Systém ochrany informačního a komunikačního systému organizačních celků

The System of Protection of Information and Communication Systém of Organizational Units

Vladimír Čechmánek

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vladimír ČECHMÁNEK**
Osobní číslo:	**A10809**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Systém ochrany informačního a komunikačního systému organizačních celků**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Popište bezpečnostní politiku informačního a komunikačního systému organizačního celku.**
3. **Popište problematiku personální bezpečnosti v sytému ochrany informačního a komunikačního systému.**
4. **Vymezte práva a povinnosti při správě a užívání informačního a komunikačního systému.**
5. **Stanovte pravidla a zásady bezpečného řízení a užívání informačního a komunikačního systému.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.**
2. **JAŠEK, Roman. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-7318-456-7.**
3. **JAŠEK, Roman. Ochrana znalostí a dat v podnikových informačních systémech. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 80-7318-095-2.**
4. **Zákon o ochraně utajovaných informací a bezpečnostní spolehlivosti. In: 412/2005 Sb. 2005.**
5. **Zákon o ochraně osobních údajů a o změně některých zákonů. In: 101/2000 Sb. 2000.**
6. **ČERMÁK, Miroslav. Řízení informačních rizik v praxi. V Tribunu EU. Vyd. 1. Brno: Tribun EU, 2009, 134 s. ISBN 978-80-7399-731-1.**
7. **BASL, Josef. Podnikové informační systémy: podnik v informační společnosti. 2., výrazně přeprac. a rozš. vyd. Praha: Grada, 2008, 283 s. ISBN 978-80-247-2279-5.**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Cílem práce bylo vytvořit literární rešerši na dané téma. Práce se zabývá bezpečnostní politikou informačního a komunikačního systému organizačního celku. Popisuje bezpečnostní politiku informačních a komunikačních systémů a problematiku personální a v systému ochrany informačního a komunikačního systému, která je jednou z nejčastějších příčin vzniku bezpečnostních incidentů. V práci jsou vymezena práva a povinnosti při správě a užívání informačního a komunikačního systému a stanovena pravidla a zásady bezpečného řízení a užívání informačního systému.

Klíčová slova: Bezpečnostní politika, bezpečnostní rizika, informační bezpečnost, bezpečnostní incident, řízení rizik.

ABSTRACT

The aim of my thesis was to create literature research on the topic. The thesis deals with security policy of information and communication systems of organizational unit. It describes the security policy of information and communication systems and also the personnel issue in the systems, which is one of the most common causes of security incidents. In this thesis are defined the rights and duties that are necessary for management and the use of information and communication systems and rules and principles of safe management and the usage of information system.

Keywords: security policy, security risk, information security, security incident, risk management.

Děkuji vedoucímu bakalářské práce Ing. Miroslavu Matýskovi, PhD., za odborné vedení, metodiku, připomínky, rady a čas který mě věnoval. Dále taky své rodině za podporu a trpělivost, kterou se mnou v kritických okamžicích měla. V neposlední řadě chci poděkovat svému zaměstnavateli za vytvoření podmínek potřebných ke studiu.

Motto:

Každý systém je tak silný, jak je silný jeho nejslabší článek.

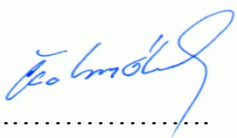
Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně



……
podpis diplomanta

OBSAH

ÚVOD **10**
I TEORETICKÁ ČÁST **11**
1 POJMY BEZPEČNOSTI INFORMAČNÍHO A KOMUNIKAČNÍHO SYSTÉMU **12**
1.1 DEFINICE ICT 12
1.2 INFORMAČNÍ BEZPEČNOST 12
1.3 BEZPEČNOST ICT 12
1.4 AKTIVA 13
1.5 BEZPEČNOSTNÍ INCIDENT 13
1.6 INTEGRITA 14
1.7 DŮVĚRNOST 14
1.8 DOSTUPNOST 14
1.9 IDENTIFIKACE 14
1.10 AUTENTIZACE 14
1.11 AUTORIZACE 15
1.12 AUDIT 15
1.13 HROZBA 15
1.14 ÚTOK 15
1.15 ÚTOČNÍK 16
1.16 ZRANITELNOST 16
1.17 RIZIKO 17
1.18 OPATŘENÍ 17
1.18.1 Charakter opatření 17
1.18.2 Cíle opatření 18
2 BEZPEČNOSTNÍ POLITIKA ICT **19**
2.1 FYZICKÁ BEZPEČNOST 20
2.2 PERSONÁLNÍ BEZPEČNOST 20
2.3 KOMUNIKAČNÍ BEZPEČNOST 21
2.4 ADMINISTRATIVNÍ BEZPEČNOST 21
2.5 ANALÝZA RIZIK 22
2.5.1 Identifikace aktiv 23
2.5.2 Identifikace hrozeb 23
2.5.3 Vlastní analýza rizik 23
2.6 NÁVRH SYSTÉMU OCHRANY 24
2.7 HAVARIJNÍ PLÁNY 24
3 AUDIT A TESTOVÁNÍ SYSTÉMU ICT **25**
3.1 PRINCIPY AUDITU 26
3.2 POSTUP AUDITU 27
3.2.1 Zahájení auditu 27
3.2.2 Přezkoumání dokumentace a příprava činností na místě 28
3.2.3 Provádění auditu na místě 28

3.2.4 Příprava, schválení a distribuce zprávy z auditu 28
3.3 PŘÍNOSY AUDITU ICT 28
II PRAKTICKÁ ČÁST 29
4 KLASIFIKACE INFORMACÍ 30
4.1 POSTUP KLASIFIKOVÁNÍ INFORMACÍ 30
4.1.1 Agenda 31
4.1.2 Citlivost informace 31
4.1.3 Kritičnost informace 31
4.1.4 Ochrana 32
4.1.5 Typické příčiny ztráty důvěrnosti, integrity nebo dostupnosti informace 33
5 ŘÍZENÍ PŘÍSTUPU K INFORMACÍM 34
5.1 UŽIVATELÉ ISOC 34
5.2 AUTORIZACE UŽIVATELŮ 34
5.3 PŘIDĚLENÍ PRÁVA UŽIVATELE 35
5.4 REVIZE PŘÍSTUPOVÝCH PRÁV 35
5.5 ZMĚNA A ODEBÍRÁNÍ PŘÍSTUPOVÝCH PRÁV 35
5.6 IDENTIFIKACE A AUTENTIZACE UŽIVATELE 35
5.7 BEZPEČNÉ PŘIHLÁŠENÍ 36
6 ZÁKLADNÍ PRAVIDLA BEZPEČNOSTI 37
6.1 PRAVIDLA FYZICKÉ OCHRANY 37
6.1.1 Bezpečnostní posouzení 37
6.1.2 Fyzická odolnost 38
6.1.3 Fyzická zranitelnost 38
6.1.4 Fyzická rizikovost 38
6.1.5 Protiopatření 38
6.2 PRAVIDLA ANTIVIROVÉ OCHRANY 39
6.2.1 Bezpečnostní role systému AVO 39
6.2.2 Zásady AVO 40
6.2.3 Chráněné a nechráněné počítače 41
6.2.4 Základní pravidla v boji proti virům 41
6.3 PRAVIDLA BEZPEČNÉ VÝMĚNY DAT 41
6.3.1 Požadavky na komunikační zařízení 42
6.3.2 Požadavky na komunikační cesty 42
6.3.3 Požadavky na komunikační služby 43
6.3.4 Požadavky na fyzický přenos dat 43
6.4 PRAVIDLA ŠIFROVÉ OCHRANY NOTEBOOKŮ 43
6.4.1 Princip šifrování 43
6.4.2 Šifrovací programy 43
6.4.3 Počítačová bezpečnost 44
6.4.4 Fyzická bezpečnost 44
6.5 PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ 44
6.5.1 Základní zásady 45
6.5.2 Prostředky zpracování osobních údajů 45
6.5.3 Ochrana osobních údajů zpracovávaných v ISOC 45

6.6 PRAVIDLA ŠKOLENÍ INFORMAČNÍ BEZPEČNOSTI 45
6.6.1 E-learning 46
6.7 PRAVIDLA ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ 47
6.7.1 Bezpečnostní slabiny 47
6.7.2 Bezpečnostní události 47
6.7.3 Bezpečnostní incidenty 48
6.7.4 Zdroje bezpečnostních incidentů 48
6.7.5 Obsah plánu 49
ZÁVĚR 50
CONCLUSION 51
SEZNAM POUŽITÉ LITERATURY 52
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 54
SEZNAM OBRÁZKŮ 55
SEZNAM TABULEK 56

ÚVOD

Bezpečnost informačních a komunikačních systémů se postupem času stává stále větším problémem, kdy je nutno řešit stále rostoucí počet uživatelů. Zatím co dříve se tento problém řešil pouze na úrovni odborníků nebo se neřešil vůbec, dnes je nutné, aby se tímto problémem dostatečně zabýval i koncový uživatel. Bezpečnost informačních a komunikačních systémů je svou částí více zaměřována na technickou ochranu než na jiné oblasti informační bezpečnosti. Spolu s technickým zabezpečením je dále nutno řešit otázku fyzické, administrativní a především podceňované personální bezpečnosti. Bez kompletního pojetí systému bezpečnostní politiky organizace jsou používané bezpečnostní mechanizmy jen náhodným experimentem, který může, ale nemusí fungovat podle našich požadavků.

U personální bezpečnosti nejde o nic jiného, než o vhodně prováděný výběr zaměstnanců a následné uplatnění pravidel, které co možná nejvíce sníží pravděpodobnost, že staneme tváří v tvář „vnitřnímu nepříteli“. Zní to jednoduše, ale praxe je v daném případě od teorie velmi odlišná. V reálném světě je situace taková, že je dnes mnoho organizací rádo, když vůbec dokáže některé pozice obsadit a případná selekce kandidátů na základě personální bezpečnosti by pro ně znamenala časové prodlevy a práci navíc. V tom případě je zapotřebí si připomenout staré dobré pravidlo, že každý systém je tak silný, jak je silný jeho nejslabší článek. Administrativní bezpečnost tvoří systém opatření jak s informacemi nakládat, aby nedošlo k jejich zneužití. Pro zajištění administrativní bezpečnosti a ochrany informací, je důležité stanovit a dodržovat jasná pravidla a zásady práce a nakládání s informacemi po celou dobu jejich životního cyklu. Každé prostředí vyžaduje určitou míru zabezpečení a zvolení úrovně zabezpečení informací přesně podle potřeb organizačního celku.

