ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

KATEDRA TECHNOLOGIÍ A MĚŘENÍ

DIPLOMOVÁ PRÁCE

Nástroj pro řízení rizik bezpečnosti informací

vedoucí práce: **Doc. Ing. František Steiner, Ph.D.** **2012**

autor: **Bc. Radomír Klimeš**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2010/2011**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Radomír KLIMEŠ**
Osobní číslo:	**E09N0026P**
Studijní program:	**N2612 Elektrotechnika a informatika**
Studijní obor:	**Komerční elektrotechnika**
Název tématu:	**Nástroj pro řízení rizik bezpečnosti informací**
Zadávající katedra:	**Katedra technologií a měření**

Zásady pro vypracování:

1. Seznamte se s problematikou systémů řízení bezpečnosti informací (ISMS).
2. Proveďte analýzu požadavků na systém řízení rizik.
3. Navrhněte řešení nástroje pro řízení rizik a hodnocení efektivnosti ISMS.
4. Navržené řešení realizujte.

Rozsah grafických prací: **podle doporučení vedoucího**
Rozsah pracovní zprávy: **30 - 40 stran**
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky**
2. **ČSN ISO/IEC 17799 Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací**
3. **Berka a spol., Bezpečná počítačová síť**
4. **Internet**

Vedoucí diplomové práce: **Doc. Ing. František Steiner, Ph.D.**
Katedra technologií a měření

Datum zadání diplomové práce: **18. října 2010**
Termín odevzdání diplomové práce: **11. května 2011**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Ing. Vlastimil Skočil, CSc.
vedoucí katedry

V Plzni dne 18. října 2010

Anotace

Předkládaná diplomová práce je zaměřena na problematiku systémů řízení bezpečnosti informací (ISMS). Jedná se o propracovaný, dokumentovaný systém, kde jsou zvolena a chráněna aktiva nesoucí informace, rizika bezpečnosti informací jsou řízena a opatření pro potlačení či prevenci rizik jsou kontrolována.

Klíčová slova

ISMS, bezpečnost informací, riziko, PDCA, aktivum, hrozba, zranitelnost, protiopatření, vyhodnocování

Abstract

The main subject of this diploma thesis is an acquaintance with information security management system (ISMS). This system is concerned with information security management and it should meet a set of policies, which are mentioned particulary out of ISO 27001.

Key words

ISMS, security of information, risk management, PDCA, asset, threat, countermeasure, evaluation

Prohlášení

Předkládám tímto k posouzení a obhajobě diplmovou práci, zpracovanou na závěr studia na Fakultě elektrotechnické Západočeské univerzity v Plzni.

Prohlašuji, že jsem diplomovou práci na téma Nástroj pro řízení rizik bezpečnosti informací vypracoval samostatně, pod dohledem vedoucího práce a za použití odborné literatury a pramenů uvedených v seznamu, který je součástí této práce.

V Plzni dne 23.5.2012 Jméno příjmení

……..

Obsah

1 ÚVOD

Hlavním cílem této diplomové práce je podrobné seznámení se s problematikou systémů řízení bezpečnosti informací (ISMS), základním názvoslovím v této oblasti a zejména s normou ČSN ISO/IEC 27001, podle které je definován rozsah celého systému v organizaci a jeho správné definování je velmi důležité při implementaci.

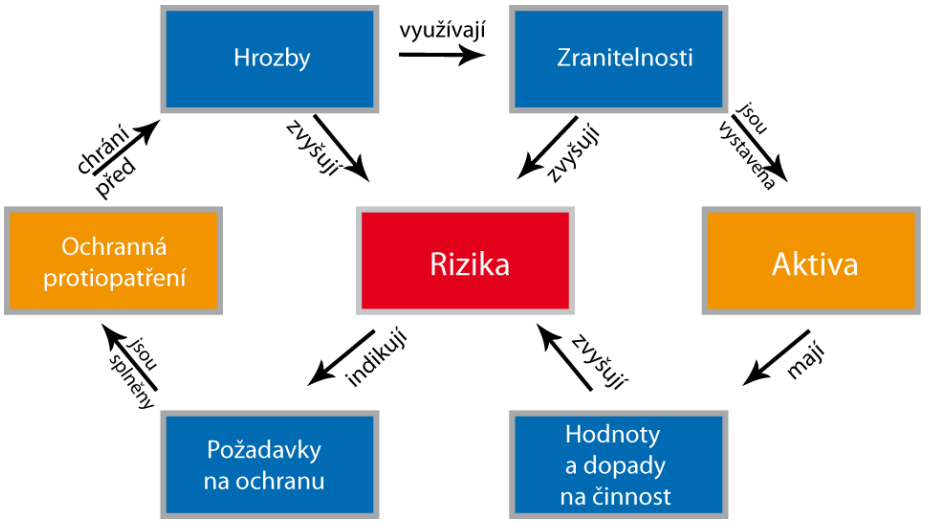
2 PROBLEMATIKA SYSTÉMŮ ŘÍZENÍ BEZPEČNOSTI INFORMACÍ (ISMS)

Systémy ISMS (Information Security Management System) lze jednoduše chápat jako efektivní a účinnou bezpečnou správu majetku společnosti, a to jak z pohledu informačních aktiv organizace, tak i informací, které organizaci svěřuje její zákazník. ISMS lze zavést do společnosti libovolné velikosti bez ohledu na obor či odvětví působení. Samotná implementace systému řízení informací je strategickým rozhodnutím managementu společnosti do její struktury, části či komplexně do společnosti celé. Hojné zavádění ISMS probíhá zejména díky efektivnímu dokumentovanému systému řízení a správě informací, která má za cíl co nejvíce eliminovat a potlačit jejich možnou ztrátu a poškození tím, že jsou určena aktiva, která se mají chránit. Dále se volí a řídí možná rizika bezpečnosti informací, zavádí se protiopatření s požadovanou úrovní záruk a následně je celý systém kontrolován a vyhodnocován. [1]

