Implementace směrnice řídící fyzickou bezpečnost počítačové sítě v prostředí státní správy

Jiří Šatava

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří Šatava**
Osobní číslo:	**A11802**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Implementace směrnice řídicí fyzickou bezpečnost počítačové sítě v prostředí úřadu státní správy**
Téma anglicky:	**Implementation of the Directive Governing the Physical Security of Computer Networks in an Office of Public Administration**

Zásady pro vypracování:

1. **Prostudujte Instrukci Ministerstva spravedlnosti čj. 24/2012-OI-SP o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti.**
2. **Seznamte se se současným stavem fyzického zabezpečení budovy generálního ředitelství úřadu státní správy dle výše zmíněné instrukce.**
3. **Popište stávající stav jednotlivých částí informační infrastruktury a její fyzické bezpečnosti s ohledem na výše zmíněné nařízení v této budově.**
4. **Neopomeňte také podpůrné systémy, např. klimatizaci, záložní zdroje energie a politiku procesní bezpečnosti.**
5. **Diskutujte případné rozpory s uvedenou bezpečnostní směrnicí a navrhněte řešení těchto rozporů.**
6. **Vypracujte komplexní návrh zabezpečení budovy vycházející ze současného stavu a splňující výše uvedenou směrnici.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003, 316 s. ISBN 80-902-9382-4.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Vyd. 2. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 316 s. ISBN 978-80-87500-19-4.**
4. **IVANKA, Ján. Mechanické zábranné systémy. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 386 s. ISBN 978-80-7318-910-5.**
5. **LAUCKÝ, Vladimír a Rudolf DRGA. Speciální technologie komerční bezpečnosti. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-146-9.**

Vedoucí bakalářské práce: **Ing. Lubomír Macků, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **3. června 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

…….
podpis diplomanta

ABSTRAKT

Práce odráží skutečnou situaci, kdy je vydána směrnice, která nastavuje standardy v oblasti bezpečnosti informačních technologií v prostředí úřadu státní správy. Jedná se o fyzické zabezpečení nejdůležitější infrastruktury, reprezentující centrální úložiště dat, servery virtuálního centra, páteřní aktivní prvky a router pro připojení do WAN. Infrastruktura je umístěna v jedné serverovně. Prvotním krokem je analýza směrnice. Dále následuje porovnání se skutečným stavem a nakonec uvedení skutečného stavu do souladu s požadavky směrnice.

Klíčová slova: směrnice, fyzická bezpečnost, serverovna, rizika, incident

ABSTRACT

Work reflects real situation, when issued directive that sets standards in the field of information technologies security in environment of state authority. It is the physical security of critical infrastructure, representing the central data storage, servers of virtual center, the core switchess and router for connection to the WAN. Infrastructure is located in single server room. The first step is analyzing of directive. Followed by a comparison with the actual situation and ultimately put into the actual state of compliance with the requirements of the directive

Keywords: directive, physical security, server room, risks, incident

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Lubomíru Macků, PhD. za řadu rad a připomínek, které výrazným způsobem přispěly ke zkvalitnění této práce.

Motto: „Pravděpodobnost výskytu rizika nelze vyloučit, pouze snížit na přijatelnou mez. ”

OBSAH

ÚVOD

Události přelomu milénia, především skandál firmy Enron, kde došlo k hrubým manipulacím s daty v účetnictví s cílem zakrýt blížící se bankrot, ukázaly potřebu zabezpečit infrastrukturu informačních a komunikačních technologií (ICT) i po stránce fyzické bezpečnosti. Výsledkem byl federální zákon přijatý Senátem a Sněmovnou reprezentantů Spojených států s účinností k 30. červenci 2002, který vešel v obecnou známost jako Sarbanes - Oxley Act. Povinnost dodržovat tento zákon se vztahovala na všechny obchodní společnosti kotované na newyorské burze. Vzhledem ke své kvalitě a komplexnosti se tato norma, respektive její části, zabývající se technickými a procesními opatřeními, stala celosvětově základem směrnic upravujících problematiku v této oblasti. Firmy a státní a veřejné instituce jsou si vědomy důležitosti zabezpečení infrastruktury informačních technologií a dat. V České republice se směrnice upravující tuto oblast implementují v masovém měřítku. Práce se zabývá praktickou implementací části směrnice s názvem Politika bezpečnosti ICT (dále jen Směrnice) v prostředí Generálního ředitelství úřadu státní správy (dále jen Úřadu)

Dotčené odstavce Směrnice jsou přílohou č. 1 této práce.

I. TEORETICKÁ ČÁST

1 POSTAVENÍ SMĚRNICE V LEGISLATIVĚ ČESKÉ RUPUBLIKY

"Veřejná správa se kromě obecně závazných právních předpisů řídí rovněž předpisy vnitřními, (interními) závaznými toliko dovnitř veřejné správy. Právními předpisy jsou ústavní zákony, zákony, zákonná opatření Senátu, nařízení vlády, právní předpisy vydávané ministerstvy a jinými správními úřady (zejména vyhlášky ústředních správních úřadů), rovněž právní předpisy vydávané orgány územních samosprávných celků v přenesené působnosti (nařízení obcí a krajů) a v neposlední řadě obecně závazné vyhlášky obcí a krajů. Pro veřejnou správu mají nemalý význam také mezinárodněprávní závazky, především mezinárodní smlouvy podle čl. 10 Ústavy, které jsou součástí právního řádu a mají aplikační přednost před zákonem. Zásadní význam pro činnost veřejné správy má s ohledem na čl. 2 odst. 3 Ústavy a čl. 2 odst. 2 Listiny základních práv a svobod, zákon. Zákonodárnou iniciativu má vláda, poslanec nebo skupina poslanců, Senát (jako celek) a zastupitelstvo kraje.

Legislativní proces pro tvorbu zákonů (zákonodárný proces) je rámcově upraven v Ústavě. Pro státní správu, zejména pro ministerstva a jiné ústřední správní úřady, které předkládají vládě ke schválení návrhy právních předpisů nebo je samy vydávají, je pak průběh legislativního procesu obecně upraven na vládní úrovni v Legislativních pravidlech vlády. Zatímco právní předpisy jsou obecně závazné a zavazují tak neomezený okruh adresátů vně veřejné správy, předpisy interní zavazují pouze samu veřejnou správu, a to v rámci vztahů nadřízenosti a podřízenosti (usnesení vlády zavazují v zásadě celou státní správu, vnitřní předpisy jednotlivých správních úřadů pak zavazují tyto úřady a úřady jim podřízené). Od normativních právních aktů, jakožto obecně závazných pramenů práva, odlišujeme interní normativní směrnice (1).