I. TEORETICKÁ ČÁST

1 POJMY BEZPEČNOSTI INFORMAČNÍHO A KOMUNIKAČNÍHO SYSTÉMU

1.1 Definice ICT

Jen malé procento českých autorů uvádí ve svých odborných textech definici ICT (Information and Communication Technologies), která by zahrnovala výčet využívaných technologií. Důvodem může být to, že je takových technologií mnoho, nebo jinými slovy, možnost označit jakoukoliv technologii za použitelnou. Informační a komunikační technologie, taktéž česky IKT (informační a komunikační technologie), zahrnuje veškeré technologie používané pro komunikaci a práci s informacemi. Informační a komunikační technologie je zastřešující pojem, který zahrnuje všechny technologie pro manipulaci a sdělování informací. Informační a komunikační technologie slouží k výpočtům, zobrazování informací, jejich dalšímu zpracování a k dalšímu přenosu mezi uživateli. ICT je jedním z nejrychleji se vyvíjejících odvětví společnosti a současně jedním z hnacích motorů ekonomik států po celém světě. V moderním světě představují informační a komunikační technologie důležitou a nepostradatelnou součást státní, podnikatelské i soukromé sféry. Z tohoto důvodu patří jejich ovládání mezi klíčové kompetence.

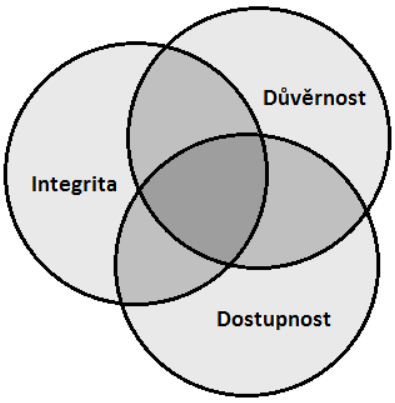
1.2 Informační bezpečnost

Informační bezpečnost je součástí bezpečnosti organizace. Cílem a úkolem řízení informační bezpečnosti je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů. Informační bezpečnost zahrnuje navíc proti bezpečnosti ICT i způsob zpracování uložení a správu archivu nedigitálních dat, zásady skartace materiálu, nakládání s informacemi během jejich transportu na jiná místa, zásady pro poskytování informací novinářům, zásady pro veřejná vystupování pracovníků organizace a podobně [10].

1.3 Bezpečnost ICT

Pojem bezpečnost ICT označuje proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb ICT na přiměřené úrovni. Bezpečnost ICT má za úkol chránit pouze ta aktiva, která jsou součástí IS (informačního systému) organizace podporovaného ICT. Proto je bezpečnost ICT relativně nejužší a komplikovanou oblastí řízení bezpečnosti, protože pracuje s „neviditelnými" daty, informacemi a službami. Zajištění systémové bezpečnosti má tři

oblasti – plánování, ochrana, reakce. Plánování mapuje přehled procesů i způsoby pokrytí výpadků ICT infrastruktury, které ovlivňují kontinuitu činnosti organizace. V současné době je zcela nemožné plánovat a vytvářet systém ICT struktury bez návaznosti na informační bezpečnost. Doby, kdy se kladl důraz na fungování a na bezpečnost se pohlíželo spíše jako na přívěsek, či se opomíjela, jsou dávno pryč.



Obr. 1. Vstah jednotlivých hledisek bezpečnosti [1].

1.4 Aktiva

Aktivum je cokoliv co má pro organizaci nějakou hodnotu, která může být působením hrozby snížena. Mezi informační aktiva můžeme zařadit HW (hardware), operační systém, komunikace, informace, know-how. Hodnota aktiva charakterizuje důležitost aktiva pro organizaci.

Aktiva rozdělujeme:

- hmotná aktiva – technické prostředky ICT (počítače, aktivní prvky počítačových sítí, tiskárny, kabelové rozvody a ostatní technická zařízení),
- nehmotná aktiva – pracovní postupy, data, programové vybavení, počítačové a komunikační služby a služby zajištění provozu.

1.5 Bezpečnostní incident

Bezpečnostní incident je událost, kterou lze označit za identifikovaný stav informačního systému, služby nebo počítačové sítě, jež může narušit pravidla bezpečnostní politiky nebo

selhání některého protiopatření nebo dříve neznámá nebo nepředpokládaná situace, která může ovlivnit bezpečnost [4].

Bezpečnostní incident je jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací. S bezpečnostní událostí přichází obvykle do prvního kontaktu běžný uživatel [14].

Průběh incidentu:

- detekce události,
- identifikace, rozhodnutí, příprava řešení,
- řešení bezpečnostního incidentu.

1.6 Integrita

Vlastnost, která potvrzuje a zaručuje neporušenost dat v průběhu jejich přenosu od zdroje k cíli [7].

1.7 Důvěrnost

Zajištění, že informace jsou přístupné nebo sděleny pouze tomu, kdo je k jejich přístupu oprávněn [14].

1.8 Dostupnost

Zajištění, že informace a důležité služby jsou dostupné uživateli, když je třeba a v potřebném rozsahu [14].

1.9 Identifikace

Proces, při němž daný subjekt proklamuje svou identitu. K tomuto účelu slouží uživatelské jméno. Příjemce identifikačních údajů provádí obvykle autentizaci.

1.10 Autentizace

Předem přesně definovaný proces, při kterém uživatel pomocí stanovených prostředků prokáže svoji identitu [6]. Autentizace uživatele se provádí zejména zadáním příslušného hesla, PINu (personal identification number), identifikační kartou nebo biometrickou identifikací.

1.11 Autorizace

Vlastnost umožňující uživateli informačního systému provést pouze aktivity, ke které má oprávnění. Současně pojem označuje proces ověření tohoto oprávnění i kladný výsledek ověření. Autorizace obvykle navazuje na proces autentizace [9].

1.12 Audit

Audit je systematický, nezávislý a dokumentovaný proces získání důkazů z auditu a jeho hodnocení s cílem stanovit rozsah splnění kritérií auditu.

1.13 Hrozba

Potencionální příčina nechtěného incidentu, jehož následkem může dojít k poškození systému nebo organizace. Hrozba je zneužitím zranitelnosti [4].

Hrozby rozdělujeme:

- přírodní a fyzické – živelné pohromy a poruchy (požáry, povodně, vichřice, poruchy v dodávce elektrické energie),
- technické a technologické – technické poruchy (datových nosičů, sítí, programů, počítačů nebo jiných komponent ICT), viry, trojské koně,
- lidské
    - neúmyslné – vyplývají z nedbalostního chování a neznalosti
    - úmyslné – cílené jednání s úmyslem poškodit nebo ohrozit zájem organizace (hackeři, mezifiremní špionáž, nebo také vlastní zaměstnanci či návštěvníci organizace).

Převážná většina hrozeb, které způsobí organizaci v ICT újmu, se zařazuje do kategorie neúmyslných hrozeb, které vznikají zevnitř organizace.

1.14 Útok

Využití zranitelného místa, může být úmyslný, neúmyslný nebo náhodný. Podle objemu způsobených škod pak katastrofický, významný, nevýznamný.

Typy útoků podle cíle:

- přerušení - proti dostupnosti, aktivní,

- odposlech - proti důvěrnosti, pasivní,
- záměna - proti integritě, aktivní,
- zfalšování - proti integritě, autenticitě, aktivní.

1.15 Útočník

Útočník je člověk, který útok provádí. Podle nebezpečnosti jejich útoků dělíme útočníky do následujících skupin:

- **Amatéři** – jedná se o skupinu lidí, kteří se většinou jen o útok pokouší. Využívají popis jednoduchého útoku dostupného na internetu, popřípadě již vytvořený program, který útok provede. Jejich nebezpečnost je malá, problémy způsobují jen výjimečně, většinou na nezabezpečených serverech.
- **Hackeři** – jedná se o vysoce kvalifikované útočníky, kteří mají dostatek znalostí, jsou však limitováni časem a prostředky. Jejich nebezpečnost je poměrně vysoká a většina systémů ICT se snaží chránit proti tomuto druhu útočníků.
- **Profesionálové** – vysoce kvalifikovaní a výborně vybavení útočníci. Jedná se o profesionální zločinecké organizace, jejich nebezpečnost je velmi vysoká a obrana proti jejich útokům je nákladná a pro většinu běžně používaných systémů nedostupná. Utočí zpravidla na systémy, které jsou pro ně obzvláště důležité.

1.16 Zranitelnost

Zranitelnost je slabé místo aktiva nebo opatření. Útočník může využít zranitelnost k vytvoření hrozby, kde slabá místa mohou vést k neautorizovanému přístupu ke zdrojům systému [4].

Zranitelnost rozdělujeme:

- **fyzickou** – budovy, počítačové místnosti,
- **personální** – vyplívají z přirozených chyb zaměstnanců,
- technických a programových prostředků – projevuje se chybou nebo poruchou,
- **nosičů dat** – selhání nosiče a následná ztráta dat,
- **elektromagnetických zařízení** – smazání obsahu nosiče dat při styku s intenzivním magnetickým polem,
- **komunikačních systémů a kabelových rozvodů** – přerušení nebo odposlech.

1.17 Riziko

Rizikem rozumíme pravděpodobnost poškození nebo zničení aktiva působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků (ztrát) vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit.
Pojem riziko se často ztotožňuje s pojmem hrozba. Je třeba brát v úvahu, že hrozba může být zdrojem pro jedno nebo více rizik a že hrozba sama o sobě riziko nepředstavuje. Hrozby pouze zneužívají zranitelnosti vedoucí k ohrožení, což je riziko, které lze snížit prostřednictvím opatření chránící aktiva před působením těchto hrozeb [1].

1.18 Opatření

Opatření znamená řízení rizika včetně politik postupů směrnic, praktik nebo organizačních struktur. Opatření se provádí na úrovni fyzické, logické nebo administrativní bezpečnosti, která snižuje zranitelnost a chrání aktivum před danou hrozbou. Stanovení přesných opatření je možné dosáhnout jen na základě analýzy rizik.
Jako příklady opatření lze uvést vhodné umístění budov a místností, uzamykání objektů, použití hesel při přístupu k systému při procesu autentizace, detailní testování systému, užití homologovaných a schválených zařízení [4].

1.18.1 Charakter opatření

- **administrativní** – tyto opatření zahrnují zejména směrnice a režimová opatření pro práci s ICT jako jsou pravidla pro používání elektronické pošty, používání vzdáleného přístupu, výměna, archivace a záloha dat,
- **fyzický** – mezi tato opatření patří používání mechanických zábranných prostředků, jako jsou zámky, trezory pro ukládání dat, pro informace s vyšším stupněm zabezpečení také poplachové zabezpečovací a tísňové systémy, kamerové systémy a systémy pro kontrolu vstupu,
- **technický a technologický** – např. autorizace a autentizace přístupu uživatelů k aktivům ICT, které se projevují např. ochranou přístupu do informačního přístupu prostřednictvím hesel.

1.18.2 Cíle opatření

- **prevenční** – minimalizuje rizika předem, jedná se např. o odhlášení uživatele při delší nečinnosti, automatické uzavírání dveří oken apod.,
- **detekční** – zajišťuje potencionální odhalování potencionálního ohrožení, zde můžeme zařadit např. pravidelné vyhodnocování přihlašovacích a auditních záznamů s možností identifikace bezpečnostních incidentů s případným vyhlášením poplachu,
- **korekční** – minimalizovat dopady poté co hrozba nastala a projevila se, např. odstranění virové infekce.