Ze zákonné podstaty podnikání vyplývá, že podnikatelský subjekt má povinnost evidovat svůj majetek a dokladovat jeho finanční hodnotu. Tento majetek je pak ve správě organizace a je adekvátně chráněn. Informace, stejně jako majetek, jsou chápány jako aktivum určité hodnoty, na němž závisí úspěch či neúspěch podnikání, a proto je nutností organizace jej chránit. Z těchto důvodů je zřetelné, že je potřeba pojmenovat a ohodnotit hrozby, které na aktiva působí, ale také zranitelnosti, které hrozbám předcházejí a jsou slabými místy aktiv společnosti. Bezpečnost informací je charakterizována zajištěním jejich důvěrnosti, dostupnosti a integrity. To znamená, že jsou informace dostupné pouze autorizovaným osobám, je zabezpečena jejich přesnost a autorizované osoby k nim mají přístup kdykoliv jej potřebují. [2]

2.1 Základní terminologie oblasti řízení rizik

Pro ucelené pochopení problematiky systémů pro řízení bezpečnosti informací je třeba znát termíny, které s tímto souvisí. Základní termíny jsou vždy součástí normy, podle které se daná organizace řídí. Jednotlivé vazby v oblasti řízení rizik, můžeme zřetelně vidět na Obr. 1.



Obr. 1: Schéma mechanismů v řízení informační bezpečnosti [1]

2.1.1 Aktivum

Jedná se o hmotný i nehmotný majetek organizace, respektive majetek, který má z pohledu bezpečnosti informací pro organizaci určitou hodnotu. U každého aktiva se předpokládá určitý ekonomický prospěch do budoucna. Aktivem mohou být budovy, stroje, zařízení, kapitál, cenné papíry ale i zaměstnanci, informace, předměty autorského a průmyslového práva nebo důležitá know-how společnosti.

Ohodnocení aktiv při analýze rizik je jedna z nejtěžších fází analýzy a to hlavně z důvodu subjektivity ohodnocení zainteresovanou osobou. Pro každou osobu v organizaci má každé aktivum jinou váhu a proto je při kvantifikaci a kvalifikaci aktiv postupovat velice obezřetně. Doporučuje se, aby toto bylo prováděno formou rozšířeného meetingu více osob, konferencí nebo brainstormingu, aby byla dosažena potřebná objektivita.

Norma ISO/IEC 13335-1:2004 definuje aktivum jako vše co má pro organizaci nějakou hodnotu.

2.1.2 Bezpečnostní incident

Jedná se o jednu nebo více událostí, která může, ale zároveň i nemusí, poškodit aktiva v organizaci. Při incidentu byla narušena důvěrnost, integrita nebo dostupnost informace. Za incident se dá považovat také porušení bezpečnostní politiky či snaha o překonání bezpečnostního opatření.

Incidenty mohou být automaticky monitorovány, jako například přihlašování na uživatelské počítače, nebo manuálně monitorovány, a to tak, že incident někdo nahlásí. Komplexní systém řízení rizik by měl mít ohodnocena nejen rizika, ale i incidenty jako například co bude organizaci stát to, pokud někdo prolomí bezpečnostní heslo a dostane se k interní důvěrné informaci. [2]

Bezpečnostní incidenty nelze brát na lehkou váhu a je třeba, aby byly pečlivě zaznamenávány a řízeny v rámci managementu incidentů. A to zejména z toho důvodu, abychom mohli další podobné incidenty odhalit, minimalizovat ztráty, které by mohli způsobit, ale abychom také mohli predikovat zranitelnosti a pokusili se je odstranit. V praxi jsou využitelné systémy pro monitoring a záznam bezpečnostních incidentů jako například SIEM, což je systém pro management bezpečnosti informací a událostí, který sbírá, provádí korelace, analýzy a následně vyhodnocuje události, které se v rámci systému objeví. [6]

Incident je normou ISO/IEC TR 18044:2004 definován jako identifikovaný výskyt určité události, při které je příležitost, pro narušení nebo chybu zabezpečení, nebo dopředu nepředpokládaná situace, která by mohla mít vliv na bezpečnost informací v rámci organizace, služby nebo sítě.

2.1.3 Hrozba

Hrozba může být aktivita, osoba nebo událost, která může poškodit nebo mít nežádoucí vliv na určitá aktiva. Dá se také říct, že hrozba je potenciální příčina incidentu. Škodná událost, kterou hrozba zanechá na aktivu, se nazývá dopad hrozby. Pod dopadem hrozby si můžeme představit určité náklady, které jsou potřebné vynaložit na obnovení činnosti aktiva nebo eliminaci následků hrozby. Konkrétním případem hrozby může být výpadek elektrického proudu, výpadek služeb internetu, přírodní katastrofa, ale i kontrola finančního úřadu či růst nebo pokles kurzu měny. [2]

Hrozby je možno rozdělit dle několika způsobů, nejčastěji je to dle úmyslu, kam patří:

- Úmyslné hrozby – jedná se o plánované hrozby, při kterých útočník využil určitých znalostí, kapacit a zdrojů
- Neúmyslné hrozby – jsou klasifikovány jako hrozby náhodného charakteru – tyto hrozby mohou být ovlivněny například tím jak je organizace umístěna od silničních nebo železničních tras, jsou-li v její blízkosti průmyslové závody pracující s nebezpečnými či chemickými odpady atp.

Dále mohou být hrozby klasifikovány dle zdroje a to:

- Vnitřní – hrozby, jejichž příčina může vzniknout uvnitř organizace
- Vnější – hrozby, jejichž zdroj přichází zvenčí nebo okolí podniku

Norma BS ISO/IEC 1335-1:2004 o hrozbě říká, že to může být potenciální příčina incidentu, která může vyústit v poškození systému nebo společnosti jako celku.