Interní normativní směrnice (za vnitřní předpis je možno v synonymu považovat též interní předpis, vnitřní směrnici, směrnici, pokyn, vnitřní normativní akt, interní akt řízení a další pojmy, spadající do definice vnitřního předpisu) nemusejí být veřejně vyhlášeny, postačuje, jsou-li vhodným způsobem sděleny těm, jichž se týkají. Lze jimi zavazovat v příslušných věcech podřízené orgány a osoby ve vnitřních vztazích veřejné správy, jakož i podřízené organizační složky státu a státní příspěvkové organizace či jiné státní organizace (2). Vnitřní předpisy nejsou prameny práva, vztahy v nich obsažené nejsou právními normami. Jejich vydáváním se uskutečňuje oprávnění řídit činnost podřízených a jejich plnění je zachováváním právní povinnosti řídit se pokyny nadřízených. Tato oprávnění a

povinnosti vyplývají z obecně závazných, normativních právních aktů, jež jsou prameny práva." [1]

2 SMYSL SMĚRNICE

Směrnice komplexně pokrývá ochranu infrastruktury ICT proti následujícím typům incidentů:

- požár

- přepětí na napájení silovou elektřinou, způsobené zpravidla indukovaným napětím po úderu blesku v okolí objektu

- výpadek napájení vlastních informačních technologií i podpůrných systémů jako jsou klimatizace, poplachový zabezpečovací a tísňový systém (PZTS), Elektrická požární signalizace (EPS), stabilní hasící zařízení (SHZ) a systémů sledujících fyzikální parametry prostředí

- změna fyzikálních parametrů prostředí (teploty, vlhkosti, úrovně hladiny vody)

- vniknutí neautorizované osoby

2.1 Řízení rizik

2.1.1 Analýza Směrnice

Směrnice pokrývá také oblasti, které nejsou předmětem této práce. Pro účely zabezpečení serverovny je třeba implementovat opatření z článku 4 FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ, týkající se serveroven a centrální úložny dat.Konkrétně jsou to odstavce 33, 34, 35, 43, 44, 45, 47, 48, 49, 50, 51. Jednotlivé požadavky podle odstavců je třeba v prvním kroku rozebrat, pak porovnat se skutečností a nakonec navrhnout postup jejich implementace, pokud již nejsou splněny.

2.1.2 Odstavec 33 - ochrana proti vlivům vnějšího prostředí a požáru

Serverovna musí být v uzavřeném prostoru, chráněném před povětrnostními vlivy. Prostor musí být stavebně ohraničen zdmi nebo příčkami s dostatečnou odolností proti vniknutí a stavební otvory musejí být okny a dveřmi s pevnou a nepropustnou výplní jako prevencí proti vniknutí vnějších vlivů prostředí. Protipožárním opatřením je instalace EPS a vhodného hasícího zařízení, kterým se rozumí hasící přístroj s čistým hasivem nebo nákladnější forma, kterou je SHZ. EPS musí být projektován, instalován, provozován a revidován podle normy České státní normy (ČSN) 34 2710. SHZ se obdobně řídí normou ČSN 8421-1 až 6.

2.1.3 Odstavec 34 - fyzická bezpečnost

Požadavek projektu na fyzickou bezpečnost, jehož součástí jsou zásahové plány pro případ vzniku incidentu. Instrukce v těchto plánech musejí obsahovat popis informačního kanálu, kterým se informace o incidentu přenese na osobu zodpovědnou za jeho řešení. Přesný popis, jak je incident charakterizován (například stavem poplach na EPS), instrukce předepisující jednání osoby pro každý typ incidentu a činnosti následující po jeho vyřešení, které spočívají jednak v opětovném uvedení dotčených prostor do původního stavu, jejich zajištění, a následné administrativní úkony, jako zápisy o incidentu a další přenesení informací, většinou nadřízeným osobám.

2.1.4 Odstavec 35 - mechanické zabezpečovací systémy

Ochrana prostor, ve kterém se centrální aktiva ICT nacházejí pomocí mechanických zabezpečovacích systémů (MZS). Směrnice nepředepisuje striktně některou ze tříd RC 1 - RC 6 normy ČSN EN 1627 - 30 (Česká státní norma Evropská norma). Je na konkrétním projektantovi, jak ohodnotí míru rizik a hodnotu aktiv ICT. Vzhledem k vnějším podmínkám a celkové ostraze budovy se jeví jako dostatečná třída zabezpečení mechanickými zábrannými systémy RC 3.

2.1.5 Odstavce 33 - 42 - organizační zásady

Organizační zásady řeší přístupy osob do serverovny, revize těchto přístupů, klíčové hospodářství a kódy k PZTS.

2.1.6 Odstavec 45 - rozmístění zařízení v serverovně

Částečně je řešeno racionálním rozmístěním zařízení v serverovně. Je zde kladen důraz na oddělení záznamových médií od diskových polí, aby v případě fyzického zničení serverovny nedošlo současně i ke zničení i těchto dat. Tato problematika je řešena současně, ovšem vzhledem ke své nákladnosti a časové náročnosti, nelze čekat na to, až bude řešení hotovo a implementace zabezpečení bude počítat s hodnotou aktiv včetně pouze jedné sady produkčních dat. Vstup osob a jejich chování je určen v Provozním řádu serverovny, který je přílohou číslo 1. této práce. V tomto odstavci je nařízena také redundance napájení technologií.

2.1.7 Odstavec 46 - záloha napájení a ochrana proti přepětí

Přívody elektřiny pro silové napájení musejí být opatřeny přepěťovou ochranou, chránící i proti indukovanému napětí v případě úderu blesku.

2.1.8 Odstavec 49 - sledování vybraných fyzikálních parametrů prostředí

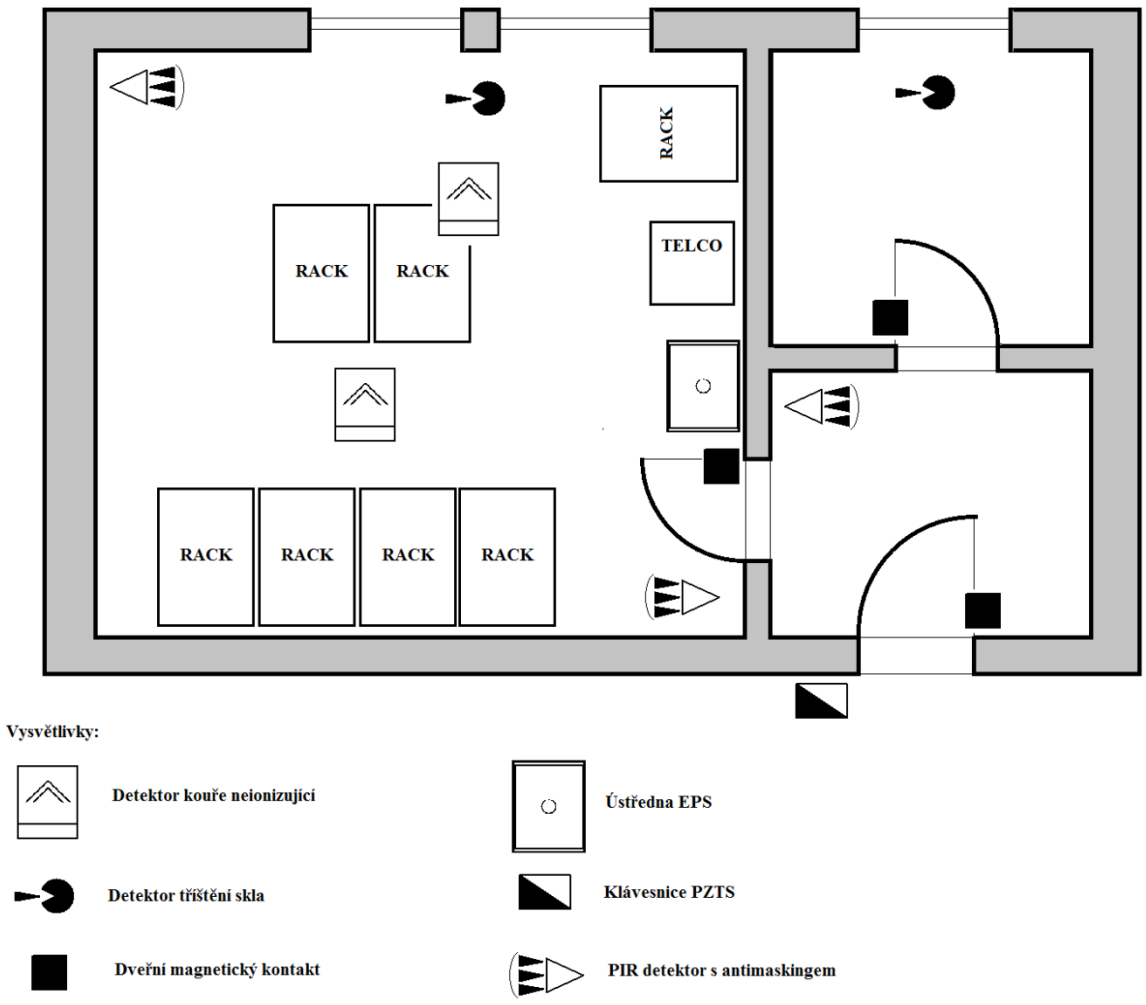
Serverovna musí být vybavena čidly sledujícími fyzikální parametry prostředí, především vlhkost a teplotu. Dále musejí být instalována záplavová čidla v dvojité technologické podlaze.

