Návrh implementace bezpečnostní politiky v informačním a komunikačním systému veřejné správy

Design implementation security policy in the information and communication system in the public administration

Bc. Josef Sedlačík

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Josef SEDLAČÍK**
Osobní číslo:	**A11330**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Návrh implementace bezpečnostní politiky v informačním a komunikačním systému veřejné správy**

Zásady pro vypracování:

1. **Formou literární rešerše popište současný stav předmětné problematiky a úroveň jeho řešení v informačních zdrojích.**
2. **Proveďte analýzu legislativních požadavků na bezpečnost informačních a komunikačních systémů veřejné správy.**
3. **Vytvořte model informačního a komunikačního systému veřejné správy a popište zásady tvorby bezpečnostní politiky z hlediska komplexního způsobu zabezpečení – systémové, fyzické, personální, atd.**
4. **Analyzujte bezpečnostní rizika pro vnější a vnitřní prostředí a na základě této analýzy navrhněte implementaci bezpečnostní politiky.**
5. **Proveďte zobecnění/ doporučení pro postup při zvládání rizik – implementaci bezpečnostní politiky v objektech veřejné správy.**
6. **Naznačte vývojové trendy v implementaci zásad bezpečnosti informačních a komunikačních systémů ve veřejné správě.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman: Ochrana znalostí a dat v podnikových informačních systémech. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.**
2. **JAŠEK, Roman: Informační a datová bezpečnost. Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.**
3. **MALANÍK, David: Význam fyzického zabezpečení IT systémů. Security Revue září 2010. ISSN 1336-9717.**
4. **Ludvík Miroslav: Teorie bezpečnosti poč. sítí. Computer Media. 98str. ISBN: 80-86686-35-3.**
5. **Thomas, Thomas M. : Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.**
6. **Doseděl, Tomáš: Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno : Computer Press, 2004. ix, 190 s. ISBN 80-251-0106-1.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá problematikou bezpečnostní politiky pro informační a komunikační systémy veřejné správy. Podává přehled o současném stavu daného tématu a soupis legislativních požadavků. Jsou zde popsány zásady a postupy pro tvorbu komplexní bezpečnostní politiky informačního systému veřejné správy, které jsou následně implementovány na modelovém příkladu městského úřadu. Výsledkem praktické části je vytvoření dokumentu bezpečnostní politiky, sloužícího jako součást dokumentace pro atestaci daného informačního systému. Závěrem práce jsou doporučené postupy pro zvládání rizik v dané problematice a pravděpodobný vývoj bezpečnosti informací v oblasti veřejné správy.

Klíčová slova:

informační systém, komunikační systém, veřejná správa, bezpečnostní politika, analýza rizik, organizační řízení bezpečnosti, systémové řízení bezpečnosti informací

ABSTRACT

This thesis deals with the security policy for information and communication systems of public administration. It gives an overview of the current state of the topic and a list of legislative requirements. There are described principles and procedures for design of comprehensive security policy in public administration information system, which are implemented on model example of the municipality. The result of practical part is document of security policy, serving as part of the documentation for attestation of the information system. Finally there are the best practices for risk management in this area and probable evolution of information security in the public sector.

Keywords:

information system, communication system, public administration, security policy, risk analysis, organizational security management, information security management system

Rád bych poděkoval svému vedoucímu doc. Ing. Jiřímu Gajdošíkovi, CSc. za odborné vedení, rady a připomínky, které mi poskytoval během tvorby mé práce.

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 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 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 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

OBSAH

ÚVOD

Informační systémy jsou v dnešní době nedílnou součástí každé organizace. Díky těmto systémům je způsob zpracování, uchování informací organizací mnohem snazší a jejich využití mnohem efektivnější. Výjimkou nejsou ani státy a státní instituce. Ba naopak. Státy a jejich vlády jsou jedním z hlavních a největších uživatelů informačních a komunikačních technologií.

S nástupem těchto technologií se začala objevovat i myšlenka jejich bezpečnosti. V dnešní době má každá organizace ve svém systému uložena svá aktiva, která jsou mnohdy tvořena citlivými informacemi, které nesmí být vyzrazeny. V případě státu se jedná o citlivé informace o nás všech, a proto musí každý systém mít určenu svou bezpečnostní politiku.

Cílem diplomové práce je navrhnout způsoby implementování bezpečnostní politiky pro informační a komunikační systémy veřejné správy. Práce je rozdělena na teoretickou a praktickou část.

V teoretické části je vysvětleno, jakým subjektem veřejná správa je a čím je tvořena. Následně je základně rozebrána teorie systému a informačních systémů. Další kapitola je věnována současnému stavu informačních a komunikačních systémů veřejné správy, které jsou součástí e-Governmentu. Zároveň jsou určeny legislativní požadavky, včetně požadovaných dokumentů na dané systémy a způsoby jejich provedení. Poté si určíme, co to je bezpečnost informačních systémů a způsoby jejich provedení. Důležitou součástí práce je bezpečnostní politika informačních systému veřejné správy a obecné postupy pro jejich provádění.

Praktická část je postavena na fiktivním modelu informačního systému v prostředí městského úřadu. Na tento model vytvoříme bezpečnostní politiku tak, aby bylo možné ji využít při žádosti o atestaci systému a tím by byla vhodná pro případný reálný systém. Následně určíme procesy pro systémové řízení rizik v informačních a komunikačních systémech veřejné správy a určíme obecná doporučení. Poslední kapitola se věnuje možnému vývoji systémů veřejné správy a tím pádem i budoucí problematice v otázkách bezpečnosti.

I. TEORETICKÁ ČÁST

1 VEŘEJNÁ SPRÁVA

V dnešní době se setkáváme s mnoha rozdílnými názory na veřejnou správu. Všechny názory vycházejí z obecného významu slova správa. Správu lze rozlišovat jako činnost ve smyslu administrativním, organizačním, plánovacím, kontrolním, řídícím, atd. [1]

V našem případě je velmi důležité rozlišit rozdíl mezi soukromou a veřejnou správou. V soukromé správě je její nositel, kterým je např. soukromá organizace, volný ve svém jednání. Tím myslíme, že určuje své vlastní úkoly a metody k dosažení cílů sama a právní řád vymezuje nositeli pouze rámec jednání. [1]

Ve veřejné správě jsou přímo určeny působnosti a pravomoci jejímu vykonavateli zvlášť. Tím je myšleno, že veřejná správa je povinna vykonávat pouze a jen úkony stanovené v zákonech, vyhláškách a jiných právních předpisech. Na rozdíl od soukromé správy je téměř nemožné změnit základní úkoly. [1]

Nicméně nejdůležitějším rozdílem mezi soukromou a veřejnou správou je monopolní postavení veřejné správy při výkonu veřejných služeb.