2 BEZPEČNOSTNÍ POLITIKA ICT

Bezpečnostní politika ICT stanovuje základní bezpečnostní požadavky a nařízení, s cílem zajistit ochranu a bezpečnost informací v organizaci, musí být v souladu s politikou celé organizace, kde stanovuje strategii, cíle, role zodpovědnosti a zásady související s informační bezpečností.

Bezpečnostní politika ICT vytváří základ pro tvorbu vnitřních norem - bezpečnostních zásad a postupů, bezpečnostních standardů a směrnic a definuje zásady chování všech účastníků – tj. uživatelů, vedoucích pracovníků, správců i třetích stran.

Cíle bezpečnostní politiky ICT:

- definovat hlavní cíle ochrany informací,
- stanovit způsob řešení bezpečnosti ICT,
- upravit pravomoci a zodpovědnosti v oblasti bezpečnosti ICT.

Bezpečnostní politika zpracovaná do obecných pravidel má trvalejší dobu platnosti a není třeba ji často aktualizovat. Výhodou je především snadnější příprava a svým obsahem je přístupnější vedení i zaměstnancům organizace. Hlavní nevýhodou obecné formulace politiky je to, že pod některými formulacemi si mnoho zaměstnanců nedokáže představit jejich konkrétní obsah. Může tak docházet ke špatné interpretaci obecných pravidel a zásad uvedených v bezpečnostní politice. Rozsáhlejší zpracování řeší bezpečnost ICT detailněji, může být však poměrně nepřehledné pro zaměstnance organizace, navíc pro jednotlivé zaměstnance jsou určeny pouze některé části této politiky. Velkou nevýhodou je nutnost časté aktualizace a následné schvalování managementem organizace. Proto je doporučeno zvláště u velkých organizací formulovat bezpečnostní politiku krátce a obecně, s následným rozpracováním do podřízené bezpečnostní dokumentace.

Bezpečnostní politika ICT na obecné úrovni by měla řešit zejména:

- fyzickou bezpečnost,
- personální bezpečnost,
- komunikační bezpečnost,
- administrativní bezpečnost, vstupní a výstupní kontroly, zprávy o incidentech,
- analýzu rizik, vyhodnocení hrozeb, plánování protiopatření,

- plánování postupu po incidentu.

2.1 Fyzická bezpečnost

V prostorách organizace, kde se nachází aktiva, je třeba chránit nejen před přírodními hrozbami, jako je například oheň nebo voda, ale i před fyzickými útočníky. Ochranu těchto hmotných aktiv má obecně na starost fyzická bezpečnost. Fyzická bezpečnost tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k aktivům organizace, popřípadě přístup nebo pokus o něj zaznamenat.

Prostředky ICT, zpracovávající kritické nebo citlivé informace organizace, by měly být umístěny v zabezpečených zónách chráněných definovaným bezpečnostním perimetrem s odpovídajícími bezpečnostními bariérami a vstupními kontrolami. Tyto prostředky by měly být fyzicky chráněny proti neautorizovanému přístupu, poškození a narušení. Jejich ochrana by měla odpovídat zjištěným rizikům. Ochrana zařízení (včetně těch, která se používají mimo hlavní lokalitu) je nezbytná jak pro snížení rizika neautorizovaného přístupu k datům, tak k zajištění ochrany proti ztrátě nebo poškození. Pozornost by měla být věnována také jejich umístění a likvidaci. Na ochranu proti možnému ohrožení nebo neautorizovanému přístupu a na ochranu podpůrných prostředků, jako například dodávky elektrické energie a struktury kabelových rozvodů, mohou být požadována zvláštní opatření.

2.2 Personální bezpečnost

Personální bezpečnost je často opomíjená a neřeší se na potřebné úrovni bezpečnosti. Přitom se uvádí, že 80% bezpečnostních incidentů mají na svědomí vlastní zaměstnanci organizace. Důležitou součástí systému ICT jsou uživatelé a správci sytému – zaměstnanci organizace na všech úrovních. K výběru těchto lidí je potřeba přistupovat s velkou precizností, vybírat kvalitní lidi, vytvořit jim podmínky pro jejich udržení v organizaci, provádět jejich školení, hodnocení a v případě nutnosti se věnovat jejich propouštění. S problematikou výběru kvalitních lidí se můžeme setkat převážně ve státní správě, kde na rozdíl od soukromých společností, ve kterých se snaží vybírat své zaměstnance podle jejich odborných a profesních schopností, výběrová řízení stání správy se ne vždy řídí tímto pravidlem. Po výběrových řízeních státní správy se často stává, že se do užívání nebo řízení systému ICT dostane osoba svou odborností a dovednostmi hluboce podprůměrná a

svou neznalostí potenciálně nebezpečná pro systém ICT. Z těchto důvodů je nutné, aby se stala personální bezpečnost oblastí bezpečnostní politiky, která je řešena na vysoké úrovni. Zárukou správného užívání informačního systému a přístupových účtů je seznámení uživatelů se systémem, s principy používání a přístupovými právy pro příslušnou funkci a činnost, což je otázkou úvodního zaškolení každého uživatele, a pravidelných školení podle potřeby a aktuálních změn [8]. Personální bezpečnost by měla být zvláštní kapitolou bezpečnostní politiky organizace, která by se měla promítnout do všech organizačních procesů, směrnic a nařízení.

2.3 Komunikační bezpečnost

Informace, které jsou přenášeny komunikačním kanálem, můžou být útočníkem odposlouchávány nebo můžou být zahlceny. Ochranu proti těmto hrozbám má na starost komunikační bezpečnost. Při přenosu informace komunikačním kanálem musí být zajištěna ochrana její důvěrnosti a integrity. Základním prostředkem pro zajištění informace při jejím přenosu komunikačním kanálem je kryptografická ochrana a její spolehlivá detekce záměrné i náhodné změny. V závislosti na komunikačním prostředí se zajišťuje spolehlivá identifikace a autentizace komunikujících stran, včetně ochrany identifikační a autentizační informace. Tato identifikace a autentizace předchází přenosu informace.

2.4 Administrativní bezpečnost

Administrativní bezpečnost má za úkol řízení bezpečnosti, ustanovení odpovědnosti a povinnosti jednotlivých skupin a osob v organizaci nejčastěji formou bezpečnostní politiky a bezpečnostních standardů. Administrativní bezpečnost tvoří systém opatření při:

- tvorbě,
- příjmu,
- evidenci,
- zpracování,
- odesílání,
- přepravě,
- přenášení,
- ukládání,

- skartačním řízení,
- archivaci,
- případně jiném nakládání.

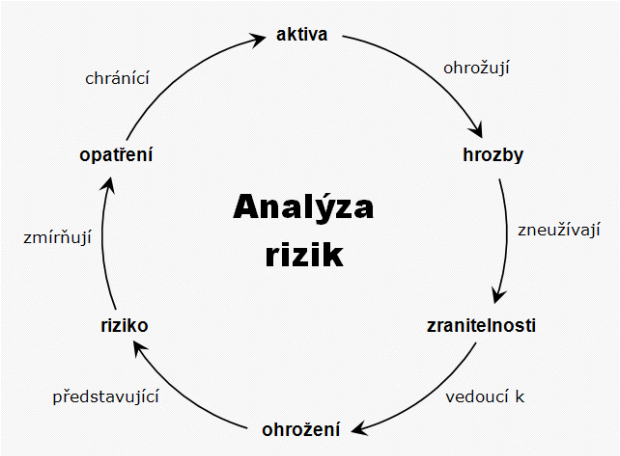
Při zajištění administrativní bezpečnosti a ochraně dokumentů s utajovanými, důvěrnými nebo citlivými informacemi je vhodné dodržovat jasná pravidla a zásady práce a nakládání s informacemi po celou dobu jejich životního cyklu [12].

2.5 Analýza rizik

Analýza rizik má v bezpečnostní politice velký význam, protože právě na jejím základě se stanovuje rozsah a úroveň bezpečnostní politiky organizace. Analýza rizik by měla přinést odpověď na otázku, působením jakých hrozeb je organizace vystavena, jak moc jsou její aktiva vůči těmto hrozbám zranitelná, jak vysoká je pravděpodobnost, že hrozba zneužije určitou zranitelnost a jaký dopad by to na společnost mohlo mít. Analýza rizik by se měla opakovat při každé významné změně systému jako je změna architektury, zjištění nové hrozby a zranitelnosti. Analýza rizik by měla být aktualizována dle velikosti organizace, složitosti systému ICT a rozsahu změn.

Analýza rizik se skládá

- identifikace aktiv
- identifikace hrozeb
- vlastní analýza rizik



Obr. 2. Analýza rizik [13].

2.5.1 Identifikace aktiv

Identifikací aktiv se zjišťuje, jaká aktiva se vyskytují v systému ICT a jakou mají pro organizaci hodnotu. Při procesu identifikace aktiv se vytváří seznam aktiv, která leží uvnitř hranice analýzy rizik [9]. Jedná se o následující aktiva:

- informace – dokumenty, databáze, sestavy dat,
- hardware – servery, pracovní stanice, tiskárny, směrovače, kabely,
- software – operační systémy, programy,
- budovy a místnosti, v nichž se aktiva nacházejí.

2.5.2 Identifikace hrozeb

V tomto kroku se identifikují hrozby, které mohou ohrožovat některé z aktiv. Při identifikaci aktiv se obvykle vychází ze seznamu hrozeb příslušných pro daný typ aktiva, uvedeného v použité metodě analýzy rizik, nebo ze zkušeností specialistů provádějících analýzu rizik. Jednotlivým aktivům jsou přiřazeny konkrétní hrozby. Nejčastěji uvažované hrozby jsou infiltrace neoprávněné osoby, nepovolené užití aplikace, porucha počítače nebo hardwarového zařízení, porucha síťových služeb, chyba uživatele IS, výpadek dodávky energie, porucha klimatizace, poškození vodou nebo požárem, krádež. U jednotlivých hrozeb se stanovuje úroveň hrozby. Také je nutné odhadnout pravděpodobnost uskutečnění hrozby. Současně se zkoumá úroveň zranitelnosti aktiva vůči hrozbě, tj. jde o nalezení slabých míst v systému ICT.

2.5.3 Vlastní analýza rizik

Po provedení identifikace aktiv a hrozeb vznikne seznam aktiv, která se v systému vyskytují včetně jejich finančního ohodnocení, a seznam hrozeb, které ICT systému v daném prostředí hrozí. Úkolem vlastní analýzy rizik je zjistit, jaká nebezpečí konkrétním aktivům hrozí. Postupně se prochází jednotlivá aktiva a určuje se vztah hrozeb ke konkrétním aktivům. Výsledkem vlastní analýzy rizik je seznam aktiv, kterým jsou přiřazeny jednotlivé hrozby. Ke konkrétní dvojici aktivum – hrozba lze přiřadit pravděpodobnost, s jakou ke konkrétní hrozbě danému aktivu dojde. Lze tedy kvalifikovaně rozhodnout, proti jaké pravděpodobnosti hrozeb bude ICT systém chráněn [3].