3 POPIS SOUČASNÉHO STAVU V PROSTORU S AKTIVY PODLÉHAJÍCÍMI OCHRANĚ

3.1 Situace v serverovně

Serverovna se nachází v přízemí budovy, které je přístupná pouze jedním vchodem s dozorem. Do objektu se nelze dostat bez prokázání totožnosti a v případě osob třetích stran, které nejsou držiteli čipové identifikační karty vydané na jméno, musí být zajištěn doprovod ze strany konkrétního zaměstnance.

Budova je vybavena PZTS a kamerovým systémem nepřetržitě sledujícím část vnějšího pláště budovy volně přístupného z ulice. Výstup z této elektronické ochrany je vyveden na nepřetržitou stálou službu umístěnou uvnitř objektu. Zabezpečení objektu je úrovni, která plně dostačuje pro umístění serverovny.



Obrázek č. 1 Plánek serverovny 1

Vlastní serverovna s aktivy ICT je umístěna v přízemí, okna jsou do velmi dobře střežené další části objektu, opatřená mřížemi. Plánek serverovny je na obrázku č. 1.

3.2 Hodnocení aktiv

V tabulce č. 1 jsou uvedena nejdůležitější aktiva umístěná v serverovně a jejich přibližná hodnota.

Tabulka č. 1 Hodnocení aktiv

Druh aktiva	**Popis**	**Počet kusů**	**Přibližná cena za kus**	**Celkem za položku**
HW	Virtualizační server	7	150 000,00 Kč	1 050 000,00 Kč
	Server	4	45 000,00 Kč	180 000,00 Kč
	PC	1	10 000,00 Kč	10 000,00 Kč
	Optický switch	2	30 000,00 Kč	60 000,00 Kč
	Ostatní aktivní prvky LAN	1	300 000,00 Kč	300 000,00 Kč
	Diskové pole Compellent	2	5 000 000,00 Kč	10 000 000,00 Kč
	Diskové pole CX-4	1	2 000 000,00 Kč	2 000 000,00 Kč
	Telekomunikační zařízení	1	N/A	
	UPS 20 kVA	2	250 000,00 Kč	500 000,00 Kč
	UPS 3 kVA	5	7 000,00 Kč	35 000,00 Kč
Data	Osobní a velmi citlivé údaje občanů souvisejících s činností Úřadu	30000	}	500 000 000,00 Kč
	Účetnictví organizace s ročním rozpočtem 11 mld Kč			
	Personalistika a mzdy současných i bývalých zaměstnanců	500		
	Uživatelská data a mailová komunikace v objemu přibl. 11 TB dat			
Přibližná hodnota aktiv celkem:				**514 135 000,00 Kč**

3.3 Řízení rizik

Riziko lze z technického pohledu chápat jako pravděpodobnost vzniku škody, tj. ohrožení lidského zdraví a životů, životního prostředí, majetkových a kulturních hodnot. [4]

Vzhledem k výše uvedeným skutečnostem, jako je dosavadní úroveň zabezpečení a hodnota aktiv, je zabezpečení zaměřeno především proti sofistikovaným útokům zevnitř, napade-

ní náhodným pachatelem z ulice není příliš pravděpodobné. Ohrožení živelnými pohromami je na srovnatelné úrovni se standardními kancelářskými prostorami v městské zástavbě v České republice, lze vyloučit povodně a záplavy.

3.4 Shrnutí teoretické části

V teoretické části byla provedena analýza současné situace v zabezpečení hlavní serverovny centrály Úřadu. Dále proběhlo seznámení se s požadavky Směrnice na fyzické zabezpečení budovy a serverovny. Implementace Směrnice bude probíhat v celém resortu ministerstva. Cílem Směrnice je reflektovat současný stav zabezpečení a upravit jej na přijatelnou úroveň. Autoři Směrnice záměrně nechali určitou volnost ve standardech zabezpečení a kladou důraz na administrativní procesy. Důvodem je využití již instalovaných systémů z důvodu nákladů, dále zachování kontinuity provozu systémů a využití znalosti obsluhy zaměstnanci. Na osobách zodpovědných za implementaci Směrnice je také hodnocení rizik a ocenění aktiv, aby byly náklady na instalaci a provoz zabezpečení adekvátní hodnotě aktiv, jež jsou chráněny.

II. PRAKTICKÁ ČÁST

4 NÁVRH IMPLEMENTACE SMĚRNICE V REÁLNÝCH PODMÍNKÁCH

Prvním krokem bude srovnání současného stavu zabezpečení s požadavky Směrnice. Požadavky byly analyzovány v teoretické části práce. Porovnání bude zpracováno formou tabulky. V případě chybějícího zabezpečení bude vytipována vhodná technologie, která oblast pokryje.