Veřejná správa představuje specifický druh společenského řízení. To vše díky své povaze institucionalizované kontroly a regulace. Slouží pro účely organizace, řízení lidí a zdrojů k dosahování cílů, které odrážejí potřeby občanů a dalších subjektů. [2]

Veřejná správa vykonává přijaté právní předpisy, ale její činnost není omezena jen na výkon právních předpisů. Sama může některé právní předpisy vydávat. [2]

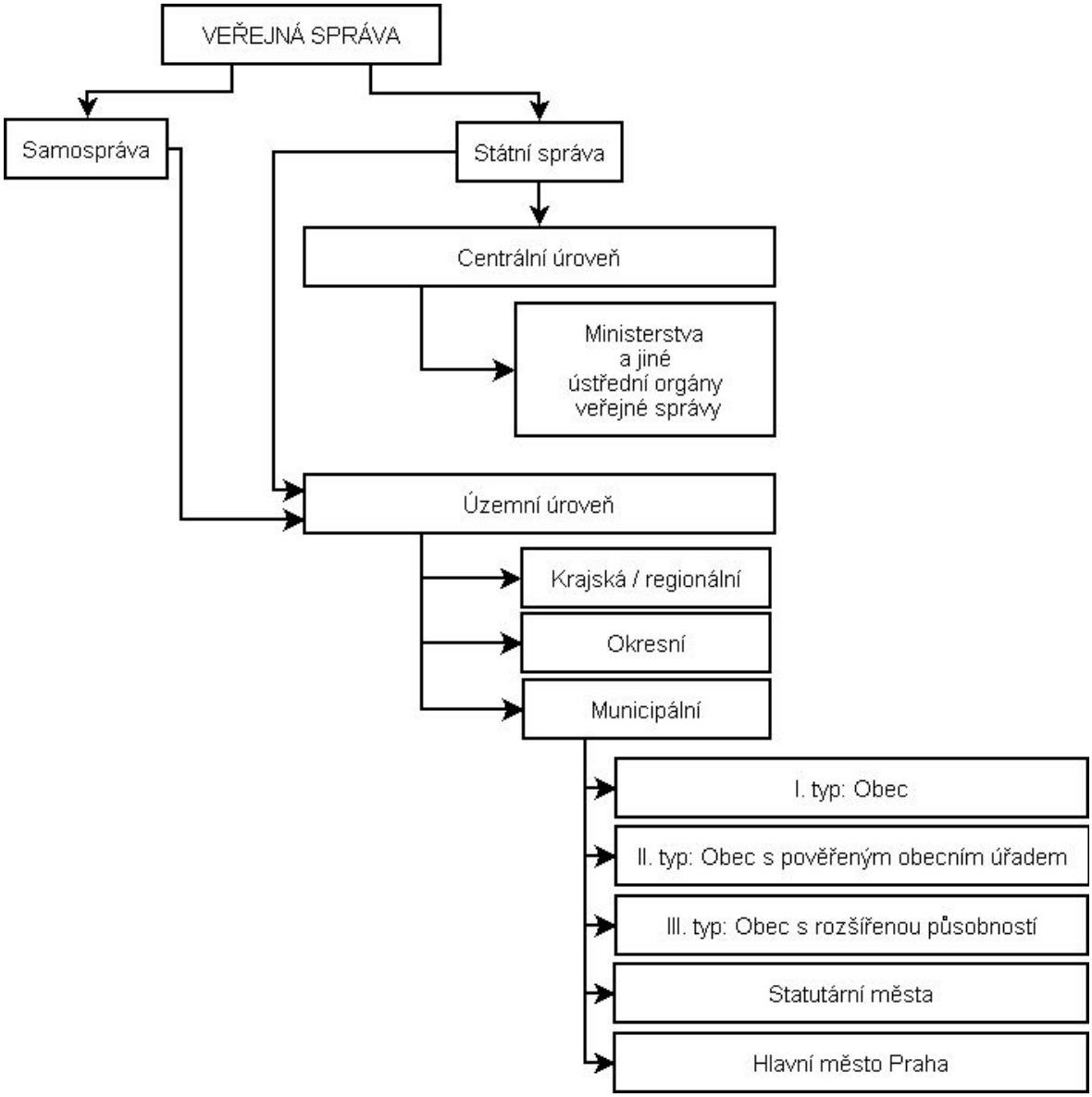
Veřejnou správu můžeme definovat jako soubor činností a úkonů zabezpečovaných na jednotlivých vládních úrovních, za které odpovídá stát a ostatní subjekty veřejné správy, kde jednotlivé úkony slouží k zajišťování veřejných služeb. Jedná se převážně o úkony, které jsou stravovacího, služebního, dozorčího či organizačního charakteru. Zároveň můžeme veřejnou správu popsat jako souhrn institucí, které vykonávají veškeré své úkony přímo nebo zprostředkovaně. [3]

Širší pojetí veřejné správy je představováno mocí zákonodárnou, výkonnou a soudní. V užším pojení se jedná o státní správu a samosprávu, která se dělí na územní a zájmovou. [3]

Funkce veřejné správy je:

- Normativní
    - Je nezastupitelná a souvisí s tvorbou právních norem.
- Ochranná
    - Zajišťuje a organizuje vnitřní a vnější bezpečnost a pořádek státu.
- Ekonomicko – regulační
    - Usměrňuje vývoj ekonomiky.
- Hospodářsko – organizátorská
    - Přerozděluje, tvoří a využívá bohatství ve veřejném sektoru.

Činnost veřejné správy, dle Ústavy a Listiny základních práv a svobod slouží všem občanům a lze ji uplatňovat v mezích stanovených zákonem. Zároveň může činit to, co není zákonem zakázáno a nemůže být nucena činit to, co zákon neukládá.



Obrázek 1 Schéma veřejné správy

2 INFORMAČNÍ SYSTÉM

2.1 Teorie systémů

S rostoucími technickými a ekonomickými požadavky na různé projekty započal výzkum teorie systémů. Tento výzkum se začal zaměřovat na různé vědecké disciplíny, jako jsou filozofie, fyzika a různé technické aplikace, až ke vzniku informatiky, která sdružila veškeré požadavky na systémy. Mezitím vznikaly různé definice systému. [3]

Příkladem jsou definice, že systém je:

- Organizovaná množina myšlenek, principů a zásad seskupených za účelem vysvětlení vnitřního uspořádání nebo činnosti celku
- Soustava zvolených principů pro řešení určitých společenských problémů
- Množina prvků, které se navzájem ovlivňují, za účelem splnit daný cíl
- Pravidelně se ovlivňující nebo vzájemně závislá skupina prvků, které se berou jako celek [3]

Zakladatelem kybernetiky, tím pádem i základního kamene teorie informačních systémů, je americký matematik Norbert Wiener. Jeho myšlenkou bylo, že každý systém využívá zjednodušený model, kde jsou zahrnuty jen důležité části, a předpokládáme, že další části, které v modelu nejsou uvedeny, nejsou nijak schopny ovlivnit systém. [3]

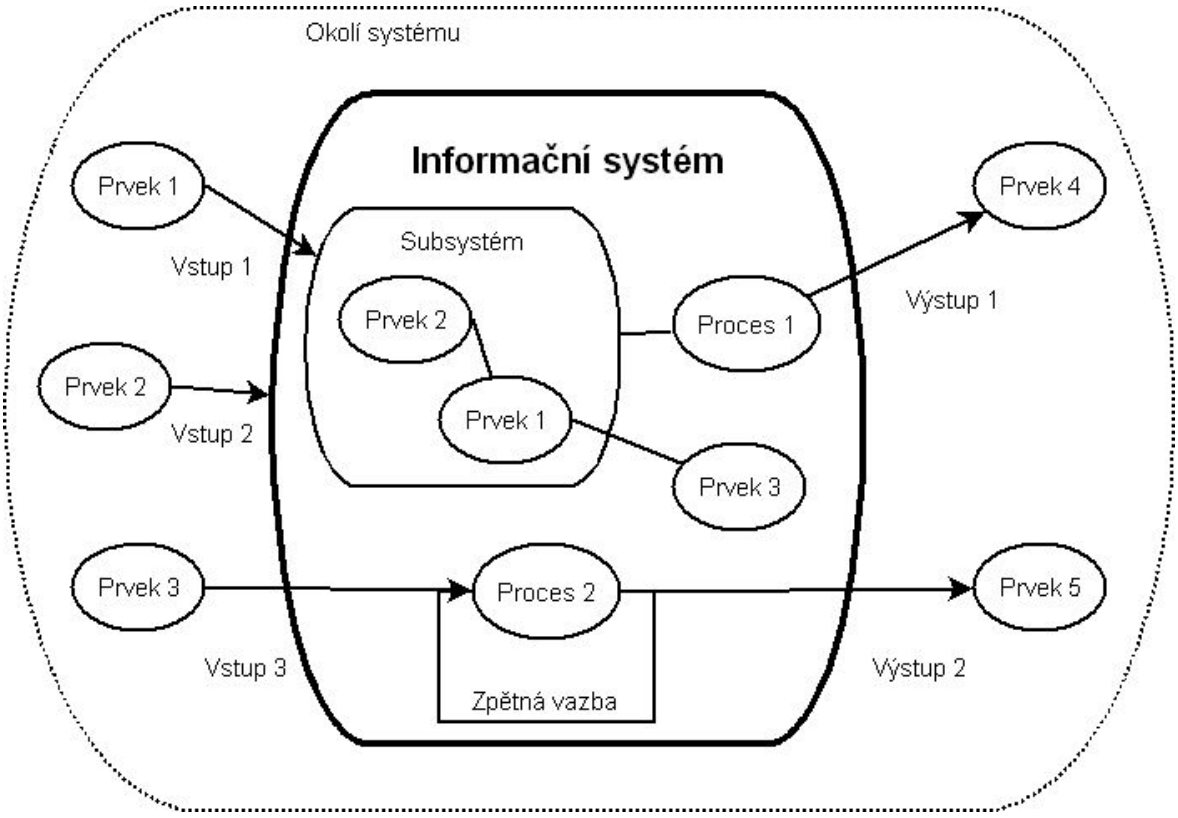
Základní dělení systému podle Wienera:

- Struktura
    - Definice množiny prvků a jejich vazeb mezi sebou a mezi podsystémy.
- Prvky
    - Berou se jako stavební prvek celého systému. Jsou to elementární a nedělitelné části systému.
- Subsystémy
    - Podmnožina prvků systému tvořící samostatný celek, který je závislý na systému

- Separabilita systému
    - Systémové výstupy zpětně neovlivňují vstupy systému.
- Okolí systému
    - Bereme jako prvky, které neleží v systému, ale přes vstupy mohou ovlivnit systém.
- Hranice systému
    - Uzavírá celý systém a odděluje od jiného.
- Vstup systému
    - Množina proměnných, jejichž prostřednictvím se uskutečňuje působení okolí na systém.
- Výstup systému
    - Množina proměnných, jejichž prostřednictvím se uskutečňuje působení systému na okolí.
- Chování
    - Vzniká dynamikou systému. Díky chování je systém schopen vyvolat změnu jeho vlastního stavu.
- Stav systému
    - Souhrn dat a atributů systému v určitém čase či časovém období.
- Stabilita systému
    - Je schopnost systému setrvávat v námi požadovaném a nastaveném stavu. [3]

2.2 Informační systém

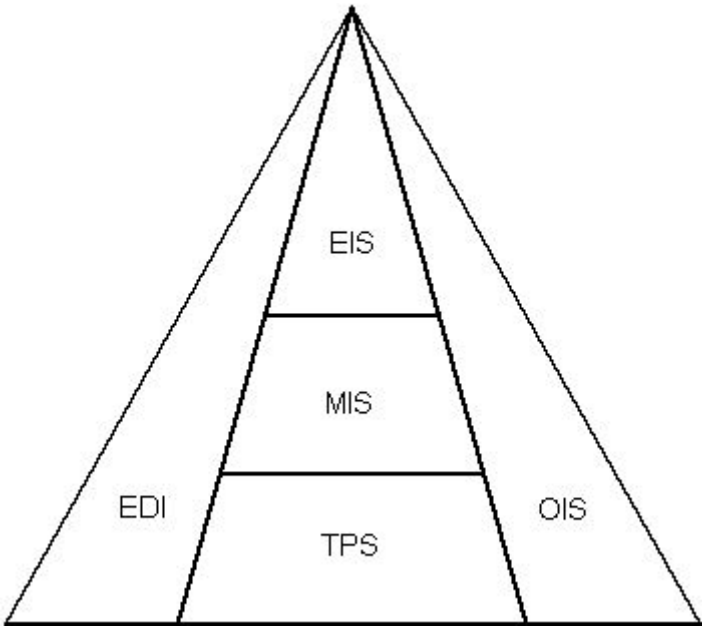
Informační systém (IS) je soubor prvků vzájemně propojených informačními vazbami. Prvky systému netvoří jen informace a informační technologie, ale i lidé, organizační struktura a řízení. Informační systémy se využívají ke sběru, přenosu, zpracování a uchování dat za účelem tvorby a prezentaci informací v něm uložených.



Obrázek 2 Struktura IS [4]

Informační systémy se dnes vyskytují v malých, středních i velkých firmách a společnostech. Výjimkou není ani veřejná správa. Rozsah a velikost informačních systémů se liší. Nicméně jakýkoliv systém je složen z menších IS. V našem případě můžeme využít globální architekturu podnikového IS, kterou můžeme nazvat základním kamenem pro jakýkoliv informační systém, včetně systémů veřejné správy.

Globální architektura podnikového IS:



Obrázek 3 Globální architektura podnikového IS

- TPS (Transaction Procesing System) Operativní řízení podniku
  - Slouží k pořizování, aktualizaci, evidenci a přehledu dat
- MIS (Management Information System) Taktické řízení podniku
  - Navazuje na TPS. Jedná se o analýzu a zpracování dat.
- EIS (Executive Information System) Strategické řízení podniku
  - Slouží pro podporu vrcholového vedení. Sleduje veškerá data a vytváří komplexní analýzy současného stavu a vývoje.
- OIS (Office Information System) Kancelářské systémy
  - Sada aplikací zaměřených na podporu kancelářských prací.
- EDI (Electronic Data Interchange) Komunikace s okolím
  - Aplikace zaměřené na podporu komunikace s dodavateli, odběrateli, zákazníky, bankami, atd. [5]

Na globální architekturu následně navazují dílčí architektury. Ty prohlubují návrh systému do větších detailů.

Dílčí architektury dělíme:

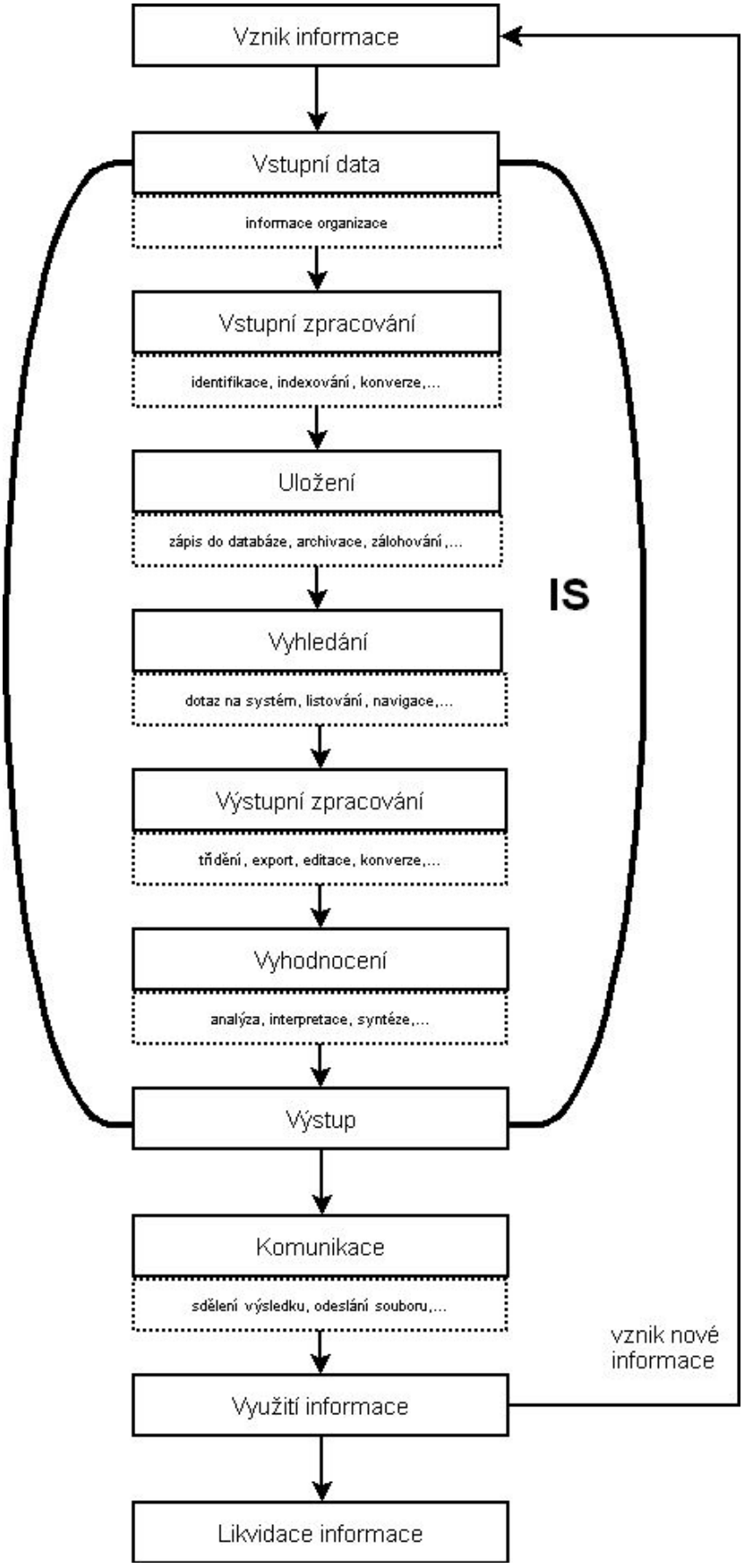
- Procesní architektura
    - Popis klíčových procesů interakce podniku s okolím
- Funkční architektura
    - Rozklad základních funkcí na dílčí celky
- Datová architektura
    - Definování entit, jejich atributů a vazeb
- SW architektura
    - Specifikace SW komponent systému
- HW architektura
    - Technické vybavení systému
- Technologická architektura
    - Propojení datové, SW a HW architektury a definuje způsob zpracování dat.