2.1.4 Zranitelnost

Zranitelností aktiva by se dala nazvat jeho slabina, která může být využita jednou nebo více hrozbami s určitým dopadem. Jedná se o hodnotu, která nám říká, jak je aktivum citlivé či imunní vůči dané hrozbě. Příkladem vyšší zranitelnosti může být slabé heslo pro přístup na zaměstnanecký počítač.

- Citlivost – ukazatel jak je dané aktivum náchylné na poškození hrozbou
- Kritičnost – to jak je aktivum pro analyzovaný subjekt důležité

Zranitelnost je normou BS ISO/IEC 1335-1:2004 charakterizována jako slabina či slabá stránka aktiva, jež může být potenciálně využita jednou nebo více hrozbami.

2.1.5 Riziko

Je to možnost, při které určitá hrozba využije slabiny, jinak řečeno zranitelnosti aktiva a způsobí tak na něm ztrátu, škodu či ho nenávratně zničí. Úroveň rizika je dána hodnotou aktiva, jeho zranitelností a velikostí hrozby. Jediná možnost jak riziko snížit či potlačit je zavedení protiopatření, jež by mělo ctít zásadu, že náklady vynaložené na protiopatření nesmí být větší než hodnota daného aktiva. Aktivum, na které nepůsobí žádná hrozba je z analýzy rizik vyloučeno. Tudíž nebudeme počítat hodnotu rizika pro aktivum papírové dokumenty, na které nemůže působit hrozba útok hackera. Po provedení náležitých opatření se akceptuje tzv. zbytkové riziko, proti němuž se již nečiní žádná další opatření a může být prohlášeno jako přijatelné. Úroveň dopadu hrozby na aktivum by měla být taktéž na nízké úrovni, aby jej bylo možné zanedbat.

Definice rizika dle ISO Guide 73:2002 udává, že se jedná o kombinace pravděpodobnosti vyskytnutí určité události, která bude mít jisté následky.

2.1.6 Protiopatření

Je to jakýkoliv proces, postup či procedura, která vede k eliminaci nebo potlačení hrozby a jejího dopadu, jež na aktivum působí. Protiopatření jsou nasazována pro zmírnění nebo předejití škody. Protiopatření je z hlediska analýzy rizik charakterizováno poměrem nákladů a dosažené efektivity. Efektivita protiopatření je používána v plánu zvládání rizik a slouží jako jeden z hlavních parametrů pro vyhodnocování aplikovatelnosti daných opatření a vyjadřuje nám, nakolik nám aplikované protiopatření snížilo účinek dané hrozby. Efektivita protiopatření se používá ve fázi zvládání rizik a je to hlavní parametr pro posouzení vhodnosti protiopatření. Do nákladu za protiopatření se kalkulují jak náklady na pořízení a aplikování, tak náklady na provozování protiopatření. [2]

Plán zvládání rizik spočívá ve vhodné volbě metody pro zvládání rizik. Tyto metody jsou následující:

- Ignorace rizika – nejhorší případ, kdy management o riziku neví nebo o něm ví, ale nečiní žádné úsilí pro jeho eliminaci či snížení
- Akceptace rizika – tato metoda by měla být aplikována pouze pro zbytková rizika, která mají pro organizaci únosnou úroveň, avšak v praxi se bohužel často tato metoda aplikuje i na rizika, jež mají velký potenciál poškodit zásadní aktiva společnosti
- Redukce rizika – cílem této metody zvládání rizik je snížit dané riziko na únosnou hranici a poté riziko prohlásit za akceptovatelné, přičemž je tato metoda aplikovatelná na všechna rizika, u kterých je vysoká pravděpodobnost výskytu hrozby
- Vyhnutí se riziku – k této metodě je přistupováno, pokud se riziko jeví jako kritické a ostatní metody zvládání rizik selhávají – akceptace rizika není možná a výskyt hrozby je jistý
- Přenesení rizika – jedná se o transfer rizika na jiný subjekt, například ekonomicky silnějšího partnera – z dceřiné společnosti na mateřskou, z organizace na pojišťovnu či z organizace na společnost poskytující outsourcing [2]

2.1.7 Analýza rizik

Analýzou rizik se rozumí systematické používání informací pro výpočet míry rizika a určení jeho ohnisek. Je to první krok procesu snižování rizik organizace. Analýza rizik je také chápána jako definování aktiv společnosti, charakteristika hrozeb, jejich pravděpodobnost a dopad na aktiva, respektive stanovení rizika a míry jejich závažnosti. Analýza rizik je součástí

managementu rizik a její fáze jsou následující:

1. Identifikace aktiv organizace
2. Stanovení hodnoty aktiv
3. Charakterizování hrozeb a slabých míst
4. Stanovení závažnosti identifikovaných hrozeb a míry zranitelností aktiv

Na začátku analýzy rizik je třeba stanovit, na jakou úroveň budeme chtít rizika eliminovat. Nikdy nemůžeme eliminovat všechna rizika, neboť by to vedlo k astronomickým nákladům při realizaci protiopatření, ale také proto, že 100% bezpečnosti nelze nikdy dosáhnout. Je proto třeba definovat jasný a transparentní přístup jak budeme k analýze rizik přistupovat, jak budeme posuzovat zbytková rizika, nebo-li rizika která jsme schopni akceptovat a podle zvolené úrovně vybereme přístup a metodu analýzy rizik. [2]

Je třeba myslet na to, že čím kvalitněji je provedená vstupní analýza rizik, tím důvěryhodnější bude následné řízení rizik. Při hodnocení rizik je neustále potřeba zvažovat:

a) Poškození aktiv, což může být způsobeno naplněním scénářů hrozeb, včetně uvedení všech důsledků
b) Reálnost výskytu takovýchto rizik při přihlédnutím na převažující hrozby, zranitelnosti a aktuálně aplikovaná opatření [8]

Analýza rizik je dle ISO Guide 73:2002 využití informací pro odhad míry rizika a k určení zdrojů z kterých pramení. [2]

2.2 Systém řízení bezpečnosti informací (ISMS)

Systém řízení bezpečnosti informací, zkratkovitě ISMS z anglického Information Security Management System, se týká zejména organizací, které potřebují spravovat důležité firemní i provozní informace jak v listinné, tak elektronické podobě, využívajíc k tomu informační technologie či informační systém.