4.1 Bezpečnostní posouzení budovy

V systémovém návrhu budou při posuzování složek rizika určujícím faktorem bezpečnostního posouzení stavební dispozice. Mezi skutečnosti, které by měly být brány v úvahu patří: Konstrukce, otvory, režim provozu, držitelé klíčů, lokalita, stávající zabezpečení, místní legislativa či předpisy, prostředí. [2]

4.2 Porovnání současného stavu zabezpečeni s požadavky Směrnice

Tabulka č. 2 Druhy rizika

Původ rizika	Druh rizika	Opatření proti riziku (implementováno A/N)
1) Přírodní vlivy	Požár	Prokazatelné seznámení s provozem SHZ osobám s právem samostatného vstupu do serverovny (A)
		Stabilní hasící zařízení (A)
	Teplota	LAN čidlo s měřením vlhkosti a teploty stažené k ostraze (A)
	Vlhkost	LAN čidlo s měřením vlhkosti a teploty stažené k ostraze (A)
	Únik vody	Čidla zaplavení v dvojité podlaze (N)
	Vlivy vnějšího prostředí	Klimatizace (A)
		Těsnící okna, trvale zavřené dveře s požární odolností (A)
	Přepětí na přívodu silové elektřiny	Jističe s přepěťovou ochranou (A)
	Výpadek napájení	UPS a připojení k záložnímu generátoru elektřiny (A)
2) Lidský faktor	Vniknutí neatorizované osoby a její případná nepovolená činnost	PZTS (A)
		Prokazatelné seznámení s provozem PZTS a předávání a mazání uživatelských přístupových kódů (A)
		Klíčový režim (A)
		MZS (A)
		Uzamykatelné racky (N)
	Lidská chyba, zlý úmysl s cílem zneužití neúplného a nedostatečně definovaného administrativního procesu pro udělení povolení ke vstupu	Instrukce pro výkon služby stálé služby v prostoru serverovny (N)
		Provozní řád serverovny (N)

4.2.1 Požár

4.2.1.1 Prokazatelné seznámení s provozem stabilního hasícího zařízení osob s právem samostatného vstupu do serverovny

Je implementováno, pomocí formálně řízeného dokumentu. Dokument obsahuje chronologicky seřazené podpisy osob s právem samostatného vstupu, že byly seznámeny s obslu-

hou SHZ v případě jednotlivých stavových hlášení. Dokument obsahuje i datum poučení a podpis osoby, která poučení prováděla.

4.2.1.2 Stabilní hasící zařízení

Místnost je vybavena SHZ typu FK-Komplet®. Použité hasivo je typu HFC 236fa. Splňuje veškeré nároky na hašení informačních technologií, není toxické. SHZ byla projektována, instalována a je servisována odborně způsobilou firmou podle úpočadavků normy ČSN 8421 - 4. Zařízení má v sobě integrovanou i ústřednu EPS. Požadavek Směrnice je pokryt dostatečně.

4.2.2 Teplota a vlhkost

Pro monitoring teploty a vlhkosti v místnosti byl zvolen přístroj TH2E s čidlem SNS_THE_5m. Výhodou tohoto řešení je online přenos hodnot vlhkosti a teploty prostřednictvím LAN (lokální počítačová síť) do miniaplikace operačního systému Windows 7. Tato miniaplikace je nainstalována členům vedení odboru informatiky a stálé službě. Požadavek Směrnice je pokryt dostatečně.

4.2.3 Únik vody

Zařízení pro únik vody není v současné době nainstalováno. V serverovně je položena dvojitá technologická podlaha se zvýšenou únosností, která není vodotěsná, proto by se případná nežádoucí voda shromáždila v prostoru pod podlahou. Tento prostor je třeba osadit záplavovým čidlem s poplachovým stavem vyvedeným ke stálé službě. Návrh vhodného zařízení s přijatelnou cenou po průzkumu trhu je kombinace čidla Jablotron LD-12 s logickou jednotkou Quido ETH 3/0. Tento systém též komunikuje prostřednictvím místní počítačové sítě LAN do miniaplikace systému Windows 7. Tato miniaplikace je nainstalována členům vedení odboru informatiky a stálé službě. Pro nejvyšší úroveň zabezpečení se používá vodotěsná komora, ve které je umístěna celá serverovna. Vzhledem k nákladům a rozsahu stavebních prací, které by nebyly v reálných podmínkách akceptovatelné, se nebude toto řešení implementovat. Požadavek Směrnice bude záplavovým čidlem s logickou jednotkou pro přenos informace do počítače stálé služby pokryt dostatečně.

4.2.4 Vlivy vnějšího prostředí

4.2.4.1 Klimatizace

Je instalována, z důvodu redundance jsou instalovány čtyři jednotky s kompresory a výměníky umístěnými vně budovy. Klimatizace podléhá pravidelné roční profylaxi. Požadavek Směrnice na klimatizaci je pokryt dostatečně.

4.2.4.2 Těsnící okna, trvale zavřené dveře s požární odolností

Serverovna je umístěna uvnitř přízemí budovy, není zde riziko proniknutí vody při případné poruše izolace střechy. Vnější obvodová zeď je pouze jednou ze stěn, tato je osazena moderními plastovými okny s dostatečnou schopností izolace proti vnější vlhkosti, prachu, průniku hmyzu nebo jiných živočichů a proti teplotním rozdílům vně a uvnitř budovy. Dveře jsou bezpečnostní třídy RC 3, s požární odolností 30 minut. Požadavek Směrnice na izolaci vůči vlivům vnějšího prostředí je pokryt dostatečně.

4.2.5 Jističe s přepěťovou ochranou

Na přívodech silové elektřiny jsou instalovány přepěťové ochrany typu SLP-275 V/3. Instalaci prováděla firma s odbornou způsobilostí. Po instalaci byla provedena řádná revize nezávislou firmou a dále jsou prováděny pravidelné revize podle §2 Nařízení vlády č 378/2001 Sb. Součástí opatření je i propojení ukostření všech spotřebičů společným uzemněním. Tyto požadavky v legislativě České republiky reprezentuje ČSN 341390.

Tato norma obsahuje několik doporučení, vztahujících se k vnitřní ochraně před bleskem. Důležité jsou údaje o pospojování, resp. oddálení kovových konstrukcí od jímacích vedení a svodů. Kvalitní vnější ochrana před bleskem samozřejmě přispívá ke snížení ohrožení elektronických zařízení uvnitř. [3]

Požadavek Směrnice na ochranu proti přepětí je pokryt dostatečně.

4.2.6 Výpadek napájení

Riziko výpadku napájení je sníženo bezvýpadkovým systémem napájení. Silové přívody elektřiny jsou jištěny záložním generátorem. Pro výpadek do startu generátoru nebo pro případ jeho poruchy je silová elektřina vedena přes dvě UPS (zdroj nepřetržitého napájení) s výstupním výkonem 20 kVA a pět UPS s výstupním výkonem 3 kVA. Všechny klíčové informační technologie se dvěma redundantními zdroji elektrické energie jsou zapojeny

vždy tak, že každý zdroj je zapojen do jiné UPS. UPS podléhají pravidelným revizím a akumulátory elektrické energie jsou vyměňovány v intervalech stanovených výrobcem, aby se preventivně předešlo jejich poruše z důvodu překročení životnosti. Podpůrné systémy, jako jsou klimatizace, která není citlivá na krátkodobý výpadek napájení z hlediska automatického startu po výpadku, PZTS a SHZ včetně ústředny EPS, obsahující vlastní akumulátory pro řádově desítky minut nezávislého provozu, jsou připojeny na záložní generátor. Celý napájení systém je jednou ročně zkoušen za přítomnosti revizního technika a techniků odboru informatiky formou simulovaného výpadku napájení silovou elektřinou z veřejné sítě. Požadavek Směrnice na zabezpečení napájení proti výpadku je pokryt dostatečně.

