešení tak, jak je navrhováno, splní požadavky formulované v bezpečnostních normách ČSN ISO/IEC řady 27000.

Kromě postupů uvedených v normách ČSN ISO/IEC řady 27000 lze využít v přístupu k auditu bezpečnosti IS řadu celosvětově přijímaných metodik, při kterých lze využít i vypracované SW nástroje. Mezi nejznámější metodiky a nástroje patří metodika ITIL (IT Infrastructure Library), COBIT (Control Objectives for Information and related Technology) i řada průmyslových metodik, které nich vycházejí.

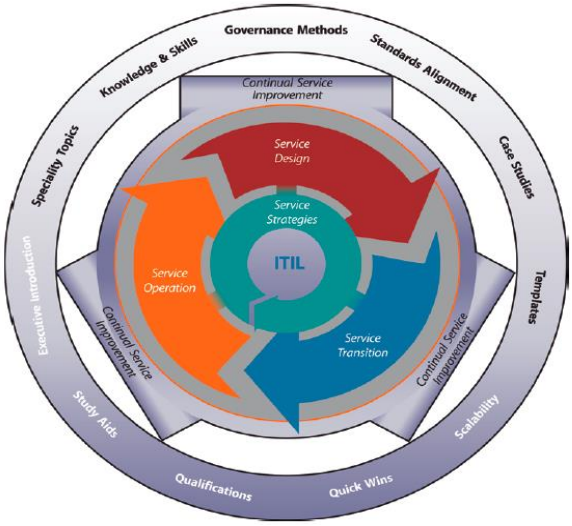
Audit bezpečnosti standardně prochází následujícími fázemi:

- popis základních cílů a zaměření auditu při stanovení hranic auditovaného systému,
- posouzení stávajících bezpečnostních parametrů systému,
- popis evidovaných hrozeb, zranitelností v jednotlivých oblastech informačního systému,
- identifikace a ocenění bezpečnostních rizik a kritických míst v systému,
- návrh bezpečnostních opatření, stanovení prioritních úkolů v postupu navrhovaného řešení příslušných opatření.

V návaznosti na vyhodnocení výsledků auditu je vhodné v rámci organizace aktualizovat stávající systémovou bezpečnostní politiku a provést celkovou revizi systému řízení bezpečnosti zpracovávaných informací, přičemž je důležité přijatá bezpečnostní opatření harmonizovat business strategií podniku.

6.6 ITIL[2]

Informace uvedené v ITIL (Information Technology Infrustructure Library) vycházejí ze zkušeností „best practice“ mnoha společností na celém světě. Jedná se de-facto o mezinárodní standard pro řízení IT služeb (IT Service Management). ITIL byl publikován poprvé v letech 1989 – 1995 u Her Majesty's Stationery Office (HMSO) v UK v rámci Central Communications and Telecommunications Agency (CCTA) – dnešní Office of Government Commerce (OGC) a měl podobu 31 knih. V letech 2000 – 2004 byla původní verze revidována a následně vyšel ITIL verze 2, který čítal již jen 7 knih. V roce 2007 se objevuje ITIL verze 3, sestávající z 5 knih, které kopírují životní cyklus služby:



Obrázek 6.2 Životní cyklus služby

ITIL v jednotlivých knihách popisuje procesy, které se většinou musí v IT vykonávat, aby jej bylo možné provozovat a jaké služby musí poskytovat podnikovým business procesům. ITIL se snaží poskytované služby formulovat z pohledu zákazníka, který služby odebírá. Vychází z procesního řízení a ze zkušeností, že společnosti, které své procesy zavedly podle ITIL, dosahují vyšší efektivity, přičemž poskytované služby splňují parametry uvedené v SLA (Service level agreement), tj. dohodě o úrovni poskytovaných služeb. Další výhoda zavedení procesů podle ITIL spočívá v tom, že společnosti v takovém případě používají stejnou terminologii, která umožňuje formalizaci přijatých opatření.

Myšlenka ITIL vychází ze skutečnosti, pro firmy je výhodné vycházet z „best practices“, tj. z tzv. nejlepší osvědčené praxe, tedy z osvědčených procesů a metod řízení. Většinou však zavádění procesního řízení se střetává s obtížemi vzhledem k tomu, že zavádění ITIL sebou nese i určitou změnu

[2] ITIL® výkladový slovník v češtině, v1.1, 6. ledna 2012 založen na výkladovém slovníku v angličtině v1.0 z 29. července 2011

struktury liniového řízení v daném podniku. To může vést k obavám z větší byrokracie a k vyvolání určitých předsudků. Nejhorší zkušenosti „worst practices“ se zaváděním ITIL jsou shrnuty v dokumentu ABC of ICT[3].

ITIL popisuje vazby mezi jednotlivými procesy a definuje, jaké by měly být vstupy, výstupy, role a metriky. Vzhledem k tomu, že nositeli každého procesu jsou lidé, musí být jasně určeno, kdo za co odpovídá. V ITIL se používá pojem role, ta je přiřazena člověku nebo týmu, který pak v rámci daného procesu vykonává jednu nebo více činností. Je zřejmé, že pokud má daná role vykonávat příslušnou činnost, musí mít nejen požadované schopnosti, ale potřebuje k tomu též nástroje, tj. HW, SW a musí být vybavena i odpovídajícími pravomocemi a nést určitou odpovědnost.