2.6 Návrh systému ochrany

Analýzou rizik byla zjištěna hodnota aktiv a pravděpodobnost hrozeb, proti kterým je potřeba systém chránit. Konkrétní hodnota této hranice závisí na finanční hodnotě chráněných aktiv. Ochrana by měla být navržena pro každou dvojici aktivum – hrozba. Vůči jedné hrozbě může být uplatněno jak několik ochranných opatření, tak i jedno ochranné opatření, které může být použito pro více hrozeb. Obecně v této oblasti platí pravidlo, že ochrana má smysl jen tehdy, pokud její náklady na zavedení nepřevýší cenu chráněných aktiv.

2.7 Havarijní plány

Analýza rizik by měla odhalit hrozící nebezpečí, na které je systém ochrany připraven. Může se stát nepředvídatelná situace, kdy dojde k selhání bezpečnostních opatření a podobně. Takový stav se označuje jako havárie nebo krizový stav systému. V takovém stavu systému je třeba jednat rychle a obezřetně, s cílem obnovit činnost důležitých částí systému a co nejrychleji obnovit poškozená data [3].

Odstranění aktuálního nebezpečí - jedná se především o odstranění následků katastrofy, která nastala (uhašení a likvidace požáru, odčerpání vody, odpojení systému od počítačové sítě a podobně).

Obnovení nejdůležitějších částí systému - v tomto kroku je třeba provést výměnu poškozených částí hardware, instalace nového aplikačního vybavení nebo konfiguraci systému.

Obnova dat - poškozená data je potřeba obnovit poslední nepoškozenou verzí těchto dat, případně oznámit uživatelům, o která data přišly. Při obnovování činnosti nesmí vzniknout znovu podmínky pro vznik havárie.

3 AUDIT A TESTOVÁNÍ SYSTÉMU ICT

Plošné nasazení systému ICT doprovázené nárůstem technologických možností, má jeden závažný důsledek – rostoucí závislost organizace na kvalitním, spolehlivém a bezpečném fungování ICT včetně všech souvisejících procesů a činností. Prosazení vyšší účinnosti a účelnosti, potřebné míry spolehlivosti a bezpečnosti u všech informačních systémů se tak stává jednou ze základních oblastí odpovědnosti vedení organizace a odpovědných pracovníků informatiky [4]. Široké spektrum oblastí, které je potřebné při auditu ICT posoudit, odpovídá i širokému spektru legislativy, normativů a dalších standardů vůči kterým je možné nebo potřebné audit ICT provádět.

Audity v oblasti ICT jsou nejčastěji prováděny vůči ustanovením norem a standardů definujících:

- systém řízení bezpečnosti informací (ISO/IEC 27000),
- systém řízení IT služeb (ISO/IEC 20000),
- zásady pro ochranu utajovaných informací (zákon č. 412/2005 Sb.),
- zásady pro ochranu osobních údajů (zákon č. 101/2000 Sb.),
- zásady pro IT Governance (CobiT),
- zásady pro konkrétní systémy a technologie (OWASP, OSSTM, doporučení NIST, SANS a další).

V oblasti ICT se provádí nejčastěji následující druhy auditů, přičemž velmi často se jedná o kombinaci těchto druhů auditů na základě požadavku.

- **Audit systému řízení bezpečnosti informací (ISMS)** zaměřený na posouzení stavu bezpečnosti informací vůči ustanovením a požadavkům norem řady ISO/IEC 27000.
- **Audit systému řízení IT služeb (ITSM)** v rámci kterého je hodnocena úroveň naplnění ustanovení norem zaměřených na řízení IT služeb, případně IT Governance (ISO/IEC 20000, ITIL, CobiT).
- **Audit ochrany osobních údajů** zaměřený na posouzení splnění požadavků zákona č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších doplňků.

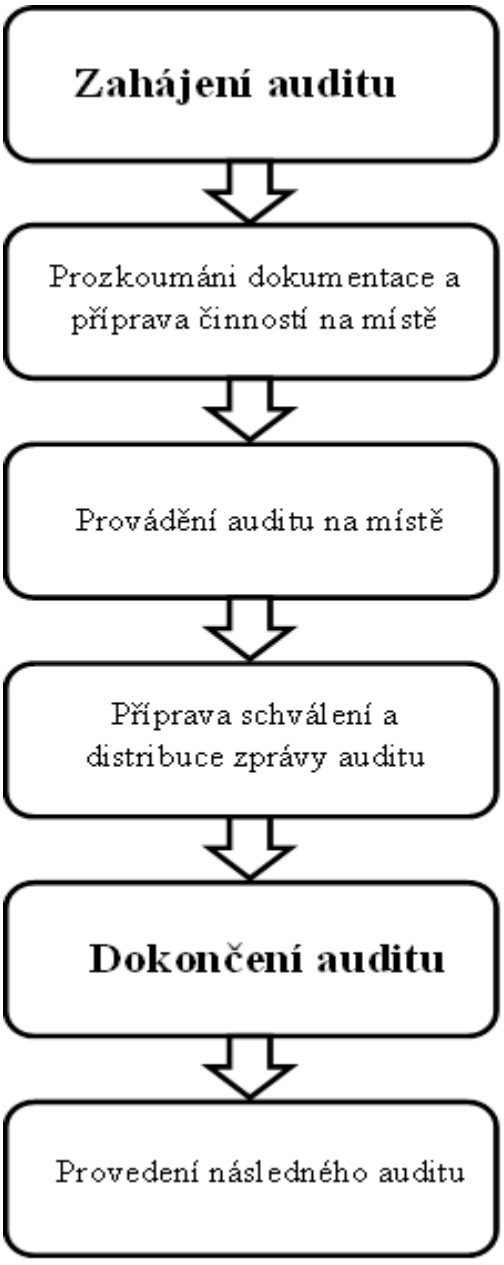
- **Audity v bankovním prostředí** posuzující úroveň naplnění znění různých regulačních opatření zaměřených na ICT (vyhláška ČNB č. 123/2007 Sb.) a dalších standardů (IT Control Objectives for Basel II, atd.).
- **Technické audity posuzující** stav v oblasti ICT, zejména konkrétních IS nebo technologií, vůči specifickým technickým standardům a doporučením (OWASP, OSSTM, doporučení NIST, SANS a další).

3.1 Principy auditu

Provádění auditů a vlastní činnost auditorů je spojena s respektováním a dodržováním řady zásad a pravidel. Právě tyto zásady řadí audit jako efektivní a spolehlivý nástroj pro podporu účinného řízení, které poskytuje nenahraditelné informace, nutné pro trvalé zlepšování systému řízení. Dodržování následujících zásad je předpokladem pro zajištění odpovídajících, dostatečných a opakovatelných závěrů [4]:

- **Etické chování** – důvěryhodnost, jednotnost, důvěrnost a diskrétnost vztahu auditora a auditované činnosti při manipulaci s informacemi a daty.
- **Spravedlivá prezentace** – zjištění, závěry a zprávy z auditu musí být vždy pravdivé a musí přesně popisovat veškeré činnosti, provedené v jeho průběhu.
- **Povinnost profesionálního přístupu** – povinnost auditora mít vysokou odbornou a profesní způsobilost a musí využívat své odborné zkušenosti, dané nejlepší vžitou praxí v oblasti ICT.
- **Průkaznost** – veškeré závěry a informace z provedeného auditu musí být ověřitelné.
- **Nezávislost** – auditor musí být naprosto nezávislý na auditované činnosti a prováděný audit je důsledně veden s cílem najít objektivní stanovisko.

3.2 Postup auditu



Obr. 3. Průběh auditu bezpečnosti [4].

3.2.1 Zahájení auditu

Zahájení auditu se věnuje zejména jmenování vedoucího auditorského týmu, definici cílů, rozsahu předmětu a kritériím auditu, hodnocením proveditelnosti auditu, vytvoření auditního týmu a navázání prvního kontaktu s auditorskou stranou.

3.2.2 Přezkoumání dokumentace a příprava činností na místě

Audity by se měly opírat o základní znalost prostředí. Tato fáze slouží ke studii existující dokumentace, která je základem pro návrh plánu auditu, včetně hrubého rozvržení úkolů. Součástí této fáze je příprava různých pracovních dokumentů auditního týmu.

3.2.3 Provádění auditu na místě

Provádění auditu na místě je hlavní částí celého auditu, kdy dochází ke sběru informací o skutečném fungování systému, k ověřování zjištěných skutečností a ke shromažďování důkazů. Hlavní činnosti v této části jsou zejména:

- úvodní setkání s auditovanou stranou,
- komunikace s auditovanou stranou,
- určení rolí a odpovědností průvodců a pozorovatelů,
- shromažďování a ověřování dokumentace,
- formulace nálezů,
- příprava závěrů auditu,
- organizace uzavřeného jednání o závěrech auditu.

3.2.4 Příprava, schválení a distribuce zprávy z auditu

Aby byly zprávy z auditu důkladně zpracovány, je důležité důkladné vyhodnocení všech zjištěných skutečností včetně zvážení možných negativních dopadů závěru auditu na organizaci a dalších vzájemných souvislostí. Tento úkon tvoří základ pro stručnou formulaci zprávy z auditu, která je vlastnictvím auditované strany, a proto musí být zachována předem určená pravidla jejího utajení. Konečná zpráva z auditu by měla obsahovat pravdivý, úplný, stručný a srozumitelný záznam o auditu [5].

3.3 Přínosy auditu ICT

Audit ICT přináší vedení organizace a ICT personálu následující přínosy:

- Ověření souladu a efektivity přijatých opatření s požadavky závazné dokumentace.
- Nezávislý a opakovatelný pohled na stav ICT.
- Posouzení efektivity opatření vůči zdrojům vynaloženým na jejich implementaci.
- Možnost účinně optimalizovat řídící a plánovací procesy v ICT.
- Účinně se připravit na případný certifikační proces dle zvoleného standardu.

II. PRAKTICKÁ ČÁST

4 KLASIFIKACE INFORMACÍ

Klasifikované informace jsou informace označené tak, aby lidem, kteří s nimi přicházejí do styku, bylo zřejmé, že tyto informace jsou citlivé a že je nutné je vhodným způsobem chránit. Klasifikace informací má význam jak uvnitř dané organizace, tak pro "třetí strany", které přicházejí s danou organizací do styku. Jestliže není provedena klasifikace informací a zpracovávané nebo vyměňované informace nejsou příslušným způsobem označeny, pak s nimi není ani zacházeno s příslušným stupněm ochrany. Vedoucí pracovníci, kteří si dostatečně neuvědomují význam klasifikace informací a nezajistí její zavedení, jsou potom často překvapeni zjištěným únikem vysoce citlivých informací. Většina organizací pracuje se spoustou informací, které je třeba klasifikovat dle vhodného klasifikačního schématu a vytvoření katalogu klasifikovaných informací je proto pro úspěšné zavedení klasifikace informací ve společnosti naprosto zásadní. Primární je klasifikace z hlediska důvěrnosti, protože vlastní obsah informace je jejím nejdůležitějším atributem. Klasifikace z hlediska dostupnosti a integrity má spíše technický význam. Z důvodu realizovatelnosti a životaschopnosti klasifikačního modelu není vhodné definovat vyšší počet tříd z hlediska důvěrnosti, integrity a dostupnosti. Jednotlivé klasifikační stupně musí být pro všechny zaměstnance srozumitelné, aby jim nečinilo problém dané informaci přidělit odpovídající klasifikační stupeň a podle toho s ní zacházet.