4.2.7 Vniknutí neautorizované osoby a její případná nepovolená činnost

4.2.7.1 Poplachový a tísňový zabezpečovací systém

Místnost je vybavena samostatným podsystémem PZTS, střežícím celou budovu. PZTS byla projektována a instalována odborně způsobilou firmou a podléhá pravidelným zkouškám a revizím. Požadavek Směrnice na zabezpečení pomocí PZTS je pokryt dostatečně.

4.2.7.2 Prokazatelné seznámení s provozem poplachového a tísňového zabezpečovacího systému a předávání a mazání uživatelských přístupových kódů

Ve formálně řízeném dokumentu je prokazatelně potvrzeno osobami s právem samostatného vstupu do serverovny, že byli seznámeni s obsluhou PZTS na uživatelské úrovni a že jim bylo umožněno nastavit si vlastní kód pro odstřežení a zastřežení prostor. V případě zániku práva na samostatný vstup je prokazatelně potvrzeno, že jejich přístupové kódy byly vymazány. Požadavek Směrnice o prokazatelném seznámení s provozem PZTS a předávání a mazání uživatelských přístupových kódů je splněn dostatečně.

4.2.7.3 Klíčový režim

Ve formálně řízeném dokumentu je prokazatelně potvrzeno osobami se právem samostatného vstupu do serverovny, že jim byly předány klíče od serverovny. V případě zániku práva na samostatný vstup je prokazatelně potvrzeno, že osoby klíče odevzdaly. Požadavek Směrnice o prokazatelném předání a případném odevzdání klíčů je splněn dostatečně.

4.2.7.4 Mechanické zábranné systémy

Obvodové zdi i příčky jsou z plných cihel. Vstupní dveře jsou trvale zavřené, jsou projektovány a instalovány odborně způsobilou firmou jako bezpečnostní třída RC 3, certifikát byl součástí dodávky. Okna jsou do střeženého prostoru, navíc osazena kovovými mřížemi s tloušťkou plného čtvercového profilu 20 mm.

Mechanické zábranné systémy mají svou zásadní nezastupitelnost zejména proto, že jsou schopny poskytnout ochranu objektu mechanickou odolností (pevností), kterou jednotlivé komponenty mají a jsou nimi charakterizovány. [5]

Požadavek Směrnice na MZS je splněn dostatečně.

4.2.7.5 Uzamykatelné racky

Racky v serverovně jsou bez některých bočních, zadních i předních otevíratelných stěn. Vzhledem k informaci od dodavatele, že již nejsou ve výrobě, bude potřeba je nahradit novými. Na základě průzkumu trhu byl zvolen masívní stojanový rozvaděč APC NetShelter SX 42 U (Jednotka výšky v racku 44,45 mm) 750mm Wide x 1200mm Deep. Důležitými parametry jsou hloubka 1200 mm, nosnost 1000 kg a konstrukce stěn umožňující chlazení instalovaných zařízení s vysokým tepelným vyzařováním. Pro infrastrukturu ICT bude potřeba pořídit dva kusy racků. Toto řešení plně pokryje požadavky Směrnice na uzamykatelné racky.

4.2.8 Lidská chyba, zlý úmysl s cílem zneužití neúplného a nedostatečně definovaného administrativního procesu pro udělení povolení ke vstupu

4.2.8.1 Instrukce pro výkon stálé služby v prostoru serverovny

Nebyly dosud vytvořeny, jejich tvorba je součástí této práce. Jsou v příloze PIII. Budou navrženy k zařazení do interní legislativy Úřadu v nejvyšším stupni důležitosti NGŘ (nařízení generálního ředitele).

4.2.8.2 Provozní řád serverovny

Nebyl dosud vytvořen, jeho tvorba je součástí této práce. Je přílohou číslo 2. této práce. Bude navržen k zařazení do interní legislativy Úřadu v nejvyšším stupni důležitosti NGŘ.

5 SOUHRN VYBAVENÍ K NÁKUPU

V Úřadu je nákup realizován prostřednictvím odboru logistiky. Ve specifikaci požadavku musí být uveden název komodity, počet kusů, parametry pro účely vypsání veřejné zakázky a předpokládaná cena pro účely finančního plánování. Analýzou byla identifikována potřeba nákupu

5.1 Čidlo a logická jednotka pro sledování teploty a vlhkosti

5.1.1 Specifikace produktu

Zařízení pro přenos informace o vlhkosti a teplotě v serverovně ke stálé službě.

5.1.2 Počet kusů

Jeden kus čidla a jeden kus logické jednotky.

5.1.3 Parametry pro zadání veřejné zakázky

Parametry byly zvoleny s ohledem na zařízení s nízkou cenou, které splňuje požadavky Směrnice pro ochranu a respektuje místní situaci v objektu, především umístění pracoviště stálé služby.

Čidlo:	Rozsah měřené teploty: -40 až +123,8 °C
	Stupeň krytí: IP 54
	Kabel ke snímači - teplotní odolnost: -60 °C až +200 °C
	Přívodní silikonový kabel délky 5 metrů
Logická jednotka:	webová stránka s aktuálními hodnotami i stránky pro konfiguraci jsou v češtině nebo angličtině.
	XML (druh formátu dat) soubor s aktuálními hodnotami.
	TCP (protokol přenosu informací v počítačové síti) protokol: Auto matické odesílání naměřených hodnot
	Automatický výpočet rosného bodu.
	Ukládání hodnot do interní paměti s kapacitou až 1000 záznamů (každý záznam s časovou značkou). Několik režimů ukládání do paměti:

(1) Časový - ukládání každých X minut;
(2) Diferenciální - k uložení záznamu dojde až když se měřená hodnota pohne o X od naposledy uložené hodnoty;
(3) Záznam mezních hodnot - ukládá se vždy jen hodnota, při které se mění tendence sledované veličiny.

Paměť extrémních hodnot – TH2E si pamatuje maximální a minimální naměřenou hodnotu od každé měřené veličiny, včetně data a času měření.Připojení a komunikace přes počítačovou síť (Ethernet).

Přenos dat protokoly TCP/IP (10/100 Ethernet).

Sledování hodnot i konfigurace přes webové rozhraní.

Odnímatelný snímač Napájení 5 V až 30 V z dodaného zásuvkového adaptéru.

Možnost uchycení na lištu DIN (německá průmyslová norma) 35 mm.

5.1.4 Předpokládaná cena

1400,- Kč včetně DPH

5.2 Záplavové čidlo a logická jednotka

5.2.1 Specifikace produktu

Zařízení pro přenos informace o hladině vody v technologické podlaze v serverovně ke stálé službě

5.2.2 Počet kusů

Jeden kus čidla a jeden kus logické jednotky.

5.2.3 Parametry pro zadání veřejné zakázky

Bylo zvoleno jednoduché zařízení s nízkou cenou, s funkcí přenosu informace do pracoviště stálé služby.

Čidlo: Indikace hladiny vody

Logická jednotka: Ovládání a dohled přes Ethernet (10/100 Ethernet; běžná počítačová síť LAN)

Komunikační možnosti: Webové rozhraní, e-mail, Sledování stavu vstupů.

5.2.4 Předpokládaná cena

3000,- Kč včetně DPH

5.3 Rack 19"

5.3.1 Specifikace produktu

Skříň pro instalaci infrastruktury v rackovém provedení 19".