Význam informačního systému:

- Automatizace rutinních činností
- Zefektivnění komunikace
- Monitorovací funkce
- Zaznamenání znalostí a zkušeností (know-how)
- Podpora při rozhodování
- Modelování reality
- Analýza stavů
- Podpora rozvoje organizace

- Podpora vzdělanosti
- Atd. [6]

Význam informačního systému může být pro každou organizaci rozdílný, ale pro všechny organizace platí pravidlo, že informační systém vždy musí vést ke zvýšení produktivity. [6]



Obrázek 4 Cyklus informace v IS

3 INFORMAČNÍ A KOMUNIKAČNÍ SYSTÉM VEŘEJNÉ SPRÁVY

Informační systémy jsou nedílnou součástí moderní společnosti, tím pádem i nedílnou součástí orgánu státní a veřejné správy. Lze si je představit jako soubor databází sdružujících informace v systematizované formě, důležitých pro výkon veřejné správy. Tyto informace jsou nadále tříděny, doplňovány, zpracovávány a vyhodnocovány.

Kategorie základních informačních systémů VS:

- EIS - Executive Information System
    - Tento systém má za úkol poskytovat z obrovského množství informací pouze klíčové, které jsou určeny pro vedoucí pracovníky.
- DSS - Decision Support System
    - Slouží jako nástroj pro podporu manažerského rozhodování. Tato aplikace porovnává současná a minulá data, tím pádem můžeme získat statistické předpovědi vývoje.
- MIS – Management Information System
    - Jedná se o informační systém, který zpracovává a třídí obrovské množství dat. Dále zajišťuje přístup všech pracovníků přesně k těm informacím, které ke své práci potřebují.
- Operativní IS
    - Informační systém, který zajišťuje a zprostředkovává rutinní procesy. Ve většině případů jsou na něj napojeny i další podsystémy.
- KMS – Knowledge Management System
    - Systém, který zabezpečuje sběr, třídění, šíření a analýzu znalostí a dovedností jednotlivých pracovníků.
- OIS – Office Information System
    - Systém zajišťující běžnou kancelářskou práci zaměstnanců. [7]

Vznik informačních systémů veřejné správy

Již v devadesátých letech začaly vznikat jednotlivé IS. Tyto systémy si vytvářeli orgány VS nezávisle na sobě, proto se nemohly považovat jako jeden fungující celek. V červenci 2002 Parlament ČR schválil zákon 365/2000 Sb., o informačních systémech veřejné správy. Toto byl první krok ke vzniku jednotného informačního systému. [8]

Vznik komunikační infrastruktury veřejné správy

Jak již bylo zmíněno, IS již fungovali dříve, pouze byly samostatné a nebyly nijak propojené. Proto vznikla myšlenka vytvořit jeden velký systém, nicméně náročnost vytvoření a implementování byla téměř nemožná. Proto vyhrál návrh ponechat stávající systémy a pouze je upravit, aby byly spolu kompatibilní a mohly mezi sebou spolupracovat. Tímto krokem se začala budovat Komunikační infrastruktura veřejné správy (KIVS). [9]

3.1 e-Government

Vlády jsou jedním z hlavních a největších uživatelů informačních a komunikačních technologií. Na počátku používaly jednotlivé státy informační technologie jen na úrovni vytvoření webových stránek a využívání e-mailové komunikace. Nicméně díky organizaci OECD (The Organisation for Economic Cooperation and Development), jejíž součástí je i Česká republika, vznikl mezinárodní projekt e-Government, který pomáhá státům využívat informační systémy pro jednotlivé úkony, jako je například shromažďování dat za účelem statistik a další vnitrostátní úkony. [10]

Existují mnohé definice popisující e-government, ale nemůžeme vytvořit jednu jedinou, protože každá vláda má vlastní priority pro tento systém. To dalo vzniku tří základních definic, které popisují e-government. [10]

- E-government je definován jako internetové poskytování služeb a dalších aktivit založených na bázi internetu jako e-konzultant.

- E-government je přirovnáván využívání informačních a komunikačních technologií, kde je kladen důraz na poskytování služeb a procesů, které zahrnují různé činnosti vlády.
- E-government je definován jako schopnost vykonávat veřejnou správu pomocí informačních a komunikačních systémů, nebo dokonce vytvořit novou formu vládnutí pomocí IKS, kdy celý výkon je spojen s využíváním internetu.

Nicméně OECD vytvořilo svou vlastní definici, která výstižně popisuje e-government.

- Využívání komunikačních a informačních technologií a zejména internetu jako nástroj pro dosažení lepší vlády. [10]

3.2 EGON

Jedná se o projekt elektronizace veřejné správy, který se začal vytvářet v roce 2006. Jeho hlavním cílem je usnadnění života občanů a výkonu veřejné správy pomocí informačních technologií. Pro správnou realizaci bylo nutné vytvořit legislativní úpravy, díky kterým se mohl začít celý projekt eGON realizovat. Jeho součástí byl i projekt Czech POINT, který se začal rozvíjet v roce 2008. Téhož roku byl přijat zákon č.300/2008 Sb., o autorizované konverzi dokumentů, který stanovuje normu pro zavedení datových schránek. V roce 2009 vznikla Komunikační infrastruktura veřejné správy (KIVS) a do plného provozu byly uvedeny i datové schránky. Nakonec byl do plného provozu spuštěn i systém základních registrů, čímž byl celý projekt eGON plně zrealizován. [11]

Obrázek 5

Struktura eGON [11]

Systém eGON se přezdívá jako „živý organismus“, kdy jednotlivé jeho části tvoří jeden velký živý systém. Jednotlivé součásti se dělí na:

- Prsty – **Czech point**
  - Soustava kontaktních míst
- Oběhová soustava – **Komunikační infrastruktura veřejné správy (KIVS)**
  - Systém sloužící pro bezpečný přenos dat
- Srdce – **Zákon č.300/2008 Sb., o autorizované konverzi dokumentů**
  - Přezdívaný taky jako zákon o eGovernmentu
- Mozek – **Základní registry veřejné správy**
  - Bezpečné a aktuální databáze dat o občanech, státních a nestátních subjektech [11]

3.2.1 Komunikační infrastruktura veřejné správy (KIVS)

KIVS můžeme popsat jako jednotný systém technické, síťové, aplikační, bezpečnostní a organizační struktury pro hlasovou a datovou komunikaci. Tento systém je určen pro všechny orgány VS, ale i pro nestátní subjekty.