4.1 Postup klasifikování informací

- Klasifikování pro potřebu vytváření a údržby katalogu provádějí nebo zajišťují příslušní pracovníci řízení managementu OC (organizačního celku).
- Klasifikování při užívání katalogu, tj. při zpracování informace v ISOC (informačním systému organizačního celku) provádějí zaměstnanci OC v případě, že zpracovávaná informace není v katalogu začleněna.
- Dojde-li k případu, že zpracovávaná informace není v katalogu začleněna, je zaměstnanec OC povinen tuto skutečnost cestou příslušného pracovníka řídícího managementu oznámit a související údaje předat správci katalogu.

Tab. 1. Vzor tabulky s klasifikačními údaji.

Agenda kód dle organizačního řádu	Informace	Aplikace kód dle seznamu	Citlivost kategorie	Kritičnost stupeň	Ochrana stupeň
112 02	Dokumenty, zprávy, záznamy	52	K3	3	3

4.1.1 Agenda

Agendou se rozumí základní skupina obsahově a věcně úzce souvisejících činností vykonávaných v rámci dané oblasti procesů, přitom procesem je organizovaný opakovaný sled na sebe navazujících aktivit, který transformuje vstupy na výstupy.

- Klasifikování se provádí v rámci agend organizačních útvarů, případně jiných forem organizačního uspořádání OC.
- Agendy v katalogu stanovuje správce katalogu.

4.1.2 Citlivost informace

Citlivost je vlastnost informace vyjadřující potřebu ochrany, protože její zpřístupnění, modifikace, zničení nebo ztráta by způsobilo někomu nebo něčemu znatelnou hmotnou anebo nehmotnou škodu.

- K informaci začleněné v katalogu se přiřadí jedna z kategorií citlivosti informace.
- Přiřazení je prováděno při vytváření katalogu, při užívání katalogu a při pravidelné údržbě katalogu.
- Kategorie citlivosti informací OC lze rozdělit následovně:

Tab. 2. Příklad rozdělení citlivých informací.

Kategorie citlivosti	Charakteristika kategorie citlivosti
K1	informace přístupná veřejnosti
K2	informace nepřístupná veřejnosti, ale přístupná všem zaměstnancům OC
K3	informace přístupná pouze vymezenému okruhu zaměstnanců OC nebo jiných adresátů
K4	informace obsahující osobní údaje zaměstnanců OC nebo jiných osob

4.1.3 Kritičnost informace

Kritičnost informace je vyjádření stupně závislosti informace na ztrátě důvěrnosti, integrity nebo dostupnosti a na dopadu takové ztráty na OC.

- K informaci začleněné v katalogu se přiřadí stupeň kritičnosti informace.
- Přiřazení je prováděno při vytváření katalogu, při užívání katalogu a při pravidelné údržbě katalogu.
- Při stanovení stupně kritičnosti informace je vhodné brát do úvahy možný dopad ztráty důvěrnosti, integrity nebo dostupnosti informace na OC, kdy dopadem může být:
    - poškození dobrého jména,
    - narušení řízení nebo provozu,
    - porušení právních předpisů nebo závazků,
    - ohrožení ekonomických zájmů,
    - přímé finanční ztráty.

Tab. 3. Příklad rozdělení kritičnosti informací.

Stupeň kritičnosti	Charakteristika stupně kritičnosti: z hlediska rizika ztráty důvěrnosti, integrity nebo dostupnosti informace
1	žádný nebo velmi nízký
2	nízký
3	střední
4	vysoký
5	velmi vysoký

4.1.4 Ochrana

- K informaci začleněné v katalogu se přiřadí jeden stupeň ochrany informace.
- Přiřazení je prováděno při vytváření katalogu, při užívání katalogu a při pravidelné údržbě katalogu.
- Stupně ochrany informací se rozdělí následovně:

Tab. 4. Příklad rozdělení stupně ochrany.

Stupeň ochrany	Charakteristika stupně ochrany
1	základní
2	zvýšený
3	vyšší
4	dodatečný
5	zvláštní

Pro ochranu informace platí, že BO (bezpečnostní opatření) konkrétního stupně ochrany musí být uplatněna pro všechny vyšší stupně ochrany, jak uvedeno následně:

Tab. 5. Stanovení ochrany informací.

Síla BO a stupeň ochrany	Typ BO a popis ochrany	Stupeň kritičnosti informace				
		1	2	3	4	5
1	základní	x	x	x	x	x
2	zvýšený	-	x	x	x	x
3	vyšší	-	-	x	x	x
4	dodatečný	-	-	-	x	x
5	zvláštní	-	-	-	-	x

4.1.5 Typické příčiny ztráty důvěrnosti, integrity nebo dostupnosti informace

Velmi důležitou fází je vyhodnocení příčin vzniku ztráty důvěrnosti, integrity nebo dostupnosti informace a vyvození příslušného ponaučení, které je obvykle představováno preventivními opatřeními, jež mají zabránit opakování tohoto bezpečnostního incidentu.

Tab. 6. Typické příčiny ztráty důvěrnosti, integrity nebo dostupnosti informace.

Typická příčina	Ztráta		
	důvěr.	integr.	dostup.
Chybná nebo nedovolená činnost personálu	x	x	x
Chybná nebo nedovolená činnost uživatele	x	x	
Krádež informace zaměstnancem nebo cizí osobou	x		x
Neautorizovaný přístup k inf. zaměstnancem nebo cizí osobou	x	x	
Neúmyslné poškození inf. zaměstnancem nebo cizí osobou		x	
Neúmyslné zničení inf. zaměstnancem nebo cizí osobou			x
Přetížení provozu			x
Škodlivý SW (software)		x	x
Teroristická hrozba nebo útok			x
Úmyslné poškození inf. zaměstnancem nebo cizí osobou		x	
Úmyslné zničení inf. zaměstnancem nebo cizí osobou			x
Chyba SW vybavení		x	x
Porucha HW vybavení			x
Chyba nebo porucha komunikačního vybavení	x	x	
Chyba služby ISOC			x
Porucha napájení			x
Porucha klimatizace			x
Požár objektu OC nebo technologického vybavení			x
Průnik vody do objektu nebo k technologickému vybavení ISOC			x
Přírodní pohroma			x

5 ŘÍZENÍ PŘÍSTUPU K INFORMACÍM

V systému ochrany ISOC je zapotřebí stanovit pravidla pro přidělování přístupu uživatelů a skupin uživatelů k informacím v rámci IS. Stanovení politiky řízení přístupu by se mělo prolínat do všech IS a aplikací. Důležitým prvkem je zajištění abstrakce definovaných pravidel a vázaní přístupových práv především na pracovní pozice (role). Pro celkovou přehlednost je proto žádoucí, zavést jednotlivé přístupové profily uživatelů na základě jejich pracovní pozice.

Pravidla řízení přístupu mají za úkol stanovit OC, prostředky a postupy řízení přístupu k informačním aktivům ISOC tak, aby byla zajištěna jejich dostupnost, integrita a důvěrnost. Pravidla řízení přístupu v ISOC se vztahují i na fyzický přístup k informačním aktivům ISOC. Přístup externích subjektů k informačním aktivům ISOC se musí řídit smluvními bezpečnostními podmínkami. Přístup zaměstnanců k externím informačním zdrojům je nutno řídit příslušnými resortními smlouvami a dohodami o spolupráci se správci externích informačních zdrojů. Za systém řízení přístupu musí odpovídat příslušná osoba, jedná se většinou o vedoucího pracovníka odboru, sekce nebo oddělení, kterému přísluší organizace a řízení systému ICT. Ten poté zejména:

- stanovuje prostředky a postupy řízení přístupu v ISOC,
- schvaluje organizaci řízení přístupu v ISOC,
- pověřuje podřízené pracovníky výkonem specifických bezpečnostních rolí řízení přístupu v ISOC.

5.1 Uživatelé ISOC

Uživatelem ISOC se zaměstnanec OC stává na základě autorizace profilu uživatele. Individuálním uživatelem ISOC je osoba, které je prokazatelně přidělen počítač do užívání, přičemž tato osoba je jeho výhradním uživatelem. Skupinovým uživatelem ISOC je osoba, která je prokazatelně oprávněna užívat počítač v rámci vymezené skupiny uživatelů.

5.2 Autorizace uživatelů

Personální útvar přidělí každému zaměstnanci OC při jeho nástupu k OC osobní číslo a místně příslušný útvar informatiky založí uživatelský účet a přidělí uživatelské jméno. Přímý nadřízený pracovník autorizuje uživatele ISOC k užívání konkrétních služeb a technických prostředků.

Autorizace uživatele ISOC se provádí tak, že příslušný pracovník schválí profil uživatele ISOC a pokyn k přidělení aplikační role, který musí odpovídat funkční roli uživatele nebo pracovnímu zařazení uživatele a jeho činnosti.

5.3 Přidělení práva uživatele

Uživateli musí být svým nadřízeným pracovníkem stanoven profil uživatel ISOC a vymezeno právo k přístupu k aplikacím organizace.

5.4 Revize přístupových práv

Přístupová práva uživatelů i externích uživatelů ISOC místně příslušní správci přístupových práv a správci zvláštních přístupových práv pravidelně, nejméně jednou ročně revidují.

5.5 Změna a odebírání přístupových práv

Při změně pracovního zařazení uživatele ISOC, jeho činnosti nebo pracoviště jsou takovému uživateli i externímu uživateli ISOC neprodleně odebrána poskytnutá přístupová práva a poté poskytnuta přístupová práva nová. Při ukončení pracovního vztahu, smluvního vztahu nebo jiné dohody jsou uživateli i externímu uživateli ISOC neprodleně odebrána přístupová práva a zneplatněn jeho uživatelský účet.

5.6 Identifikace a autentizace uživatele

Každý uživatel ISOC musí mít příslušným útvarem organizace založen uživatelský účet a přiděleno jednoznačné a neopakovatelné uživatelské jméno. Pro jednoznačnou identifikaci účtů zaměstnanců je vhodné zvolit jejich osobní číslo v organizaci. U organizace s vyšším počtem zaměstnanců, by byla identifikace uživatelského jména např. podle příjmení zaměstnance nepřehledná a mohlo by dojít k nechtěné změně uživatele. Někdy je potřeba rozlišit, zda se jedná o uživatelský nebo administrátorský účet. V tomto případě je doporučeno před nebo za osobní identifikátor přidat znak, který nám tento účet rozliší např. Uxxxx určuje, že se jedná o uživatelský účet, kde xxxx představuje osobní číslo zaměstnance. Naopak u účtu Axxxx, je zřejmé že se jedná o účet administrátora.