5.3.2 Počet kusů

Dva kusy.

5.3.3 Parametry pro zadání veřejné zakázky

Parametry racků byly zvoleny s ohledem na vysokou hmotnost in stalovaných zařízení, především UPS, hloubka byla zvole v hodnotě 1200, protože jsou zde zařízení s velkou hloubkou a množstvím kabelů, které jsou za nimi v pořadačích.

Výška:stojanu: 42 U, Šířka stojanu: 19", Hmotnost (statická zátěž): 1300 kg, Hmotnost (dynamická zátěž): 1000 kg, minimální hloubka: 1200 mm, konstrukce dveří a stěn umožňující chlazení při provozu zařízení s celkovým příkonem 10 kW.

Dodávka musí obsahovat: šachtový hardware, dokumentaci, klíče, stejně zaklínované dveře, boční panely a zadní panel, vyrovnávací paty, montážní hardware, předinstalovaná kolečka, uživatelskou pří ručku, organizéry svislé kabeláže

5.3.4 Předpokládaná cena

145 000,- za oba racky včetně DPH.

ZÁVĚR

Směrnice odhaluje slabá místa v zabezpečení a standardizuje jej v celém resortu ministerstva. Na příkladu serverovny generálního ředitelství Úřadu lze ukázat, že slabá místa zabezpečení jsou často pouze nedotaženosti již implementovaného řešení a z důvodu takzvané provozní slepoty nebo chybně nastavených priorit tvoří slabá místa. Směrnice je podle názoru autora práce koncipováa velmi vyváženě s ohledem na podmínky resortu, se znalostí úrovně aktiv a finančních možností.

Přímé finanční náklady na implementaci části směrnice, která je předmětem této práce, činí přibližně 175 000 Kč včetně DPH. Další činnosti spočívají v kontrole procesů a doplnění některých chybějících dokumentů.

Záběr Směrnice je však mnohem širší, implementaci opatření je věnován čas přesahující dva roky.

Směrnice již prošla auditem jakosti procesů. Účelem těchto procesů je podrobně vyhodnotit efektivnost, stupeň inovací a výkonnost pracovních procesů a postupů. [6]

Veškerá slabá místa v zabezpečení byla zpracována a předložena vedení Úřadu. Bylo možno získat globální pohled na situaci kvůli centralizovanému nákupu materiálu a služeb pro účely implementace požadavků. Úřad má 36 poboček, vybavení a služby externích firem jsou nakupovány hromadně, což znamená ušetření nákladů a velkou redukci administrativní práce při nákupu formou VŘ. Sumarizovaná data jsou průběžně aktualizována a tvoří přehledný manažerský nástroj , informující vedení Úřadu i ministerstva i průběhu implementace Směrnice. Pokynem vedení Úřadu bylo nařízeno, že všechny administrativní a technické požadavky, typicky chybějící dokumentace, hesla k aktivním prvkům a korektní zapojení UPS, musejí být implementována bezodkladně a nebudou v sumarizaci.

Největším problémem při implementaci fyzického zabezpečení bylo získání komplexního pohledu na problematiku a stanovení si výchozího bodu pro uvedení požadavků Směrnice do souladu se skutečností. Jako tento výchozí bod byla zvolena kontrola dokumentace a její doplnění.

V tabulce, jenž je přílohou této práce byla uvedena, jsou uvedena pouze ta opatření, které budou znamenat vynaložení prostředků z rozpočtu Úřadu. Tabulka bude předána nejvyššímu managementu k naplánování centralizovaného řešení.

SEZNAM POUŽITÉ LITERATURY

[1] VAVERA, PHD., JUDr. František. Ministerstvo vnitra České republiky: Vnitřní předpisy ve zkratce. [online]. [cit. 2015-04-16]. Dostupné z: http://www.mvcr.cz/clanek/vnitrni-predpisy-ve-zkratce.aspx

[2] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Vyd. 2. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.

[3] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003, 316 s. ISBN 80-902-9382-4.

[4] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 316 s. ISBN 978-80-87500-19-4.

[5] IVANKA, Ján. Mechanické zábranné systémy. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 386 s. ISBN 978-80-7318-910-5.

[6] LAUCKÝ, Vladimír a Rudolf DRGA. Speciální technologie komerční bezpečnosti. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-146-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT Informační a komunikační technologie

PZTS Poplachový, zabezpečovací a tísňový systém

EPS Elektrická požární signalizace

SHZ Stabilní hasící zařízení

ČSN Česká státní norma

MZS Mechanické zábranné systémy

LAN Lokální počítačová síť

UPS Uninterruptible Power Supply/Source, zdroj nepřetržitého napájení

U Jednotka výšky v racku 44,45 mm

NGŘ Nařízení generálního ředitele

XML Druh formátu dat

TCP/IP Protokol přenosu informací v počítačové síti

DIN Německá průmyslová norma

HZS Hasičský záchranný sbor

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PROVOZNÍ ŘÁD SERVEROVNY

I. Úvod

Serverovna slouží k uschování aktiv ICT a k jejich řádnému provozu. V serverovně není dovoleno skladování žádného materiálu a nejsou povoleny žádné činnosti které nesouvisejí s provozem informačních technologií zde instalovaných.

§1 Vymezení okruhů osob

Osoba odpovědná za chod serverovny: Vedoucí oddělení provozu ICT. Tato osoba rozhoduje o tom, kdo bude osobou určenou k samostatnému přístupu. Osoba odpovědná za chod serverovny odpovídá za revize podpůrných zařízení (PZTS, SHZ, klimatizace, UPS, měření teploty a vlhkosti) a za proškolení všech osob s právem samostatného přístupu do serverovny v obsluze s těmito zařízeními. Proškolení musí být písemně doloženo podpisem proškolené osoby. Dále odpovídá za odstranění všech závad, poruch a řešení incidentů. Vydává klíče od serverovny a uživatelský kód k PZTS. Je držitelem master kódu k PZTS.

Osoba s právem samostatného přístupu do serverovny: Vybraní zaměstnanci odboru informatiky, pověření správou aktiv ICT v serverovně umístěných. Dále členové vedení úřadu, ostraha objektu a správa budovy. Seznam těchto osob je v písemné podobě a jakákoli jeho změna do něj musí být ihned zanesena.

Ostatní osoby: jakékoli další osoby, pokud zde provádějí činnosti, které přímo souvisejí s provozem serverovny. Jejich přístup je dovolen pouze v doprovodu osoby odpovědné za chod serverovny nebo osoby s právem samostatného přístupu do serverovny. Tento doprovod nesmí nechat ostatní osobu, případně osoby, bez dohledu a odpovídá za všechny činnosti, které jsou v serverovně touto osobou nebo osobami prováděné.

§2 Chování v serverovně

Do serverovny je zakázáno vnášet jídlo, pití, kouřit zde, manipulovat s otevřeným ohněm a provádět cokoli dalšího, co by mohlo aktivovat SHZ. Je zakázána jakákoliv manipulace s hardwarem, s racky, s podpůrnými zařízeními zde instalovanými, která by vedla k ohrožení chodu zařízení, k úniku, ztrátě, nebo poškození dat a softwarového vybavení. Toto ustanovení se vztahuje i na činnosti prováděné mimo prostor serverovny za pomoci vzdáleného přístupu.