Pojem ISMS primárně zavedla norma ISO/IEC 17799, což je mezinárodní norma přejatá z Britského standardu BS 7799-1:1999, jež byla publikována Mezinárodní organizací pro normalizaci (ISO) roku 2000. Novější verze, která byla revidována a je součástí nové řady norem v oblasti bezpečnosti informací nese název ISO 27000.

2.2.1 Normalizace v oblasti ISMS

V případě managementu bezpečnosti informací (ISMS) se jedná o systém, který je

dokumentovaný a ve kterém jsou chráněna definovaná informační aktiva, řízena rizika bezpečnosti informací a následná opatření jsou kontrolována. Tento pojem byl původně zaveden normou ISO/IEC 17799, což byla norma převzatá z britského standardu BS 7799-1:1999 publikovaná roku 2000 Mezinárodní organizací pro normalizaci (ISO). Řada ISO 27000 byla rezervována pro normy, které se týkají bezpečnosti informací, podobně, jako je tomu tak v případě řízení kvality, pro kterou platí normy série ISO 9000. Rodina norem ISO 27000 obsahuje definice pojmů a terminologický slovník pro všechny ostatní normy z této série. Norma byla publikována v roce 2005. V současné době se pro posuzování implementace ISMS používá původní Britský standard převzatý do české národní soustavy jako norma ISO/IEC 27001, podle které se taktéž provádí certifikace.

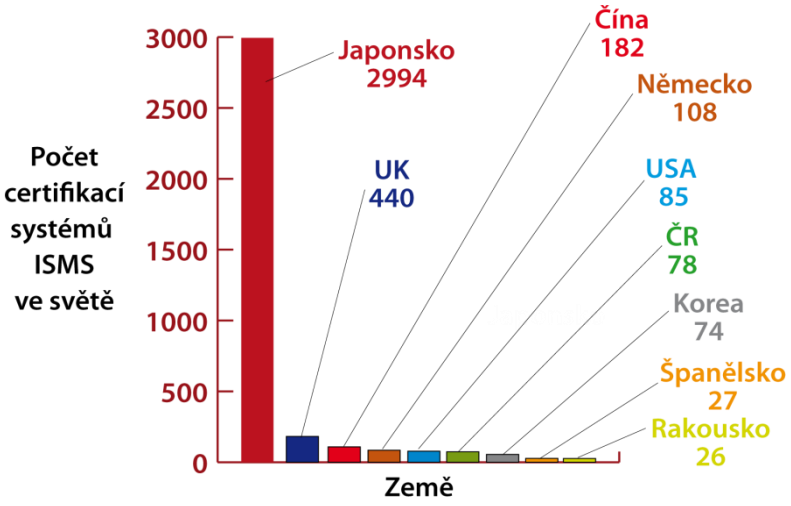
Stejně jako v jiných oblastech je snaha společností být v souladu s touto normou a to zejména z následujících důvodů:

- zavedení komplexního řízení bezpečnosti – upuštění od neuceleného a nesystémového ISMS
- řízení a kontrola investic do ISMS
- transparentnost a inventura vlastních aktiv, jejich kvantifikace a klasifikace
- potlačení nebo odstranění rizik co se týče oblasti informačních systémů
- snaha o vyšší povědomí zaměstnanců při práci s informacemi, které mohou být pro společnost zásadní
- vyšší konkurenceschopnost a důvěryhodnost pro klienty, partnery a dodavatele
- plnění legislativy
- zlepšení image firmy navenek a kultivace firemní kultury

Při zavádění systému řízení bezpečnosti informací se tedy postupuje dle ČSN ISO/IEC 27002:2006, která skýtá doporučení nejlepších postupů tzv. best practices.

Česká republika poměrně brzy začala s implementacemi systému bezpečnosti informací do firemního prostředí, tudíž má dobré postavení co se týče počtu certifikačních auditů a úspěšných certifikací v rámci průzkumu zapojení celého světa. Na následujícím obrázku Obr. 3 můžeme vidět, jak si ČR stojí v porovnání se světovými velmocemi. Z obrázku je patrné, že zcela výsadní postavení, co se do počtu certifikací ISMS týče, má Japonsko. S velkým odstupem následuje Velká Británie, Čína či Německo. Česká republika se nachází přibližně uprostřed, co do pořadí úspěšných certifikací ISMS. Významný podíl na tomto mají auditoři Elektrotechnického zkušebního ústavu, jež je členem Českého sdružení pro certifikaci

systémů jakosti CQS. [7]



Obr. 3: Zastoupení jednotlivých zemí co do počtu certifikací ISMS [7]