5.7 Bezpečné přihlášení

V rámci přihlašovací procedury se uživatel ISOC identifikuje a svoji identitu autentizuje prostřednictvím uživatelského jména a hesla. Pro bezpečnou autentizaci musí mít uživatel bezpečné heslo, které je nutno optimálně zvolit. Příliš přehnané nároky na bezpečnost hesla vedou k tomu, že si je uživatelé zaznamenávají v okolí své pracovní stanice a jeho odhalení není pro útočníka problém. Také volba slabého, nebo snadno rozluštitelného hesla může mít fatální následky. Heslový systém ISOC by měl být vůči uživateli nastaven tak, že heslo musí mít délku minimálně 8 znaků, nesmí obsahovat 2 a více po sobě jdoucích stejných znaků, nesmí obsahovat pouze číselné nebo pouze písmenné skupiny, stanovit dobu platnosti hesel na 30 až 90 dnů, v závislosti na používaném prostředí [2]. Tím bude omezena doba, během níž lze odhalit uživatelské heslo a získat přístup k prostředkům sítě.
Zkušenosti z praktického nasazení ukazují, že optimální volbou pro bezpečnost systémů i pohodlí uživatelů je kombinované využití čipové karty pro více podnikových systémů a aplikací. Čipová karta může být běžně osazena jedním nebo dvěma čipy s kontaktním i bezkontaktním rozhraním. Tato kombinace umožňuje použít jednu kartu pro fyzický i logický přístup, elektronický podpis i šifrování. Karta se tak stává „generálním klíčem“, který otevírá přístup k prostředkům a informacím organizace. Hlavní bezpečnostní potenciál čipové technologie spočívá ve využití nesymetrické kryptografie, privátních klíčů uložených na čipu a certifikátů veřejných klíčů. Vzhledem ke komplexnosti implementace infrastruktury s veřejnými klíči je žádoucí využívat systém pro správu certifikátů, nejlépe v kombinaci se systémy pro správu klíčů a karet.

6 ZÁKLADNÍ PRAVIDLA BEZPEČNOSTI

Účelem této části je stanovit základní provádění ochrany informačního systému OC, vytvořit základní pravidla a povinnosti při řízení, správě a užívání, vymezit odpovědnost a snažit se uživatele s vydanými akty řízení seznamovat, následně je dodržovat a uplatňovat v praxi.

6.1 Pravidla fyzické ochrany

Cílem fyzického zabezpečení je zamezení neoprávněného přístupu, zneužití informací neoprávněnou osobou a narušení aktivit OC. Citlivé informace je zapotřebí uchovávat v zabezpečených oblastech na základě definování bezpečnostních zón s přiměřenými bezpečnostními bariérami a vstupními kontrolami. Technická zařízení IS musí být umístněná tak, aby byla dostatečně chráněná před nepovolanými osobami. Součástí fyzické ochrany je zajištění provozuschopnosti a správné funkčnosti fyzických aktiv ISOC. Systém FO (fyzické ochrany) ISOC musí obsahovat:

- popis fyzického prostředí,
- specifikaci zařízení ISOC, včetně jeho umístění,
- hodnotu fyzické rizikovosti zjištěnou v rámci bezpečnostního posouzení FO ISOC,
- negativní poznatky z bezpečnostního posouzení FO ISOC,
- stav protiopatření a návrh přijatelných nápravných anebo preventivních opatření,
- přílohu - Zprávu z bezpečnostního posouzení FO ISOC.

6.1.1 Bezpečnostní posouzení

Cílem bezpečnostního posouzení FO je dosažení co nejvyšší fyzické odolnosti a eliminace nebo alespoň minimalizace fyzické zranitelnosti a rizikovosti. Účelem bezpečnostního posouzení FO ISOC z hlediska fyzického prostředí a zařízení je:

- odhad a hodnocení odolnosti fyzického prostředí a zařízení ISOC (fyzická odolnost),
- odhad a hodnocení zranitelnosti fyzického prostředí a zařízení ISOC (fyzická zranitelnost),
- odhad a hodnocení rizikovosti fyzického prostředí a zařízení ISOC (fyzická rizikovost).

6.1.2 Fyzická odolnost

Odhad a hodnocení fyzické odolnosti zahrnuje údaje související s dislokací, hranicí a zónováním prostorů objektů OC, přičemž:

- údaje související s dislokací zahrnují umístění, stavební provedení, vlastnictví, provozování, správu a užívání objektů; dále přítomnost zaměstnanců, přístup a příjezd k objektům a parkování,
- údaje související s hranicí zahrnují vstupy, prostupy a vjezdy do objektů a parkování,
- údaje související se zónováním zahrnují zóny určené pro veřejnost, pro veřejnost i zaměstnance, pouze pro zaměstnance a chráněné prostory (zóny) objektů OC.

Pokud tyto údaje nejsou v plném rozsahu zahrnuty v hodnocení fyzické zranitelnosti, musí se zvlášť ohodnotit. Hodnotám fyzické odolnosti jsou přiřazeny koeficienty, pomocí kterých se upraví hodnota fyzické zranitelnosti.

6.1.3 Fyzická zranitelnost

Odhad a hodnocení fyzické zranitelnosti vychází z pravděpodobnosti uplatnění hrozeb vůči fyzickému prostředí a zařízení ISOC v rámci konkrétního objektu. Zdrojem hrozeb může být náhodná či úmyslná činnost lidí, chyby, poruchy či havárie stavebně technologického vybavení či vnější vlivy. Při odhadu a hodnocení fyzické zranitelnosti se nejprve provádí identifikace a hodnocení fyzických hrozeb.

6.1.4 Fyzická rizikovost

Odhad a hodnocení fyzické rizikovosti vychází z identifikace a hodnocení fyzických hrozeb a z odhadu a hodnocení fyzické zranitelnosti ISOC. Vyhodnocení (metrika) fyzické rizikovosti využívá čtyřúrovňovou stupnici: nízká (1), nízká až střední (2), střední až vysoká (3), vysoká (4) míra rizika. Rizikovost, jejíž míra je střední až vysoká nebo vysoká rizikovost je reálnou fyzickou rizikovostí ISOC.

6.1.5 Protiopatření

Účelem protiopatření fyzické ochrany ISOC je eliminace nebo alespoň minimalizace fyzické rizikovosti. Tato protiopatření mají charakter organizačně personální,

administrativně procedurální a technický. Protiopatření jsou členěna do úrovní fyzické ochrany ISOC. Musí být uplatněna tak, jak je uvedeno v následující tabulce.

Tab. 7. Stanovení protiopatření.

Úroveň FO	Stupně rizika			
	nízké	nízké až střední	střední až vysoké	vysoké
1 - základní	x	x	x	x
2 - zvýšená	-	x	x	x
3 - dodatečná	-	-	x	x
4 - zvláštní	-	-	-	x

6.2 Pravidla antivirové ochrany

Další důležitou součástí zabezpečení dat, je AVO (antivirová ochrana). Neaktuální, nebo žádný antivirový program může mít pro systém fatální následky. Data nemají dostatečnou nebo dokonce žádnou ochranu, proto o ně může uživatel kvůli mnohdy sofistikovaným virům velice snadno přijít. Každý nedostatečně zabezpečený počítač představuje riziko nejen pro svého uživatele, ale i pro ostatní. Může být infikován počítačovými viry a červy, nebo se stát hlavním cílem pro hackery, kteří pak mohou zneužít počítač k útokům na jiné systémy v síti. Z tohoto důvodu je zabezpečení počítačů systémem AVO povinné. Nejčastějšími zdroji nákazy jsou e-maily, instalace volně šiřitelných programů nebo pouhé užívání Internetu. Je přitom nutno říci, že stoprocentní jistota není vzhledem na lidský faktor ani při firemních zdrojích. Vysoce rizikovým zdrojem jsou i hackerské stránky nabízející heknuté verze komerčních resp. shareware programů, generátory klíčů a podobně. Tyto soubory jsou často zavirované, ať už z nepozornosti jejich tvůrců nebo i úmyslně. Typickou psychologickou fintou používanou tvůrci virů s cílem jejich rychlého rozšíření je šíření zavirovaných souborů resp. trójských koní pod jménem některého z populárních freeware/shareware programů v ještě neexistující verzi, kterou uživatelé v naději na nové vylepšení rádi vyzkoušejí. Jinou variantou je vybavení souboru fiktivní dokumentací slibující hesla serverů, zajímavý spořič obrazovky apod.

6.2.1 Bezpečnostní role systému AVO

V systému AVO, je důležité stanovit role odpovědnosti za správu a užívání. Z toho důvodu se zřizují bezpečnostní role, které mají za úkol stanovit a řídit pravidla AVO OC.

Role správce AVO

Správce systému AVO OC je za svou činnost odpovědný a odpovídá za:

- zpracování, revizi a aktualizaci pravidel AVO ISOC,
- zpracování, revizi, aktualizaci a dohled plnění realizačního plánu pravidel AVO ISOC,
- metodické řízení doménových administrátorů systému AVO ISOC,
- centrální administraci AVO ISOC.

Role doménový administrátor

Doménový administrátor je svou odborností odpovědná za:

- dodržování pravidel AVO ISOC,
- plnění realizačního plánu pravidel AVO ISOC,
- metodické řízení pracovníků nebo příslušníků útvaru informatiky OC v oblasti AVO,
- administraci AVO ISOC v bezpečnostní doméně ISOC.

Role lokální administrátor

Lokální administrátor je za svou odbornou činnost odpovědný svému doménovému administrátorovi systému AVO ISOC. Odpovídá zejména za:

- dodržování pravidel AVO,
- lokální administraci AVO,
- řešení virové nákazy a jejích důsledků v oblasti své působnosti.

6.2.2 Zásady AVO

Antivirový program použitý v ISOC nesmí neúměrně omezovat běh aplikačních programů na serverech ani na pracovních stanicích uživatelů ISOC či jinak neúměrně negativně ovlivňovat jejich činnost. V takovém případě se připouští lokální úprava jednotné politiky použitého antivirového programu.

6.2.3 Chráněné a nechráněné počítače

V ISOC musí být antivirovým programem chráněny všechny počítače, které obsahují elektrická, elektromagnetická, optická či radiová (bezdrátová) datová rozhraní, a které to z hlediska své funkce umožňují. Počítače ISOC, které není možné nebo účelné vybavit antivirovým programem schvaluje správce AVO a to na návrh útvaru informatiky OC, v jehož působnosti je takový počítač instalován.

6.2.4 Základní pravidla v boji proti virům

Samotné pořízení antivirového programu a jeho instalace na chráněný počítač však nestačí. Může se jednat o sebelepší program, a přesto se může stát, že nebude schopen počítač uchránit, pokud nebudou respektována některá základní pravidla AVO.

1. Nasazení kvalitního antivirového systému.
2. Antivirový systém musí být neustále aktualizovaný (program i virové databáze).
3. V antivirovém systému musí být zapnuta rezidentní ochrana.
4. Neznámá přenosná média musí být před vložením do počítače otestována antivirovým programem. K tomuto účelu je vhodné používat „karanténní počítač“ pro kontrolu médií, který je umístěn mimo LAN (Local Area Network) OC.
5. Zamezit přístup nedůvěryhodným osobám ke svému počítači.
6. Soubory stažené z internetu zkontrolovat antivirovým programem.
7. Nevyžádanou nebo podezřelou e-mailovou poštu neotvírat a ihned smazat.
8. Provádět pravidelnou zálohu dat.
9. Věnovat velkou pozornost „neobvyklému“ chování počítače, jako je delší zavádění systému, podezřelé padání programů.
10. Při sebemenším podezření na přítomnost viru kontaktovat příslušného lokálního administrátora AVO OC.