Jedná se o sloučení jednotlivých komunikačních linek veřejné správy v jednu datovou síť. Byla vytvořena za účelem zefektivnění služeb, úspory, ale hlavně bezpečnosti a sdružení přenášených informací, a tím zlepšení jejich dostupnosti. [12]

KIVS je využíván jako rozhranní ISZR a zajišťuje:

- Důvěryhodnost dat
    - Přenášená data jsou chráněna před zneužitím
- Dostupnost služeb
    - Spolehlivost služeb vyjádřená procentuálně

3.2.2 Základní registry veřejné správy

Základní myšlenkou je vytvoření jednotných registrů za účelem odstranění zbytečné byrokracie, nejednotnosti, multiplicity a neaktuálnosti databází o občanech a státních i nestátních subjektech.

Jedná se o registry:

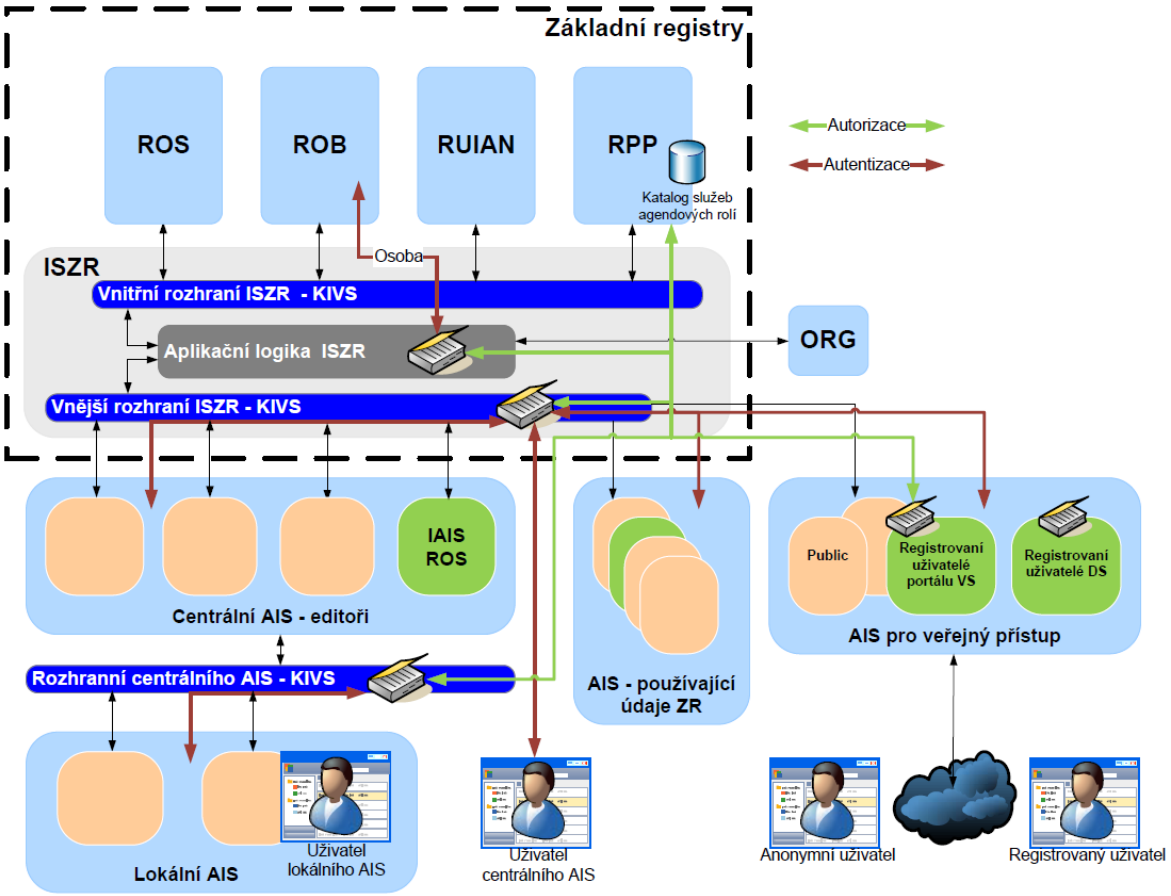
- Základní registr obyvatel
- Základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci,
- Základní registr územní identifikace, adres a nemovitostí
- Základní registr agend orgánů veřejné moci a některých práv a povinností

Jsou platformou pro bezpečné sdílení dat v rámci celé veřejné správy ČR. Je definována zákonem č. 111/2009 Sb., o základních registrech a zákonem č. 227/2009 Sb., o správě základních registrů.

Ty to registry slouží jako orgány veřejné moci, které již nemusí získávat referenční údaje z různých zdrojů. Tím slouží i občanům, kteří již nemusí údaje opakovaně dokládat, ale jsou pouze jen jednou sděleny a pak uloženy do základního registru, kde je nadále mohou využívat další agendové systémy, resp. informační systémy veřejné správy. [13]

Základní registry obsahují právně závazné a platné referenční údaje. Proto jsou jednotlivé agendové systémy povinny přizpůsobit své údaje tak, aby mohly být začleněny do systému.

Architektura základních registrů:



Obrázek 6 Logická architektura Základních registrů [13]

- ROS
    - Základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci
- ROB
    - Základní registr obyvatel
- RUIAN
    - Základní registr územní identifikace, adres a nemovitostí
- RPP
    - Základní registr agend orgánů veřejné moci a některých práv a povinností
- ORG
    - Specifický informační systém základních registrů, který zajišťuje ochranu osobních referenčních údajů uložených v systému základních registrů
- ISZR
    - informační systém základních registrů, je definován jako referenční rozhraní pro přístup k základním registrům
- Vnitřní rozhraní ISZR
    - Rozhraní sloužící k bezpečné komunikaci mezi jednotlivými komponentami systému a je nedostupné mimo systém
- Aplikační logika ISZR
    - Slouží pro výkon ISZR; udržuje sadu povolených služeb; zajišťuje frontu zpráv; zprostředkovává AIFO pro jednotlivé agendy prostřednictvím ORG
- Vnější rozhraní ISZR
    - Zajišťuje publikaci služeb; primárně řídí vstupní a výstupní fronty; předává požadavky aplikační logice ISZR
- Centrální AIS (editoři)
    - Provádí editační služby referenčních údajů
- AIS

  - Agendový informační systém

- Lokální AIS
  - Poskytují prostředí pro uživatele editorů
- Ostatní AIS
  - Využívají služeb systému základních registrů pro čtení referenčních údajů
- AIS pro veřejný přístup
  - Využívají omezených služeb systému [13]

Bezpečnost referenčních údajů v základních registrech

Bezpečnost informací je důležitá v každém systému. Výjimkou není ani systém základních registrů, ba naopak. Z důvodu uložení informací o jak fyzických, tak právnických osobách musí být systém o to víc zabezpečen.

Proto jsou veškeré informace, odesílané či přijaté systémem, označeny identifikátory. Tyto identifikátory dělíme na:

- Zdrojový identifikátor fyzické osoby (ZIFO)
- Agendový identifikátor fyzické osoby (AIFO)

Identifikátory jsou neveřejné, slouží pouze interní využití ve veřejné správě a generuje je Úřad pro ochranu osobních údajů.

ZIFO je veden pouze v evidenci zdrojových identifikátorů fyzických osob v systému základního registru. Orgány státní správy mají pro identifikaci přidělené AIFO, které je jen v rámci dané agendy.