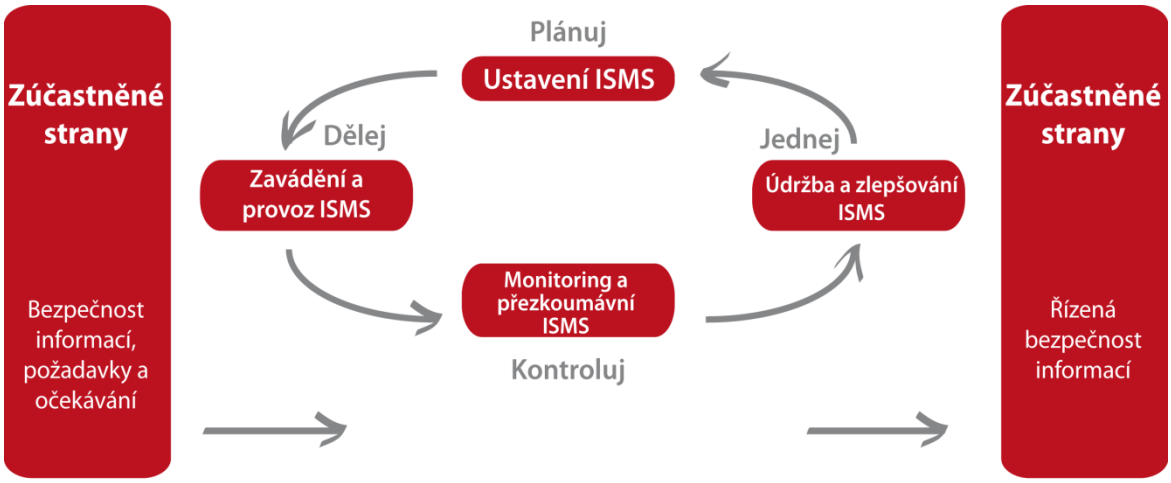
2.2.1.1 Norma ČSN ISO/IEC 27001

Struktura této normy pro certifikační audit obsahuje osm částí. První část se týká předmětu normy, následují normativní odkazy, termíny a definice, systém managementu bezpečnosti informací, odpovědnosti managementu, interní audity ISMS, přezkoumání vedením organizace a konečně zlepšování ISMS. Jako příloha této normy jsou uvedeny normativní cíle opatření a jednotlivá opatření.

Je to tedy hlavní norma pro systém řízení bezpečnosti informací, jež byla publikována v říjnu 2005, poskytující popis vhodného systému řízení, strukturu a procesy pro ISMS podle opatření, které byly definovány v ISO/IEC 27002. Hlavní části této normy jsou rovněž uvedeny v příloze certifikační normy ISO/IEC 27001.

Podle této normy je definován rozsah celého ISMS a jeho správná definice je zásadní při implementaci do organizace. Systém řízení bezpečnosti nemusí zahrnovat celou organizace, ale pouze její část, pro kterou po úspěšné certifikaci platí vydaný certifikát.

Norma ISO/IEC 27001 zavádí model PDCA aneb Plánuj-Dělej-Jednej-Navrhni opatření (kontroluj), který byl zaveden již do normy BS 7799:2002. To byla převratná novela, která se podobala novele normy ISO 9001:2000 týkající se managementu jakosti. Na Obr. 4 můžeme vidět strukturu modelu PDCA, jakožto základní kroky pro dosažení nepřetržitého a kontinuálního zdokonalování.



Obr. 4: Princip modelu PDCA (Plan-Do-Check-Act) [7]

V první fázi **Plánuj** (Plan) se definuje bezpečnostní politika, plány, cíle, procesy a procedury, které souvisejí se systémem řízení rizik a ISMS. Toto musí korespondovat s celkovou firemní kulturou, politikou a cíli organizace. V této fázi modelu PDCA jsou postupně řešeny tyto kroky:

- Definice rozsahu a politiky ISMS
- Určení systému přístupu k hodnocení rizik
- Identifikace, analýza a vyhodnocení rizik
- Zrevidování cílů opatření a jednotlivých opatření pro zvládání rizik
- Akceptace hladiny zbytkových rizik vedením
- Souhlas vedení k implementaci a provozu ISMS
- Prohlášení o aplikovatelnosti (SoA)

V další fázi procedury PDCA **Dělej** (Do) se zavede bezpečnostní politika, řízení a procedury. Jedná se zejména o:

- Formulování plánu zvládání rizik (PZR)
- Zavedení plánu zvládání rizik a bezpečnostních opatření
- Určení metriky pro měření účinnosti implementovaných opatření
- Řízení provozu, údržby a zdrojů ISMS
- Zavedení procedur pro zjištění, reakci a dopad bezpečnostních incidentů

Ve fázi **Kontroluj** (Check) se ověřuje úroveň testu, výsledků a zda-li jich bylo dosaženo. V případě se vyskytují určité odchylky, je třeba se zaměřit na problémy a překážky, které zlepšení brání. Provádí se zde:

- Monitorovací procedury
- Přezkum účinnosti systému řízení informační bezpečnosti
- Přezkum úrovně zbytkového a akceptovatelného rizika
- Interní audit a analýza řízení ISMS
- Aktualizace bezpečnostních plánů
- Zaznamenání činností a událostí, které mají vliv na ISMS

V konečné fázi tohoto přístupu **Jednej** (Act) se využije nápravných opatření a prevencí, které jsou založeny na výsledcích analýzy řízení, aby bylo dosaženo kontinuální a nepřetržité zlepšování ISMS. Koná se:

- Implementace zlepšení, které byly identifikovány
- Provedení nápravných a preventivních akcí
- Konzultace výsledků a návrhů pro zlepšení s vedením a zainteresovanými stranami
- Garance zlepšení zdokumentovaných cílů

Norma ČSN ISO/IEC 27001 je propojena s normami ČSN ISO/IEC 9001:2000, která se týká managementu kvality a také s ČSN ISO/IEC 14001:1996 týkající se environmentálního managementu. Propojení a kompatibilita jednotlivých norem je zaručena z důvodu podpoření konzistentního a jednotného zavedení, zejména provozu. Součástí ČSN ISO/IEC 27001 je přímé srovnání kapitol norem ČSN ISO/IEC 9001:2000 a ČSN ISO/IEC 14001:1996 s ČSN ISO/IEC 27001. Jedná se o systémy řízení, přičemž organizace má jeden systém řízení, který splňuje požadavky více norem.