6.3 Pravidla bezpečné výměny dat

Data a informace představují pro každou organizaci velmi důležitý majetek a neoprávněný přístup k nim nebo dokonce jejich ztráta může mít značně negativní dopady. Jejich únik pak může mít za následek citelné finanční ztráty nebo dokonce i konflikt se zákonem. Cílem konceptu bezpečné komunikace je zajistit pomocí dnes dostupných technologií efektivní a bezpečnou výměnu dat mezi organizacemi a jejími partnery a případnou kontrolu.

Komunikační prostředky ISOC musí být odolné proti vlastním chybám tak, aby nebyly možným zdrojem ztráty dostupnosti, integrity a důvěrnosti přenášených dat anebo možným zdrojem nedostupnosti komunikačních služeb ISOC.

6.3.1 Požadavky na komunikační zařízení

Komunikační zařízení ISOC musí:

- mít porty určené pro vzdálenou správu, dohled a monitoring být chráněny před neautorizovaným přístupem a nevyužívané porty musí být deaktivovány,
- být jednoznačně určeno identifikačním číslem nebo jiným údajem pro potřebu vzájemné autentizace,
- obsahovat mechanismus pro záznam oprávněných lokálních a vzdálených přístupů i pokusů o neoprávněný přístup,
- být umístěno v prostorách, do kterých má fyzický přístup pouze vymezený počet oprávněných osob a kde jsou zajištěny výrobcem nebo dodavatelem předepsané parametry fyzického prostředí.

6.3.2 Požadavky na komunikační cesty

Komunikační cesty ISOC musí:

- být zdvojeny a musí být zajištěno automatické přesměrování přenášených dat z přenosové cesty nefunkční na cestu funkční v případě, že její odolnost je nižší, než je požadováno nebo je-li riziko vlastní chyby vyšší, než je přípustné,
- být vybavena tak, aby byl možný její dohled a monitoring, jak ze strany příslušného operátora, tak i ze strany OC,
- být v případě kabeláže LAN provedena tak, aby k ní neměly nekontrolovatelný fyzický přístup neoprávněné osoby.

6.3.3 Požadavky na komunikační služby

Komunikační služby ISOC musí:

- umožnit časové nebo adresné omezení, například omezením přístupu na některé adresy (servery) Internetu, k některým složkám nebo souborům Intranetu a podobně,
- zahrnovat účinnou antivirovou a antispamovou ochranu služby elektronické pošty,
- zahrnovat vybavení rozhraní mezi ISOC a Internetem, technologií firewall, antivirovou a antispamovou ochranou,
- zahrnovat dodatečnou autentizaci, nejlépe dedikovaným autentizačním serverem, uživatele v rámci služby vzdáleného přístupu do ISOC.

6.3.4 Požadavky na fyzický přenos dat

Data přenášená na fyzických datových nosičích, včetně notebooků, musí být chráněna před ztrátou jejich dostupnosti, integrity a důvěrnosti vhodnými BO technického i netechnického charakteru, například šifrováním.

6.4 Pravidla šifrové ochrany notebooků

Účelem šifrové ochrany notebooků je stanovit OC prostředky šifrové ochrany notebooků tak, aby byla zajištěna ochrana citlivých informací zpracovávaných v noteboocích uživatelů ISOC, a to zejména mimo objekty OC.

6.4.1 Princip šifrování

Šifrování dat na disku funguje pro potřeby uživatele velice transparentně. Šifrovací produkt vytvoří novou virtuální diskovou jednotku, která je ve skutečnosti odkazem na nějaký soubor na disku, či zašifruje celou partition. Pokud se při startu počítače nezadá správné heslo do tohoto programu, daný disk vůbec není vidět, případně není přístupný ani pro čtení. Tváří se jako nenaformátovaný oddíl, na němž jsou zapsána náhodná data.

6.4.2 Šifrovací programy

Nástrojů na šifrování existuje nespočet. Od těch úzce specializovaných, až k těm, které umožňují šifrovat nad rámec svého hlavního použití. Je možnost využití služeb mnoha šifrovacích programů a doporučit konkrétní program je velmi těžké, přesto existuje šifrovací program TrueCrypt, který svými funkcemi, cenou a využitím, stojí za uvedení.

TrueCrypt je jeden z nejpoužívanějších šifrovacích programů. Jedná se open source nástroj pro šifrování obsahu dat na disku pro operační systémy Microsoft Windows, Linux a Mac OS X. Nástroj umožňuje vytváření virtuálních disků v podobě souboru, který lze snadno připojit a pracovat s ním, jako s jakýmkoliv jiným pevným diskem, nebo zašifruje celý diskový oddíl. K souborům lze po připojení jednotky k souborovému systému počítače přistupovat běžným způsobem, což se stane až po zadání hesla - šifrovacího klíče. V případě, že je médium chráněno proti zápisu, tak disk bude připojen, ale nebude umožněno na něj zapisovat.

6.4.3 Počítačová bezpečnost

Uživatel je povinen šifrovat všechna citlivá data představující informace, jejichž kategorie citlivosti byla stanovena klasifikací informací a jsou uvedeny v katalogu klasifikovaných informací. Data kategorie K2-K4 je z důvodu zajištění dostupnosti, integrity a důvěrnosti informací, nutno šifrovat pomocí šifrovacího programu. Šifrována mohou být i jiná data podle úvahy uživatele služby. Uživatel služby je dále povinen šifrovat data kategorie K2-K4, která kopíruje na přenosná počítačová média, například na flash disk, optický disk, externí pevný disk atp., pro potřeby zálohování nebo fyzického přenosu. V případě fyzického přenosu musí být na cílový počítač nainstalován šifrovací program stanovený těmito pravidly.

6.4.4 Fyzická bezpečnost

Uživatel služby je povinen chránit notebook s instalovaným šifrovacím programem před fyzickým poškozením, zničením, ztrátou nebo odcizením. Uživatel služby nesmí ponechat notebook s instalovaným šifrovacím programem po přihlášení se k tomuto notebooku přístupný další osobě.

6.5 Pravidla ochrany osobních údajů

Ochrana osobních údajů je v České republice regulována zákonem č. 101/2001 Sb., o ochraně osobních údajů a o změně některých zákonů a dalšími právními předpisy. Správcům a zpracovatelům jsou při ochraně osobních údajů ukládány především povinnosti, zatímco subjektům údajů jsou dána práva. Na ochranu práv subjektů, údajů a kontrole plnění povinností správce a zpracovatele osobních údajů byl zřízen Úřad na ochranu osobních údajů. Za neplnění povinností stanovených správci nebo zpracovateli osobních údajů hrozí správci nebo zpracovateli osobních údajů sankce. Plnění povinností

uložených správci a zpracovateli předpokládá tyto povinnosti znát a vědět, jak je realizovat [11]. K výkladu zákona a tím i k osvětlení jednotlivých povinností stanovených správci nebo zpracovateli osobních údajů a k praktickému provádění ochrany osobních údajů, lze využít různé nástroje.

6.5.1 Základní zásady

Osobní údaje mohou být v ISOC zpracovávány pouze za podmínky, že jsou přijata taková BO, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití. Přijatá a provedená BO musí být zdokumentována. Zpracovatelé a příjemci osobních údajů zpracovávaných v ISOC jsou povinni dodržovat rozsah a způsob zpracování a seznamování se s osobními údaji, které stanoví správce evidence osobních údajů. Aplikace obsahující osobní údaje by měly být vybaveny nebo upraveny tak, že při jejich spuštění bude v dialogovém okně uvedeno upozornění na to, že aplikace obsahuje osobní údaje.

6.5.2 Prostředky zpracování osobních údajů

Prostředky systému ICT užité při zpracování osobních údajů v ISOC musí poskytovat záruku spolehlivosti a odolnosti proti vlastním poruchám i chybám personálu a dále poskytovat možnost zajištění ochrany přenášených dat. Pro potřeby likvidace osobních údajů na datových nosičích, musí mít zpracovatelé nebo příjemci osobních údajů k dispozici pokyny pro postup jejich výmazu, přepisu anebo mít k dispozici prostředky fyzického ničení nosičů.

6.5.3 Ochrana osobních údajů zpracovávaných v ISOC

Ochrana osobních údajů zpracovávaných v ISOC musí být zajištěna uplatněním pravidel řízení přístupu, antivirové ochrany, bezpečné výměny dat, šifrové ochrany notebooků a fyzické ochrany, která jsou stanovena pro ochranu dat, včetně osobních údajů, a prostředků pro zpracování informací v ISOC.

6.6 Pravidla školení informační bezpečnosti

Jak již bylo v práci uvedeno, uživatelé představují v současnosti nejslabší článek bezpečnosti informací v organizaci. A to nejen proto, že uživatelé zpravidla neradi čtou směrnice, a tudíž nedodržují jejich nařízení, ale i proto, že často rádi experimentují a

dopouštějí se tak řady zásadních prohřešků proti bezpečnosti. Z tohoto důvodu je nutností, neustálým a důsledným vštěpováním základních bezpečnostních pravidel a pracovních návyků efektivně zařídit, aby je uživatelé znali a chovali se podle nich.

Řešením výše nastíněného stavu může pro organizaci být školení na míru sestavené dle konkrétních požadavků pro uživatele určité specifické úrovně. Obsah školení může být upraven na základě platné bezpečnostní dokumentace OC. Uživatel musí mýt přístup ke studijním materiálům, prezentacím, směrnicím a nařízením v oblasti bezpečnosti organizace a to i v elektronické formě. Školení lze realizovat mimo prezenční formy také formou e-learningu.

6.6.1 E-learning

E-learning je vzdělávací proces, využívající ICT k tvorbě kurzů, k distribuci studijního obsahu, komunikaci mezi uživateli a správci bezpečnosti a k řízení studia. Základem elektronického vzdělávání jsou neustále dostupné a jednoduše aktualizovatelné informace v elektronické podobě. Předpokladem efektivního vzdělávání je profesionální metodické a technické zpracování těchto materiálů a jejich doplnění o studijní aktivity. Velmi vhodný nástroj pro elektronickou podporu vzdělávání a školení je systém řízení vzdělávání Moodle.

Moodle je dostupný certifikovaný Open Source výukový systém vhodný pro firmy, školy, úřady a další organizace, které chtějí využít forem e-learningu ve výuce zaměstnanců v uživatelsky přívětivém a jednoduchém prostředí. Každý kurz v tomto systému je strukturovaným prostředím a skládá se z jednotlivých instancí modulů, jako je fórum, studijní materiál, přednáška, test, slovník a další. Velké množství modulů základní instalace spolu s nepřeberným množstvím volně dostupných modulů třetích vývojářských stran umožňují uživatelům jednoduše vytvářet, sestavovat a udržovat obsah výuky (ať již on-line kurzů, nebo i podkladů ke klasické prezenční výuce), včetně vytváření různých forem testů přímo přes jednoduchá webová rozhraní.