V ITILu je doporučeno pro každý proces vytvořit tzv. RACI tabulku, která bude v záhlaví obsahovat role a v řádcích jednotlivé činnosti, které se musí v rámci procesu vykonat. U každé činnosti by mělo být uvedeno, kdo ji vykonává (Responsible), kdo je odpovědný za výsledek (Accountable), s kým je nutno postup konzultovat (Consult) a koho je třeba informovat (Inform). Pro úplnost je třeba dodat, že ITIL používá ještě pojem funkce a myslí tím organizační jednotku nebo tým, který určitý proces nebo aktivity v rámci daného procesu vykonává. Ač je všech pět knih, které tvoří jádro ITIL poměrně rozsáhlých, není v nich uveden detailní popis procesů, neboť ITIL popisuje jen hlavní aktivity v rámci daných procesů.

6.7 COBIT

Standard pro postupy řízení a pro kontrolu a audit stavu ICT v organizaci.

Je určen top manažerům k posuzování fungování ICT v podniku z pohledu struktury, pravomocí a zodpovědnosti a auditorovi pro provádění auditu systému řízení ICT.

COBIT – soubor nejlepších praktik a postupů, které pomáhají organizaci dosáhnout strategických cílů pomocí efektivního využití dostupných zdrojů a minimalizaci IT rizik. Soubor praktik, pro správné postupy řízení, kontroly a auditu informačních technologií.

[3] Bernam, ABC of ICT - An Introduction to the Attitude, Behavior and Culture of ICT, ISBN-13: 978-9087531409

COBIT vzájemně propojuje:

- řízení podniku (Enterprise governance);
- řízení a správu informatiky (IT governance);.
- Realizace:
- propojení podnikových a IT cílů;
- definováním metrik a modelů zralosti pro měření dosahování cílů a
- definováním odpovědností vlastníků podnikových a IT procesů.

6.8 PRINCE2

V současnosti je nejrozšířenější metodikou řízení projektů v Evropě.

Metodika PRINCE2 definuje veškeré dokumenty, důležitá pravidla a postupy pro řízení projektu se opírá o sedm principů, tvoří ji sedm procesů a popisuje sedm témat.

Principy PRINCE2:

- průběžné zdůvodnění projektu;
- poučení se ze zkušeností;
- definované role a zodpovědnosti;
- řízení pomocí etap;
- dohled nad projektem na základě výjimek;
- důraz na produkty;
- nutnost upravit metodiku podle aktuálního prostředí.

V rámci konkrétního projektu jsou práce rozděleny do dvou základních kroků. V prvním kroku dá projektový manažer dohromady základní podklady pro to, aby mohl projektový výbor posoudit, zda se vůbec pouštět do často nákladného plánování.

Je-li projektový výbor přesvědčen o vhodnosti projektu, dává své schválení, přechází se do druhého kroku, tj. stanovování projektových strategií, plánování projektu, nastavení komunikace, projektových kontrol.

V PRINCE2 existuje jednoznačný proces určující fungování projektového výboru. Pravomoci a zodpovědnosti za vývoj projektu jsou jednoznačně stanoveny a rozděleny mezi projektového manažera a řídící výbor projektu. PRINCE2 dává dokonce plnou zodpovědnost za projekt do rukou sponzora

projektu předsedajícího řídícímu výboru, a nikoliv samotnému projektovému manažerovi. Toto rozdělení vnáší do metodiky jasný řád a zvláště méně zkušeným projektovým manažerům vymezuje pravidla hry.

Nicméně v rámci každého projektu je nutné metodiku PRINCE2 přizpůsobit konkrétnímu účelu, přičemž je nutné dodržovat principy, které jsou páteří celé metodiky.

Po naplánování projektu a vypracování obchodního případu (zdůvodnění projektu či obhájení investice) opět přichází schválení řídícího výboru, který dává pokyn k zahájení následné etapy. Právě striktní rozdělení projektu na etapy dává zodpovědným manažerům možnost včas identifikovat případné problémy a zasáhnout. V projektech PRINCE2 by tedy nemělo docházet k tomu, že vedení projektu pozná až příliš pozdě nevyhnutelné překročení rozpočtu nebo zásadní nedodržení časového harmonogramu.

Kapitola pojednává procesním řízení bezpečnosti dle cyklu PDCA. Je vysvětlen důvod řešení bezpečnosti v rámci procesního řízení. Je ukázáno, proč je nutné při realizaci bezpečnosti informačního systému postupovat dle požadavků ISMS. Studenti se seznámí s
pojmy ITIL, COBIT, Prince2. Velký důraz je kladen ne nutnost při realizaci bezpečnosti informačního systému postupovat dle doporučení ČSN norem řady 27000.

1. Co je to PDCA?
2. Co znamená ISMS?
3. Popište základní charakteristiky metodik CoBIT, ITIL a Prince2.
4. Shrňte základní oblasti řešené v jednotlivých ČS normách řady 27000.

Literatura k tématu:

[1] SMEJKAL, Vladimír. Právo informačních a telekomunikačních systémů. 2., aktualiz. a rozš. vyd. Praha: C.H. Beck, 2004. Právo a hospodářství (C.H. Beck). ISBN 8071797650.

[2] MATES, P. a V. SMEJKAL. E-*government v České republice: právní a technologické aspekty*. 2. vyd. Praha: Leges, 2012. 464 s.ISBN 978-80-875-7636-6.