2.2.1.2 Norma ČSN ISO/IEC 27002

Struktura této normy odpovídá struktuře ČSN ISO/IEC 27001 a sestává se z nejlepších bezpečnostních praktik a příkladů z praxe, což může být využito jako kontrolní seznam praktik, které je potřeba učinit pro bezproblémový chod ISMS v podniku. Aktuální verze normy byla publikována roku 2005 (ISO/IEC 27002:2005) a je mezinárodně přijatým standardem v této oblasti.

Norma ČSN ISO/IEC 27002 se skládá z 11 základních oddílů bezpečnosti, jež jsou dále rozděleny do dalších 39 kategorií bezpečnosti. Do výčtu obsahu této normy náleží:

- Bezpečnostní politika
- Organizace a bezpečnost
- Klasifikace a řízení aktiv
- Bezpečnost lidských zdrojů
- Fyzická bezpečnost a bezpečnostní prostředí
- Řízení komunikací a provozu
- Řízení přístupu
- Vývoj, údržba a rozšíření ISMS
- Zvládání bezpečnostních incidentů
- Řízení kontinuity činností organizace
- Soulad s požadavky

V jedenácti hlavních oddílech této normy je zohledněno 39 cílů pro ochranu informačních aktiv proti narušení důvěrnosti, dostupnosti a integrity. Cíle opatření poskytnou dostatečný základ pro definici sady tvrzení pro bezpečnostní politiku. Avšak ne všechny jsou aplikovatelné v specifickém firemním prostředí a proto je třeba určité přeformulování nebo přizpůsobení aktuálním podmínkám a potřebám organizace.
Norma jako všechny ostatní neobsahuje požadavky, ale návody na splnění požadavků z normy ČSN ISO/IEC 27001. Co všechno musí být ve skutečnosti implementováno a ponechává rozhodnutí na zainteresovaných osobách. Cíl není aplikovat veškerá opatření, které norma obsahuje, ale spíše naplnit aplikovatelné cíle opatření. Toto zajišťuje velkou flexibilitu a volnost uživatelům při implementaci, avšak může přivodit potíže při certifikaci, protože může být složité posoudit, zda-li jsou aktuální bezpečnostní opatření v souladu s příslušnou normou.

2.2.1.3 Norma ČSN ISO/IEC 27005

Základem této normy, jejíž poslední publikace byla vydána v červenci roku 2009, jsou revize dříve vydaných norem ISO/IEC TR 13335-3:1998, ISO/IEC TR 13335-4:2000 a některé oddíly z normy britské normy BS 7799-3. Norma ČSN ISO/IEC 27005 obsahuje věcná doporučení a techniky pro analýzy informačních rizik a stejně jako norma 27002 se ohlíží na požadavky ISMS dle ISO/IEC 27001:2005. Mezi činnosti, které čítá tato norma, patří například:

- Stanovení kontextu – základní specifika pro řízení bezpečnosti informací, definice rozsahu a hranic a také organizační struktury pro řízení rizik
- Hodnocení rizik – analýza, kvantifikace a kvalifikace rizik a definice prioritních rizik pro soulad s kritérii a cíli hodnocení rizik
- Zvládání rizik – analýza protiopatření k potlačení či odstranění rizika, vyvarování se rizika nebo jeho přenosu a definice plánu zvládání rizik
- Akceptace rizik – akceptování a formální zdokumentování akceptovatelné hladiny rizik včetně odpovědnosti za toto rozhodnutí
- Monitoring a přezkoumávání – sledování rizik a jejich přezkoumávání [5]

2.2.2 Rizikové faktory ISMS

Pokud bychom hledali nejrizikovější faktory v typické organizaci, což jsou určité příčiny vzniku rizik, které zvyšují jeho pravděpodobnost, jistě bychom na první místo zařadili personál a zaměstnance firmy, zejména její management. Je statisticky dokázáno, že 50 – 80 % ztrát informací způsobí management vlastní organizace. Tento fakt je ovšem dán tím, že management pro svou práci a zejména pro rozhodování potřebuje co nejširší spektrum informací, což platí zejména pro rizika porušení důvěrnosti informací. Zaměstnanci společnosti se také ovšem mohou stát zranitelným kvůli hrozbám tzv. sociálního inženýrství, kdy útočník využívá důmyslné manipulace a zneužívá důvěřivosti a slabosti zaměstnance firmy. Jako příklad těchto hrozeb by se dalo uvést prozrazení přístupů na počítače obsahující zásadní agendu pro chod společnosti, volný přístup do kanceláří s kompromitujícími informacemi či přímo úmyslné poškození některých nosičů informací. [1]
V některých typech organizací mohou být také vysoká rizika v oblasti hardwarových prostředků, což může čítat například ztrátu důležitých dat vlivem poškození pevných disků počítačů, síťových serverů, zásadních databází uložených na externích médiích a podobně.
S rychlým vývojem informačních technologií dochází ke zvyšování míry informačních rizik. V dnešní době je také moderní používat výraz kybernetická kriminalita, kdy prostřednictvím globálních sítí dochází k úniku či kompromitaci důležitých informací při takřka stoprocentní anonymitě útočníka či hackera. Samozřejmě ne vždy dochází k úmyslnému útoku na informační média, což by se dalo nazvat jako nevědomý zásah do informační bezpečnosti, kam by mohla být začleněna například neautorizovaná a neúmyslná modifikace některých záznamů, nesprávné použití zdrojů a aktiv, nesprávné použití zařízení zpracovávající informace, chyba údržby systémů či neúmyslné zničení některých záznamů a záznamových

médií.