Školení by mělo být zakončeno testem, který zahrnuje všechny aspekty bezpečnostní problematiky. Školení uživatelů mohou předcházet testy sociálním inženýrstvím, které zmapují jejich bezpečnostní povědomí. Školení by mělo být mj. založeno na praktických zkušenostech bezpečnostních konzultantů, které získali při realizaci nejrůznějších bezpečnostních projektů.

6.7 Pravidla zvládání bezpečnostních incidentů

Nedílnou součástí preventivní a aktivní ochrany ISOC je důsledné a efektivní řešení bezpečnostních incidentů včetně odstraňování jejich příčin a následků. Je nanejvýš nutné, aby na možnost narušení bezpečnosti ISOC byli jejich správci a uživatelé připraveni a měli k dispozici funkční struktury, efektivní postupy, pravidla a technické prostředky vedoucí k co nejrychlejšímu odstranění problémů při minimalizaci škod.
Z hlediska praktických potřeb správy bezpečnosti ISOC se způsob zvládání bezpečnostních incidentů přiměřeně vztahuje i na řešení bezpečnostních slabin a bezpečnostních událostí informačního systému.

6.7.1 Bezpečnostní slabiny

Bezpečnostní slabinou je slabé místo informačního aktiva OC vyplývající z nedostatků při jejich zadávání, akvizici, vývoji, výstavbě, provozu a údržbě. Může se jednat například o nevhodný návrh BO anebo protiopatření, nedostatečný dohled nad nimi, jejich nedostatečná údržba a servis, jejich nedodržování či nevyhovující obsluha. Bezpečnostní slabina může být příčinou bezpečnostní události nebo bezpečnostního incidentu. Příkladem bezpečnostní slabiny ISOC je neprovádění aktualizace signatur antivirového programu.
Personál, ale zejména zaměstnanci OC pověření výkonem bezpečnostních rolí proto musí působit k tomu, že bezpečnostní slabiny ISOC budou eliminovány nebo alespoň minimalizovány uplatněním vhodných protiopatření v rámci bezpečnostních záměrů, specifikací a projektů tvořících neoddělitelnou část zadávací, projektové a provozní dokumentace ISOC.

6.7.2 Bezpečnostní události

Bezpečnostní událostí ISOC je identifikovaný stav tohoto IS, ukazující na možné porušení bezpečnostní politiky nebo selhání BO anebo protiopatření, může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informačního systému a informací v něm zpracovávaných.
Bezpečnostní událost nemusí mít vždy za důsledek negativní dopad ani na ISOC, ani na OC. Příkladem bezpečnostní události ISOC je průnik viru zachyceného a zneškodněného antivirovým programem.

6.7.3 Bezpečnostní incidenty

Bezpečnostním incidentem ISOC je jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost ohrožení bezpečného provozu tohoto informačního systému a ohrožení bezpečnosti informací v něm zpracovávaných. Bezpečnostní incident vždy má nebo může mít za důsledek negativní dopad na ISOC. Příkladem bezpečnostního incidentu ISOC je průnik viru nezachyceného a ne-zneškodněného antivirovým programem.

6.7.4 Zdroje bezpečnostních incidentů

Zdrojem bezpečnostních incidentů ISOC je nevhodná lidská činnost, chyby či poruchy prostředků pro zpracování dat v ISOC nebo působení přírodních a jiných sil.
Za nevhodnou lidskou činnost nutno považovat neúmyslné i úmyslné aktivity lidí, zejména pak:

- chyby personálu,
- chyby uživatelů,
- krádež informačního aktiva,
- neautorizovaný přístup k objektům, zejména k datům v ISOC,
- neúmyslné poškození či zničení informačního aktiva,
- úmyslné přetížení provozu technologických prostředků,
- neúmyslné či úmyslné zavirování systému nebo jeho části,
- úmyslné poškození či zničení informačního aktiva,
- ztráta informačního aktiva.

Za chyby či poruchy prostředků pro zpracování dat v ISOC nutno považovat zejména:

- chyby SW vybavení (počítačových programů),
- poruchy HW vybavení (technických prostředků),
- chyby či poruchy COM vybavení (komunikačních prostředků),
- chyby či poruchy informačních nebo komunikačních služeb,
- poruchy napájení,
- poruchy klimatizace.

Za působení přírodních a jiných sil nutno považovat zejména:

- nedostatek personálu ISOC způsobený např. epidemií, dopravními problémy apod.,
- požár,
- průnik vody,
- přírodní pohroma, např. povodeň.

6.7.5 Obsah plánu

Plán zvládání bezpečnostních incidentů ISOC musí osahovat zejména:

- působnost plánu,
- účinnost plánu (datum),
- určení plánu,
- aktivace plánu,
- platnost plánu,
- kontakty na zúčastněné organizační útvary a zaměstnance OC,
- věcný a časový postup uplatnění plánu,
- zdroje pro uplatnění plánu (data, SW, HW a COM prostředky, komunikační služby, podpůrná technologie),
- kdo a kdy plán zpracoval a schválil.

ZÁVĚR

Cílem práce bylo zpracovat bezpečnostní politiku informačního a komunikačního systému organizačního celku do obecných pravidel, které jsou svým obsahem přístupnější a srozumitelnější uživatelům informačního a komunikačního systému. Práce se snaží formulovat bezpečnostní politiku krátce a obecně. Popisuje, jaké úrovně bezpečnosti se musí řešit v této obecné úrovní. Poukazuje na problematiku, kdy je stále častěji řešená otázka technického zabezpečení, přitom i ty nejdokonalejší technické prvky zabezpečení, jsou jen „kusem železa“ bez řádné konfigurace, správy a následného užívání.

V práci je popsán postup vytvoření kvalifikačního schématu, který rozděluje informace zpracovávané v informačním systému z hlediska jejich významu pro informační bezpečnost. Pro stanovené skupiny definuje konkrétní způsob jejich ochrany a nároky na jejich důvěrnost a dostupnost, příp. stupeň citlivosti informace. Následně je popsán systém řízení přístupu k takto klasifikovaným informacím, který definuje pravidla potřebná pro přidělování přístupu uživatelů a skupin uživatelů k informacím v rámci informačního systému. Další kapitola stanovuje základní pravidla bezpečnosti, kde jsou navržena pravidla antivirové ochrany, fyzické ochrany, bezpečné výměny dat, ochrany osobních údajů, šifrové ochrany notebooků. V závěru práce je popsáno, jak efektivním školením informační bezpečnosti zařídit, aby uživatele tyto stanovené bezpečnostní pravidla znali a chovali se podle nich.

Práce svým obsahem a stanovenými pravidly ochrany informací může být použitelná v průmyslu komerční bezpečnosti pro problematiku zabezpečení obraného konkurenčního zpravodajství na úrovni ochrany informací, dat, informačních a komunikačních systémů. Práce byla vytvořena na základě praktických zkušeností při správě, užívání a řízení informačního a komunikačního systému velké organizace. Svým rozsahem se snaží být použitelná jak pro využití v organizacích, v podnicích tak i v soukromých společnostech. Proto pro účel práce nebyla vybrána žádná konkrétní společnost ani organizace.

CONCLUSION

The aim of the thesis was to put the issue of security policy of information and communication system of organizational unit into the general rules which are its content more accessible and understandable to the users of information and communication system. The thesis attempts to formulate the security policy briefly and in general way. It describes the level of security that must be dealt with at this general level. It points out the issue of technical support, which is increasingly dealt with. However even the most sophisticated technical security features are only "piece of iron" without proper configuration, management and subsequent use.

In the thesis we can find the description for process of creating the qualifying scheme, which divides information processed by the information system with regard to their importance to information security. For the groups that were created it subsequently determines the specific way of their protection and their claims to confidentiality and availability, eventually a degree of sensitivity of the information. As further is described system of access management for such classified information, which defines the necessary rules for the allocation of access for users and groups of users to information within the information system. The next chapter sets out the basic rules of security, where the rules of anti-virus protection, physical protection, secure data exchange, protection of personal data and encrypted notebook protection are suggested.

In the conclusion of the thesis is described how to through effective information security training course arrange that the users know the security rules and act accordingly to them. Thesis with its content and established rules of protection of information can be applicable in commercial security industry focused on the issues of security defensive competitive reporting service on the level of protection of information, data and information and communication systems. The thesis is formed on basics of practical experience in the administration, usage and management of large organization. Its scope is trying to be applicable for usage in organizational units, enterprises and private companies. Therefore, for the purpose of the thesis was not selected any particular company or organization.

SEZNAM POUŽITÉ LITERATURY

[1] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribunu EU Vyd. 1. Brno: Tribun EU, 2009, 134 s. ISBN 978-80-7399-731-1.

[2] DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti*. Vyd. 1. Brno: CP Books, 2005, 50 s. ISBN 80-251-0574-1.

[3] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

[4] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[5] DOUCEK, Petr. *Řízení projektů informačních systémů*. Vyd. 1. Praha: Professional Publishing, 2004, 162 s. ISBN 80-86419-71-1.

[6] JAŠEK, Roman. *Informační a datová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-7318-456-7.

[7] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 80-7318-095-2.

[8] KOVACICH, Gerald L. *Průvodce bezpečnostního pracovníka informačních systémů: zavádění a prosazování bezpečnostní politiky informačních systémů*. Vyd. 1 Brno: Unis, 2000, 200 s. ISBN 80-860-9742-0.

[9] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Vyd. 1. Brno: Computer Press, 2007, 154 s. ISBN 978-80-251-1511-4.

[10] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[11] ČESKO. Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. dubna 2012. In: *Sbírka zákonů České republiky*. 2005. Dostupné z: http://www.uoou.cz/uoou.aspx?menu=4&submenu=5

[12] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. 2005. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/

[13] ČERMÁK, Miroslav. *Clever And Smart* [online]. 2010 [cit. 2013-03-19]. Dostupné z: http://www.cleverandsmart.cz/clanky/

[14] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Český normalizační institut, 2006.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AVO Antivirová ochrana.

BO Bezpečnostní opatření.

FO Fyzická ochrana.

HW Hardware.

ICT Information and Communication Technologies.

IKT Informační a komunikační technologie.

IS Informační systém.

ISOC Informační systém organizačního celku.

LAN Local Area Network

OC Organizační celek.

PIN Personal identification number.

SW Software.

SEZNAM OBRÁZKŮ

Obr. 1. Vstah jednotlivých hledisek bezpečnosti 13
Obr. 2. Analýza rizik 22
Obr. 3. Průběh auditu bezpečnosti. 27

SEZNAM TABULEK

Tab. 1. Vzor tabulky s klasifikačními údaji. 31
Tab. 2. Příklad rozdělení citlivých informací. 31
Tab. 3. Příklad rozdělení kritičnosti informací. 32
Tab. 4. Příklad rozdělení stupně ochrany. 32
Tab. 5. Stanovení ochrany informací. 33
Tab. 6. Typické příčiny ztráty důvěrnosti, integrity nebo dostupnosti informace. 33
Tab. 7. Stanovení protiopatření. 39