AIFO je odvozeno z kódu agendy a ze ZIFO, kde nelze zpětně získat ZIFO dané osoby. Každá osoba je v agendách vedena pod jiným identifikátorem AIFO. Tím pádem zabezpečíme zneužití osobních údajů úředníky či jinými osobami.

Zároveň se v ISZR provádí identifikace, autentizace a autorizace uživatelů, kteří žádají systém o informace a jejich oprávnění jsou kontrolována Registrem práv a povinností.

Všechny žádosti jsou kontrolovány systémem Základních registrů a jsou uchovávány záznamy o událostech spojení. [13]

3.3 Legislativní požadavky na ISVS

Legislativní požadavky na tvorbu a správu informačních a komunikačních systémů veřejné správy jsou zakotveny v následujících právních dokumentech:

- **Zákon č. 365/2000 Sb.**, o informačních systémech veřejné správy
- **Zákon č. 81/2006 Sb.**, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a další související zákony
- **Zákon č. 18/2012 Sb.**, kterým se mění některé zákony v souvislosti s přijetím zákona o Celní správě České republiky (novela zákona č. 365/2000 Sb.)
- **Vyhláška č. 528/2006 Sb.**, o informačním systému o ISVS
- **Vyhláška č. 529/2006 Sb.**, o dlouhodobém řízení ISVS
- **Vyhláška č. 530/2006 Sb.**, o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS
- **Vyhláška č. 469/2006 Sb.**, o informačním systému o datových prvcích
- **Vyhláška č. 52/2007 Sb.**, o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní
- **Vyhláška č. 53/2007 Sb.**, o referenčním rozhraní

Další právní dokumenty upravující tvoru a správu ISVS:

- **Zákon č. 106/1999 Sb.**, o svobodném přístupu k informacím
- **Vyhláška č. 442/2006 Sb.**, kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup

- **Vyhláška č. 64/2008 Sb.**, o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)
- **Zákon č. 101/2000 Sb.**, o ochraně osobních údajů
- **Zákon č. 227/2000 Sb.**, o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- **Zákon č. 499/2004 Sb.**, o archivnictví a spisové službě a o změně některých zákonů
- **Nařízení vlády č. 495/2004 Sb.**, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- **Vyhláška č. 496/2004 Sb.**, o elektronických podatelnách
- **Vyhláška č. 193/2009 Sb.**, o stanovení podrobností provádění autorizované konverzi dokumentů
- **Zákon č. 300/2008 Sb.**, o elektronických úkonech a autorizované konverzi dokumentů
- **Vyhláška č. 194/2009 Sb.**, o stanovení podrobností užívání informačního systému datových schránek
- **Metodický pokyn** řízení kvality informačních systémů veřejné správy

3.3.1 Novela zákona č. 365/2000 Sb.

Zákon o informačních systémech veřejné správy určuje práva a povinnosti pro vytváření, užívání a správu ISVS. Zákon byl novelizován zákonem č. 81/2006 Sb. a zákonem č. 18/2012 Sb. Zákon stanovuje postupy pro rozvoj ISVS tak, aby byly kvalitním nástrojem pro výkon veřejné správy. [14]

Nadále upravuje provoz Portálu veřejné správy, výstupy z ISVS, pravidla pro akreditaci a pověřování atestačních středisek k provádění atestací, základní pravidla udělování atestů a fungování atestačních středisek. [15]

K zákonu č. 365/2000 Sb. a jeho novelám byl Ministerstvem vnitra vydán metodický pokyn, který slouží jako pomůcka pro naplnění povinností vyplívající z tohoto zákona. Materiál slouží ministerstvům a jiným správním úřadům. Zejména správcům informačních systémů veřejné správy.

Zákon č. 81/2006 Sb. podstatně upravuje a doplňuje znění zákona č. 365/2000 Sb.

Zákon č. 18/2012 Sb. nepřináší zásadní změny týkající se ISVS, spíše jen doplňuje informace pro orgány celní správy.

3.3.2 Vyhláška č. 528/2006 Sb.

Vyhláška stanovuje povinnost správcům ISVS podávat informace o provozu ISVS do informačního systému o ISVS. Dále vyhláška obsahuje informace o dostupnosti a obsahu zpřístupněných informačních systémů.

3.3.3 Vyhláška č. 529/2006 Sb.

V této vyhlášce jsou stanoveny požadavky na strukturu, obsah informační koncepce a provozní dokumentaci ISVS.

3.3.4 Vyhláška č. 530/2006 Sb.

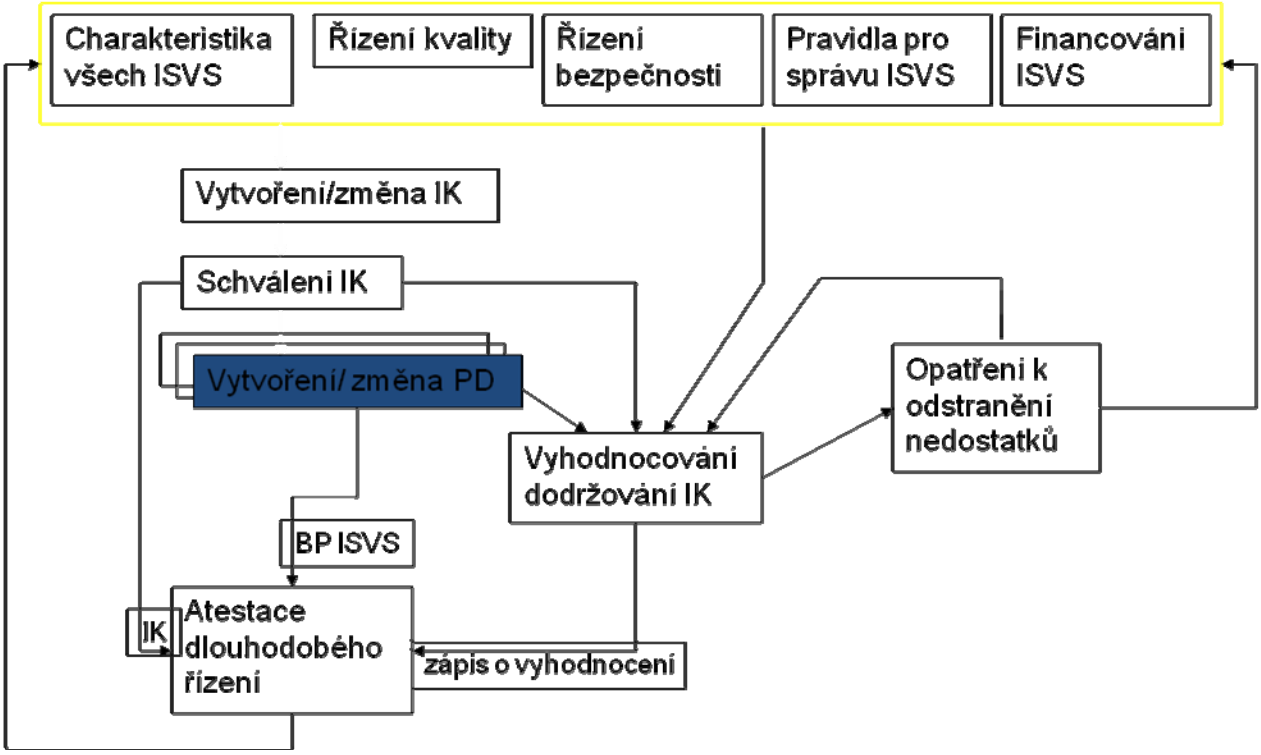
Vyhláška upravuje postupy atestačních středisek pro posuzování dlouhodobého řízení ISVS, kde je stanovený kompletní atestační postup i s jeho výsledky, kterým jsou atestační střediska povinna se řídit.