§3 Práce v serverovně

Všechny činnosti ostatních osob musejí být předem písemně specifikovány, písemně schváleny managementem Úřadu. Po celou dobu provádění činností nesmějí být ponecháni ostatní zaměstnanci bez dozoru výslovně určených osob. O jakékoliv činnosti musí být proveden objektivní a ucelený zápis v "Provozním deníku serverovny". Toto ustanovení se vztahuje i na činnost prováděné mimo prostor serverovny za pomoci vzdáleného přístupu.

§4 Incidenty

Každou mimořádnou událost, zjištěnou jakoukoliv osobou, je třeba zaznamenat do Provozního deníku serverovny a písemně o ní informovat i osobu odpovědnou za chod serverovny. Osobou odpovědnou za chod serverovny je vedoucí oddělení provozu ICT.

PŘÍLOHA P II: DOTČENÉ ODSTAVCE SMĚRNICE

4 FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

4.1 Zabezpečené oblasti

4.1.1 Serverovny a centrální úložny dat

Technické zásady:

33) Prostory, kde jsou uloženy centrální komponenty systémů ICT, centrální zálohy a archivy (dále jen "centrální aktiva systémů ICT"), musí být:

a) chráněny před hrozbami vnějšího prostředí;

b) ohraničeny uzavřeným a jasně definovaným perimetrem bez existence slabých, snadno proniknutelných míst;

c) vybaveny elektronickým požárním systémem (EPS) a vhodným hasicím zařízením.

34) Pro prostory, kde jsou uložena centrální aktiva systémů ICT, musí být vypracován projekt fyzické bezpečnosti a provozní řád, který je jeho součástí. Součástí provozního řádu nebo obsahem samostatného dokumentu musí být pokyny k ochraně aktiv systémů ICT (dokumentů, nosičů informací, archiválií, technologií apod.) v situacích, kdy bezprostředně hrozí, že dojde k jejich prozrazení, zneužití, poškození nebo zničení.

35) Prostory, kde jsou uložena centrální aktiva systémů ICT, musí být chráněny mechanickými prostředky (bezpečnostní dveře a zámky, mříže) a napojeny na elektronický zabezpečovací systém (EZS) proti neoprávněnému vniknutí.Úroveň opatření musí odpovídat důležitosti informací zde umístěných a požadované úrovni dostupnosti informací a služeb systémů ICT.

Organizační zásady:

36) Přístup do prostor resp. úschovných objektů (trezorů apod.), kde jsou uložena centrální aktiva systémů ICT, smí mít pouze pracovníci v rolích, které potřebují přístup do těchto prostor k plnění svých pracovních povinností.

37) Vstup návštěv (osob bez samostatné možnosti přístupu, včetně pracovníků úklidu, údržby, dodavatelů apod.) do prostor, kde jsou uložena centrální aktiva systémů ICT, je možný pouze po schválení osobou určenou provozním řádem, a to pouze v doprovodu některého z pracovníků, který má povolen přístup podle předchozího odstavce.

38) Datum a čas příchodu a odchodu návštěv do/z prostor, kde jsou uložena centrální aktiva systémů ICT, včetně identifikace účastníků návštěvy a pracovníka, který je doprovázel, musí být zaznamenán a návštěvníci musí být pod stálým dohledem oprávněné osoby. Záznamy o vstupech musí být uchovány minimálně po dobu 1 roku.

39) Musí být určena osoba/role odpovídající za udržování seznamu osob, které mají

povolen přístup k centrálním aktivům systémů ICT a mají k dispozici klíče, autentizační **předměty**, kódy EZS apod., a to včetně historie (již neplatných povolení).

40) Přístupová práva do prostor, kde jsou uložena centrální aktiva systémů ICT, musí být kontrolována minimálně jednou za 6 měsíců. O této kontrole musí být proveden záznam.

41) Prostory, kde jsou uložena centrální aktiva systémů ICT, při nepřítomnosti oprávněných osob, musí být fyzicky uzamčeny a, pokud je to možné, monitorovány EZS.

42) Na pracovištích, kde jsou uložena centrální aktiva systémů ICT, nesmí být ukládány hořlavé nebo jinak nebezpečné materiály (např. prázdné obaly od technického vybavení), je zakázáno zde jíst, pít a kouřit.

4.1.2 Kanceláře

Organizační zásady:

43) Systémy ICT, určené pro zpracování vnitřních agend justiční složky, a jejich části musí být umístěny v prostorách bez volného přístupu veřejnosti.

44) Kritické systémy ICT a jejich další aktiva,zejména evidované nosiče informací, musí být v době mimo přítomnost oprávněných osob umístěny a ukládány v souladu s provozním řádem, který je součástí projektu fyzické bezpečnosti.

4.2 Bezpečnost zařízení

4.2.1 Umístění zařízení a jeho ochrana

Organizační zásady:

45) Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup. Přitom je třeba zvažovat:

a) minimalizaci nadbytečného přístupu do pracovních prostor;

b) umístění prostředků pro zpracování a ukládání dat tak, aby bylo sníženo riziko možného odezírání informací;

c) izolování aktiv, která vyžadují zvláštní ochranu, s cílem snížit rozsah požadované celkové ochrany;

d) pravidla omezující jídlo, pití a kouření v blízkosti zařízení ICT;

e) monitorování působení vnějšího prostředí (jako např. teploty a vlhkosti).

46) Všechny centrální komponenty systémů ICT musí být chráněny před selháním napájení.

47) V periodě stanovené provozní dokumentací systému ICT, nejdéle však jednou za 6 měsíců, musí být překontrolována zařízení napojená na generátor náhradního napájení nebo na UPS a zkontrolováno, zda je výkon generátoru a příkon UPS dostatečný (s ohledem na nárůst způsobený nově připojenými technologiemi).

Technické zásady:

48) Ve všech serverovnách systémů ICT musí být nasazena ochrana proti blesku na elektrickém vedení.

49) V prostorách s umístěnými komponentami kritických systému ICT musí být kontinuálně monitorována teplota; výstupy monitorování musí být pravidelně (min. 1x za 30 minut) sledovány.

50) Všechny centrální komponenty systémů ICT musí být

* buď napojeny na UPS a generátor náhradního napájení s dobou náběhu menší než je doba provozu UPS. Generátor musí být pravidelně kontrolován a v případě delšího používání musí být zajištěno zásobování pohonnou hmotou

* nebo napojeny na UPS a musí být nastaven řízený shutdown všech serverů.

51) Veškeré podpůrné služby jako elektřina, topení/ventilace a klimatizace musí být přiměřené systému, který podporují. Klimatizace musí být napojena na generátor náhradního napájení, pokud je použit.

4.2.2 Bezpečnost kabelových rozvodů

Technické zásady:

52) Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat a podporu informačních služeb, musí být chráněny před poškozením či odposlechem.

53) Kabely i zařízení centrálních komponent systémů ICT musí být zřetelně označeny a musí být udržován seznam propojení.