Rizika se dají vyčíslit buďto kvantitativně nebo kvalitativně a při jejich vyčíslování nemusí být započítávány pouze nebezpečí od třetích stran a zaměstnanců společnosti, ale i například živelné katastrofy jako povodeň, úder blesku, požár, zemětřesení, ale i selhání podpůrných funkcí jako je dodávka elektřiny, dodávka vody, centrální vytápění, ventilace či klimatizace.

Další nezanedbatelné riziko představuje riziko spojené s dodavateli, zákazníky a jinými podnikatelskými subjekty, tudíž rizika, která mohou mít zásadní vliv na budoucnost fungování celé společnosti. Do této kategorie můžeme zařadit hrozby jako ztráta image či porušení smluvních závazků, což mohou být kritické faktory pro budoucí fungování celé firmy. [3]

2.2.2.1 Kvantitativní analýza rizik

Kvantitativně lze následky vyhotovených scénářů vyjádřit financemi nebo-li peněžními jednotkami, tzn. jaké budou ztráty při naplnění určitého scénáře. Popis každého scénáře musí umožnit finančně kvantifikovat následky dobrého jména firmy, ztráty podílu na trhu, náklady na odškodné atd.

Kvantitativní analýza rizik je vysoce náročná jak na zdroje, tak na čas, protože je náročné, někdy i nemožné stanovit peněžní hodnotu aktiva, když se v případě AMI Praha a.s. jedná o zdrojové kódy, přístupová práva klientů, osobní data pracovníků atd.

Výhodou kvantitativní analýzy však je jednodušší rozhodování při práci s plánem zvládání rizik a následným výběrem vhodných protiopatření.

2.2.2.2 Kvalitativní analýza rizik

Tento druh analýzy je méně náročný na zdroje i čas, kdy není potřeba uvádět přesnou finanční hodnotu aktiva, avšak není zde tak vysoká kontrola nákladů ve fázi zvládání rizik, když vybíráme optimální protiopatření.

Vyjádření škody finančními prostředky má velké plus v tom, že umožňuje porovnat výši škod v případě realizace konkrétní hrozby s celkovými náklady na protiopatření. Takovéto objektivní porovnání nemůže být nikdy docíleno v kvalitativní metodě, neboť klasifikace rizika jako nízké, střední, vysoké může být velmi subjektivní. [4]

2.2.3 Náklady na ISMS

V případě implementace ISMS do společnosti kteréhokoliv druhu se zajisté nabízí námitka, že minimalizovat všechna současná rizika informační bezpečnosti musí být velmi nákladné a dovolit si to mohou finančně silné subjekty a organizace. Jak již bylo zmíněno v předešlé části, zřejmě nejvíc kritickou oblastí do které by měla společnost investovat je personalistika a to konkrétně věnování času na trénink zaměstnanců a budování povědomí o zásadách informační bezpečnosti. Faktem také je, že prakticky žádná existující firma nezačíná s opatřeními v oblasti informační bezpečnosti od nuly. Organizace potřebuje přiměřený, efektivní systém managementu bezpečnosti informací, který vychází z hodnocení rizik. Management pak musí stanovit kritickou hodnotu akceptovatelného rizika, kterou může v čase posouvat. Pouze rizika, která v daném okamžiku přesahují stanovený práh, je nutno ošetřit bezpečnostními opatřeními. Tento pragmatický přístup umožňuje managementu vyvarovat se bezhlavého investování a stanovovat priority investic podle míry rizik a tím pádem splnit reálného a schválený rozpočet.

2.2.4 Implementace ISMS do organizace

Implementace efektivního ISMS požaduje velké znalosti v oblasti bezpečnosti informací, přehled o metodikách a jejich vhodnosti, praktické znalosti norem ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27004, ISO/IEC 27005 a dalších. Ve skutečnosti proto nebývá příliš časté, aby se organizace věnovala samotné implementaci ISMS do své firemní kultury. Zkušenosti z praxe říkají, že je třeba se také vyvarovat některých „poradců“, kteří implementují tzv. unifikované systémy managementu, načež dojde ke zkopírování dokumentace z jedné firmy do druhé s malým pozměněním a přizpůsobením identifikačních údajů. Odpovědný manažer organizace se samozřejmě může přiklonit k rozhodnutí implementovat takovýto způsob řízení rizik informační bezpečnosti, nicméně již z principu nemůže dojít k potřebnému výslednému efektu, kterým je kontrola rizik důležitých informačních aktiv, jichž si organizace velice cení a jsou takřka životně důležitá pro její fungování a správný chod.
Lze použít metodické přístupy k analýze, hodnocení a řízení rizik, které se osvědčily v jiných firmách podobného odvětví či druhu, avšak metodika pro analýzu a řízení rizik by měla být vždy přiměřená charakteru a velikosti organizace, její bezpečnostní politice a celkově jejímu přístupu k bezpečností politice. Stejně tak tomu bude u soupisu veškerých aktiv společnosti, který již z principu bude pro každou organizaci vždy odlišný a související hrozby, které se vážou na konkrétní potencionální bezpečnostní rizika. Stejně tak tomu bude i s plánem zvládání rizik a k němu náležícím bezpečnostní opatření a protiopatření. Z těchto důvodů

proto nelze unifikovat či individualizovat přístup k řízení bezpečnostních incidentů, havarijní připravenosti, tréninku a školení personálu či dalším záležitostem, která jsou zásadní pro implementaci a správný chod ISMS ve společnosti.