3.4 Informační koncepce

Jedná se o dokument, který je vydaný ke každému ISVS, dle vyhlášky č. 529/2006 Sb. Jsou zde uvedeny dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaného ISVS, včetně předpokládaných změn v systému. Dále principy pořizování, vytváření a

provozování ISVS. Informační koncepce obsahuje charakteristiku systému, která je spravovaná daným orgánem veřejné správy. [16]

Informační koncepce je vytvářena pro celý orgán veřejné správy, nikoliv pro jednotlivé ISVS. Proto se doporučuje, aby v informační koncepci byly uvedeny všechny IS, tzn. ISVS i provozní IS. [16]



Obrázek 7 Proces dlouhodobého řízení ISVS [17]

Informační koncepce by měla obsahovat tyto systémy:

- ISVS, které daný orgán spravuje
- ISVS, u kterých je daný orgán provozovatelem, případně uživatelem (není povinností)
- Provozní IS, který daný orgán spravuje (není povinností)
- Provozní IS, u kterých je daný orgán provozovatelem (není povinností)
- Kombinované IS, kde subsystém kombinovaného systému je ISVS
- Subsystémy kombinovaného IS, kde tento systém je provozním IS

Provozní IS, dle novely zákona 365/2000 Sb., jsou systémy zajišťující informační činnosti nutné pro provoz daného orgánu. (např. účetnictví, IS o rozhodnutích o přidělení nebo odnětí dotací)

Ke každému ISVS musí daný orgán veřejné správy vést provozní dokumentaci.

3.5 Provozní dokumentace

Provozní dokumentace je vždy zpracována dle zásad a postupů uvedených v informační koncepci. V tomto dokumentu uvádí orgán VS aktuální stav ISVS. Jsou zde popsány funkční a technické vlastnosti každého ISVS, jenž je pro daný orgán správcem. Dále jsou zde uvedena technická opatření pro zachování vlastností celého ISVS. [18]

Provozní dokumentaci tvoří:

- Bezpečnostní dokumentace ISVS
    - Bezpečnostní politika ISVS
        - Je součástí dokumentu pouze tehdy, pokud systém má vazby na ISVS jiného správce, nebo orgán VS není správcem tohoto systému.
    - Bezpečnostní směrnice pro činnost bezpečnostního správce systému
        - Zde jsou podrobně popsány bezpečnostní funkce, které využívá správce systému, včetně návodu na tyto funkce
- Systémová příručka
    - Obsahuje popis všech funkcí, které využívá správce pro provádění činností v ISVS, podrobný popis ISVS nebo odkaz na dokument o ISVS a definování skupin uživatelů či jednotlivých uživatelů a jejich oprávnění a povinnosti při užívání ISVS. [18]
- Uživatelská příručka
    - Obsahuje popis všech funkcí, které využívá uživatel pro provádění činností v ISVS a vymezení oprávnění a povinností uživatelů daného ISVS. [18]

3.6 Referenční rozhraní

Jedná se o soustavu právních, organizačních, technických a dalších opatření, která vytvářejí jednotné integrační prostředí pro všechny ISVS. Toto integrační prostředí (referenční rozhraní) umožňuje komunikaci a vazby jednotlivých systémů mezi sebou a zároveň jejich vzájemnou kompatibilitu. [19]

Přes referenční rozhraní dochází k bezpečné výměně oprávněných informací jak mezi ISVS, tak i mezi ISVS a dalšími subjekty. [19]

Správcem referenčního rozhraní je podle zákona č. 365/2000 Sb. Ministerstvo vnitra, které zároveň stanovuje technické a funkční náležitosti uskutečňovaných vazeb mezi IS. Všechny tyto náležitosti musí být dle zákona dokládány atestem. [19]

Dle vyhlášky č. 469/2000 Sb. o datových prvcích, všechny orgány VS, které uskutečňují vazby pomocí referenčního rozhraní, musí zajistit zápis nebo změnu a vyhlášení datových prvků, které hodlají používat v souladu s touto vyhláškou. Zároveň musí přizpůsobit ISVS vyhlášeným datovým prvkům. [19]

Dále musí být každé uskutečňování vazeb mezi ISVS prostřednictvím ISVS dle vyhlášky č. 53/2007 Sb., zaznamenáno a uloženo do systému. Záznam musí obsahovat informace o žádajícím IS, čas a záznam o poskytnutí či neposkytnutí vyžadované informace nebo služby. [19]

3.7 Atestace

Ministerstva, orgány VS, ale i dodavatelé a provozovatelé IS jsou povinni, dle novely zákona č. 365/2000 Sb., dodržovat určitá pravidla a povinnosti při vytváření, užívání a provozování ISVS. Tyto atesty jsou prováděny atestačními středisky pověřenými Ministerstvem vnitra ČR. Dodržování těchto pravidel je prokazováno Atestem dlouhodobého řízení ISVS a Atestem referenčního rozhraní ISVS. [20]

ATS dlouhodobého zařízení ISVS

Na základě této atestace je stanovena shoda dlouhodobého zařízení ISVS s požadavky novely zákona č. 365/2000 Sb., vyhlášky č. 529/2006 Sb. a vyhlášky č. 530/2006 Sb. Následně je vydán certifikát příslušnému orgánu na dobu až 5 let.

Při ATS dlouhodobého zařízení ISVS se posuzují následující faktory:

- Úplnost informační koncepce
- Úplnost provozní dokumentace
- Srozumitelnost, přehlednost a logická konzistence IK a PD
- Kvalita konkrétního řešení
- Vyhodnocování dodržování IK
- Příjímání opatření k odstranění nedostatků [18]

ATS referenčního rozhraní ISVS

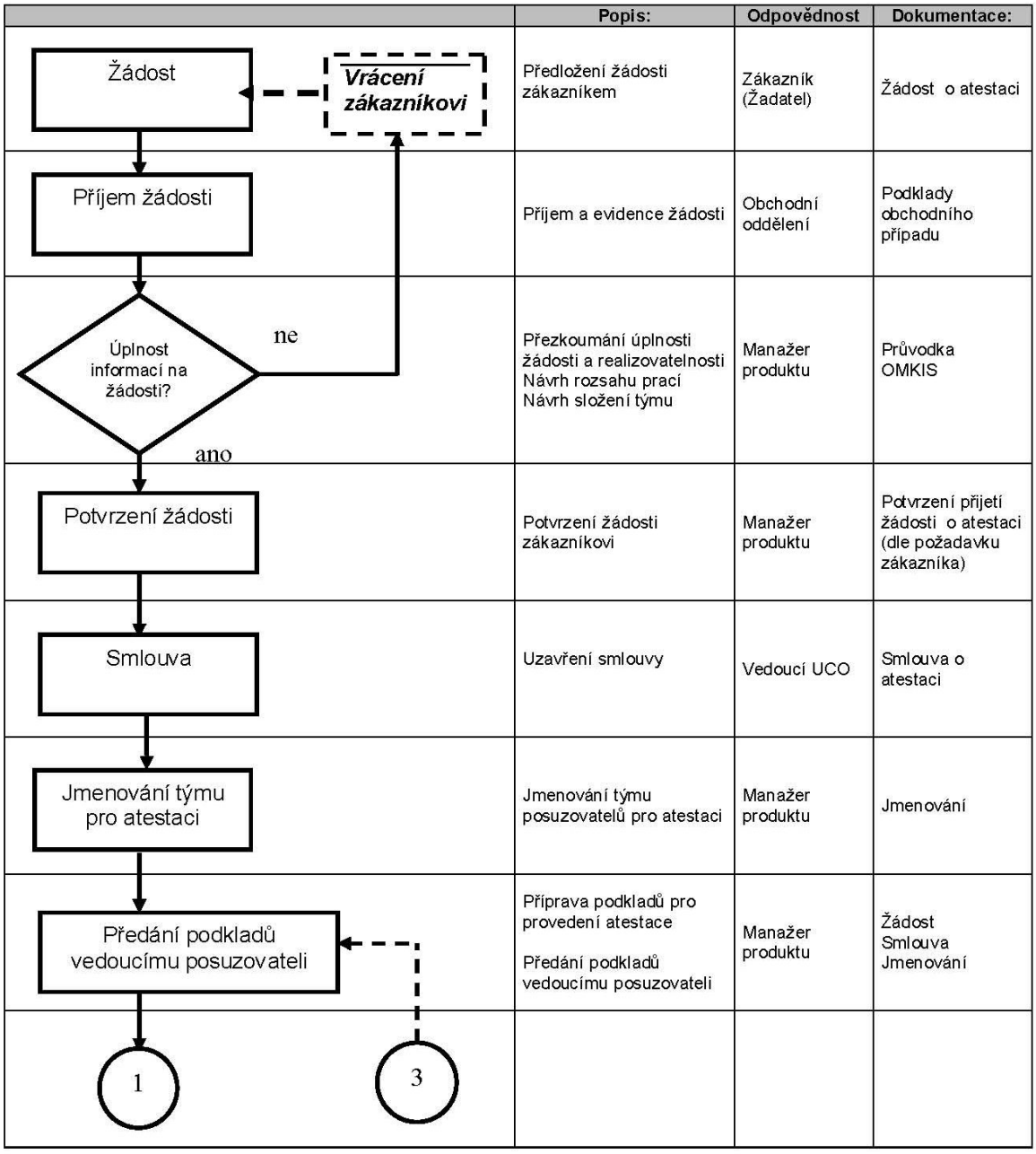
- Na základě této atestace je stanovena shoda způsobilosti k realizaci vazeb ISVS s jinými IS prostřednictvím referenčního rozhraní s vyhlášky č. 53/2007 Sb. a vyhlášky č. 52/2007 Sb. Následně je vydán certifikát příslušnému orgánu na dobu až 5 let. [21]