54) U kritických systémů ICT musí být zvážena další opatření:

a) instalace pancéřového potrubí a zamčených místností nebo skříní;

b) použití alternativního směrování nebo alternativních přenosových cest poskytujících přiměřenou bezpečnost;

c) použití optických kabelů;

d) použití stínění kabelů na ochranu před elektromagnetickým vyzařováním.

55) Aktivní prvky zajišťující komunikaci mezi centrálními komponentami systému ICT a koncovými zařízeními musí být umístěny v prostorách pod kontrolou justičních složek.

4.2.3 Údržba zařízení

Organizační zásady:

56) Komponenty systému ICT(zařízení) musí být v intervalech předepsaných výrobcem/dodavatelem kontrolovány pro zajištění jejich stálé dostupnosti a integrity (prováděna profylaxe).

a) Zařízení musí být udržována a provozována v souladu s doporučeními dodavatele;

b) Opravy a servis zařízení smí provádět pouze oprávněné osoby;

c) O všech závadách nebo podezřelých chybách, o preventivních prohlídkách a opravách musí být pořízeny záznamy;

d) V případech, kdy je údržba prováděna bez dohledu oprávněné osoby, musí být ze zařízení odstraněny veškeré informace.

4.2.4 Bezpečnost zařízení mimo prostory justiční složky

Organizační zásady:

57) Před přemístěním zařízení mimo chráněné prostory musí z něho být odstraněny všechny informace (např. vyjmutím veškerých nosičů informací nebo jejich bezpečným výmazem). V opačném případě musí být zařízení pod neustálým dohledem odpovědného pracovníka justiční složky nebo jiné oprávněné smluvní strany.

58) Použití prostředků pro zpracování informací mimo budovy justiční složky, bez ohledu na jejich vlastníka, podléhá schválení odpovědnou osobou.

59) Zařízení používané mimo prostory justiční složky musí být zabezpečeno s přihlédnutím k různým rizikům, která vyplývají z jejich použití mimo justiční složku.

a) Zařízení ICT a nosiče informací, při cestách mimo justiční složku, nesmí být ponechána bez dozoru(zejména nesmí být ponechána bez dozoru v dopravním prostředku, v autě, ve veřejných prostorách, v konferenčních centrech nebo zasedacích místnostech apod.). Mobilní výpočetní zařízení a sdělovací technika (viz 6.7) musí být přepravována jako příruční zavazadla a v rámci možností ukrývána. V případě, kdy uživatel musí nechat mobilní výpočetní zařízení bez dozoru, musí jej ponechat v uzamčených prostorách nebo úložných schránkách s dostatečně omezeným přístupem (z toho je vyjmut automobil, ve kterém nesmí být zařízení ponecháno bez dozoru);

b) Musí být dodržovány pokyny výrobce týkající se ochrany zařízení, například zajištění ochrany proti působení silného magnetického pole;

c) Pro práci doma musí být určena vhodná opatření na základě hodnocení rizik.

4.2.5 Bezpečné zničení nebo opakované použití zařízení

Organizační zásady:

60) Všechna zařízení obsahující paměťová média (počítače, velkokapacitní tiskárny, multifunkční zařízení apod.) musí být před jejich zničením nebo opakovaným použitím zkontrolována a musí být zajištěno, že data a licencované programové vybavení jsou odstraněny nebo bezpečně vymazány nebo zničeny (viz 5.7.2).

4.2.6 Přemístění majetku

Organizační zásady:

61) O přemístění zařízení ICT musí být proveden záznam.Tato zásada se vztahuje

a) na veškerá zařízení umístěná v serverovnách;

b) na výpočetní zařízení koncových uživatelů, která nejsou mobilními zařízeními (viz 6.7), a to v případech, kdy by měla být přemístěna mimo prostory justiční složky resp. organizační jednotky.

PŘÍLOHA P III: INSTRUKCE PRO VÝKON SLUŽBY VZTAHUJÍCÍ SE K SERVEROVNĚ

Poplach PZTS na opakovacím panelu ústředny umístěný u stálé služby: Stálá služba okamžitě osobně zkontroluje střežený prostor serverovny. V případě planého poplachu, po kontrole prostoru, opět zastřeží serverovnu svým kódem. V případě narušení prostoru osobou s právem samostatného přístupu do serverovny zjistí důvod poplachu. V případě narušení prostoru osobou bez práva samostatného přístupu do serverovny tuto osobu zadrží do příjezdu Policie ČR, kterou po zadržení osoby vyrozumí. V případě poruchy PZTS okamžitě telefonicky vyrozumí osobu odpovědnou za provoz serverovny o této skutečnosti a do odstranění závady věnuje tomuto prostoru zvýšenou pozornost.

Zjištění hladiny vody v technologické podlaze: Stálá služba okamžitě osobně zkontroluje střežený prostor serverovny s důrazem na objevení případného vnikání vody do serverovny. V případě zjištění zdroje úniku provede provizorní opatření k odstranění, například uzavření hlavního uzávěru vody, uzavření větve ústředního topení, kontrola oken, jestli do místnosti nevniká voda v případě srážek podle plánů budovy. Okamžitě telefonicky vyrozumí osobu odpovědnou za provoz serverovny o této skutečnosti.

Zvýšení teploty nebo vlhkosti nad stanovenou mez: Jedná se o zvýšení teploty na 28 stupňů Celsia, 80% relativní vlhkosti nebo obou hodnot současně. Stálá služba neprodleně zkontroluje situaci v serverovně, funkci klimatizace a případně zdroj vlhkosti, především únik páry nebo horké vody. Provede základní opatření ke snížení hodnot, především otevření oken a dveří, v případě, že je klimatizace nefunkční. V případě poruchy PZTS okamžitě telefonicky vyrozumí osobu odpovědnou za provoz serverovny o této skutečnosti a do odstranění závady věnuje tomuto prostoru zvýšenou pozornost.

Výpadek napájení: Informace o tomto stavu přívodu elektřiny v serverovně není součástí zabezpečovacích systémů. Informaci o výpadku stálá služba odvodí od jiných instalací v budově, například osvětlení, nebo elektrospotřebičů na umístěných na pracovišti. O výpadku okamžitě informuje správce budovy a osobu odpovědnou za provoz serverovny podle plánu vyrozumění.

Stavová hlášení ústředny EPS na opakovacím panelu ústředny umístěného na pracovišti stálé služby:

Porucha:

Stálá služba o poruše okamžitě informuje správce budovy a osobu odpovědnou za provoz serverovny podle plánu vyrozumění a až do odstranění poruchy věnuje zvýšenou pozornost požární situaci v serverovně.

Hašení (Požár):

Způsob vyrozumění o požáru:

Signál na opakovacím panelu ústředny umístěný u stálé služby,

Nahlášení požáru v serverovně třetí osobou z titulu stálé služby jako místní ohlašovny požáru.

Zprozorování požáru stálou službou při obhlídce objektu.

Reakce stálé služby na požár:

Stálá služba okamžitě oznamuje požár na tísňovou linku HZS 150 (Hasičský záchranný sbor), kontroluje okolí serverovny, aby nedošlo k rozšíření požáru, které případně eliminuje ručním hasícím přístrojem. V žádném případě nevstupuje do serverovny v okamžiku hašení ani po něm. O požáru informuje správce budovy a osobu odpovědnou za provoz serverovny podle plánu vyrozumění.