Z výše uvedených aspektů vyplývá, že ISMS není pouze pro organizace, působící v oblasti informačních technologií. Implementace systému managementu bezpečnosti informací se týká všech firem, které chtějí chránit svoje kritické informace a zejména know how jejich podnikání. Dále však také svoje marketingové, obchodní, účetní aktivity či personální agendu, která má nemalou váhu pro správný chod organizace. Proto nezáleží na oboru činnosti, charakteru a velikosti organizace, ale zejména na tom, jak si management uvědomuje hodnotu spravovaných informací, které chce racionálně a účinně chránit.

Právě proto bychom měli v souvislosti s ISMS položit důraz především na ty typy organizací, které působí ve specifickém odvětví a mají velkou odpovědnost za duševní majetek svých klientů a zákazníků. Mezi takovéto subjekty určitě patří zdravotnická zařízení, advokátní kanceláře, společnosti zabývající se outsourcingovou správou informačních technologií, poskytovatelé hostingových služeb a v neposlední řadě též státní správa, úřady a všechny subjekty, které spravují informace o fyzických i právnických osobách.

Samotná implementace ISMS může být v dnešním tvrdém konkurenčním prostředí vysoce zásadní a to z důvodu toho, že zákazníci po svých dodavatelích požadují jasný doklad o uplatňování důvěryhodných postupů v oblasti bezpečnosti informací. K těmto náročným zákazníkům již patří státní správa, dále výrobci, kteří poskytují svou výrobní dokumentaci dodavatelům, firmy, které si vývoj zajišťují externě a kooperují s dalšími podnikatelskými subjekty apod. Takovým důkazem důvěryhodnosti pro zákazníky může být certifikát ISMS vydaný certifikačním orgánem, který při auditu nezávisle posoudí a potvrdí, že informační bezpečnost je v organizaci řízena systémově ve shodě s mezinárodním standardem či příslušnými normami. [1]

2.2.5 Pravidelné činnosti managementu rizik

Pouhou implementací systému řízení rizik tento proces zdaleka nekončí. Management bezpečnostních rizik je soustavná a trvalá činnost, v případě menších společností se týká pouze části pracovních povinností zejména z důvodu vysokých nákladů na specializované pracovníky v oblasti ISMS. Tato činnost by měla být přidělena specializovanému pracovníkovi v rámci organizace anebo outsourcingové společnosti, která bude jednotlivá rizika řídit. Nesmí se však opomenout, že odpovědnost za řízení rizik zůstává v organizaci. Ve většině organizací je však jasně určen manažer bezpečnosti rizik s jasně danou

odpovědností za ISMS.

Tyto osoby či týmy pro řízení rizik musí umět zejména:

- systematicky řídit a organizovat přístup k monitorování známých a rizik a navrhování vhodných opatření, protiopatření atd.
- sledovat priority jako politiku, cíle, poslání a současný stav celé společnosti
- naslouchat a vnímat opačné názory a zároveň jim vyjít vstříc, pokud je to nejlepší pro firmu
- prezentovat potřeby velice přesvědčivým způsobem, hlavně co se týče vyšších výdajů na eliminaci rizik
- dobře komunikovat na všech úrovních společnosti
- porozumět problematice rizik, mít znalost bezpečnostních technologií a IT řešení

Aplikovaná řešení musí být neustále kontrolovány a monitorovány, aby bylo zajištěno správné a efektivní fungování dané implementace. Velké množství nástrojů bezpečnosti informací vyžaduje pravidelnou údržbu ale také administrativní podporu. Tyto operace musejí být organizované a periodicky se opakující, aby byly informace stále aktuální např. seznam aktiv, objevující se nové hrozby a incidenty.

Informace pro přezkoumávání systému managementu rizik vychází z informací od uživatelů ISMS, empirických zkušeností a příkladů, auditních zpráv či interním a externím přezkoumávání, porovnávání a měření produktů a služeb. [2]

3 SEZNAM POUŽITÉ LITERATURY

[1] ISMS : SystemOnline.cz [online]. CCB spol. s r.o., c2001-2009 [cit. 2009-01-01]. Dostupný z WWW:<http://www.systemonline.cz/it-security/bezpecnost-informaci-se-netyka-jen-it-firem-1.htm>.

[2] Doc. Ing. ŠEBESTA, DrSc., Ing. ŠEBESTOVÁ, Ing. ŠTVERKA, Ing. STEINER, PhD., Mgr. SEDLÁČEK. Systém managementu bezpečnosti informací. ZČU Plzeň. Plzeň [s.n.], 2007. 90 stran. ISBN 978-80-7283-239-2.

[3] Doc. Ing. ŠEBESTA, DrSc., Ing. ŠEBESTOVÁ, Ing. ŠTVERKA, Ing. STEINER, PhD. Praktické zkušenosti z impementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005. ZČU Plzeň. Plzeň.[s.n.], 2007. 70 stran. ISBN 80-7283-204-2

[4] Analýza rizik [online]. Miroslav Čermák [cit. 2010-25-7]. Dostupný z WWW:< http://www.cleverandsmart.cz/analyza-rizik-kvantitativni-vs-kvalitativni/>.

[5] Normy z oblasti ISMS [online]. Risk Analysis Consultants s.r.o., c2012. Dostupný z WWW:<www.iso27000.cz>.

[6] Auditing a monitoring [online]. Miroslav Čermák [cit. 2010-31-8]. Dostupný z WWW:< http://www.cleverandsmart.cz/siem-auditing-a-monitoring//>.

[7] ISMS podle ISO/IEC 27001 : SystemOnline.cz [online]. CCB spol. s r.o., c2001-2009 [cit. 2009-01-01]. Dostupný z WWW:< http://www.systemonline.cz/it-security/management-bezpecnosti-informaci-podle-iso-iec-27001.htm>.

[8] Riziko a nalýza rizik [online]. Czech Trade, c1997-2012. Dostupný z WWW:< http://www.businessinfo.cz/cz/clanek/rizeni-rizik/co-je-to-riziko-a-analyza-rizik/1001617/42740/>.