Při ATS referenčního rozhraní ISVS se posuzují následující faktory:

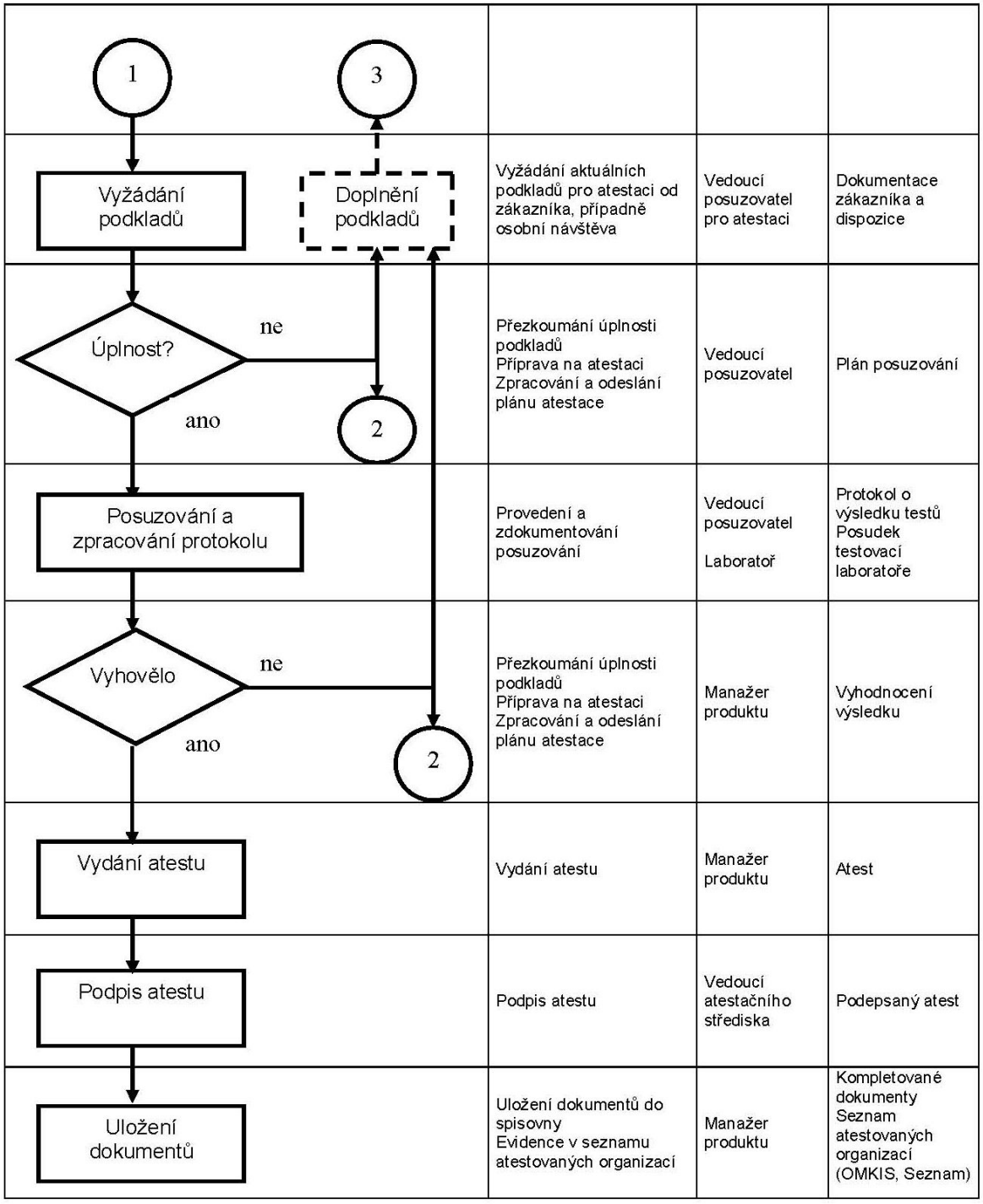
- Údaje o dostupnosti ISVS do IS o ISVS
- Soulad realizace vazby s popisem funkční služby
- Soulad s dokumentací služby
- Zajištění bezpečnosti poskytované služby a rozsah přístupových oprávnění
- Soulad datových prvků při realizaci vazby [21]

ATS – obecný postup

Postup atestace je složitý postup, při kterém je potřeba mnoho dokumentů. Celý postup včetně potřebných dokumentů je uveden v následujícím schématu.



Obrázek 8 Obecné schéma postupu atestace část 1 [22]



	Vyžádání aktuálních podkladů pro atestaci od zákazníka, případně osobní návštěva	Vedoucí posuzovatel pro atestaci	Dokumentace zákazníka a dispozice
	Přezkoumání úplnosti podkladů Příprava na atestaci Zpracování a odeslání plánu atestace	Vedoucí posuzovatel	Plán posuzování
	Provedení a zdokumentování posuzování	Vedoucí posuzovatel Laboratoř	Protokol o výsledku testů Posudek testovací laboratoře
	Přezkoumání úplnosti podkladů Příprava na atestaci Zpracování a odeslání plánu atestace	Manažer produktu	Vyhodnocení výsledku
	Vydání atestu	Manažer produktu	Atest
	Podpis atestu	Vedoucí atestačního střediska	Podepsaný atest
	Uložení dokumentů do spisovny Evidence v seznamu atestovaných organizací	Manažer produktu	Kompletované dokumenty Seznam atestovaných organizací (OMKIS, Seznam)

Pozn.: 2 Odmítnutí vydání atestu

Obrázek 9 Obecné schéma postupu atestace část 2 [22]

4 OBECNÁ BEZPEČNOST IS

Informační bezpečnost je soubor pravidel, která je potřeba bezpodmínečně dodržovat, aby byly informace chráněny při jejich vzniku, zpracování, ukládání, přenosu a likvidaci. Tato bezpečnost je dodržována prostřednictvím logických, technických, fyzických a organizačních opatření, která chrání informace proti jejich ztrátě důvěryhodnosti, integrity a dostupnosti. [23]

Informační systém je bezpečný pouze tehdy, pokud informace, které zpracovává, jsou chráněny při jejich vstupu, zpracování, uložení, přenosu a výstupu. [23]

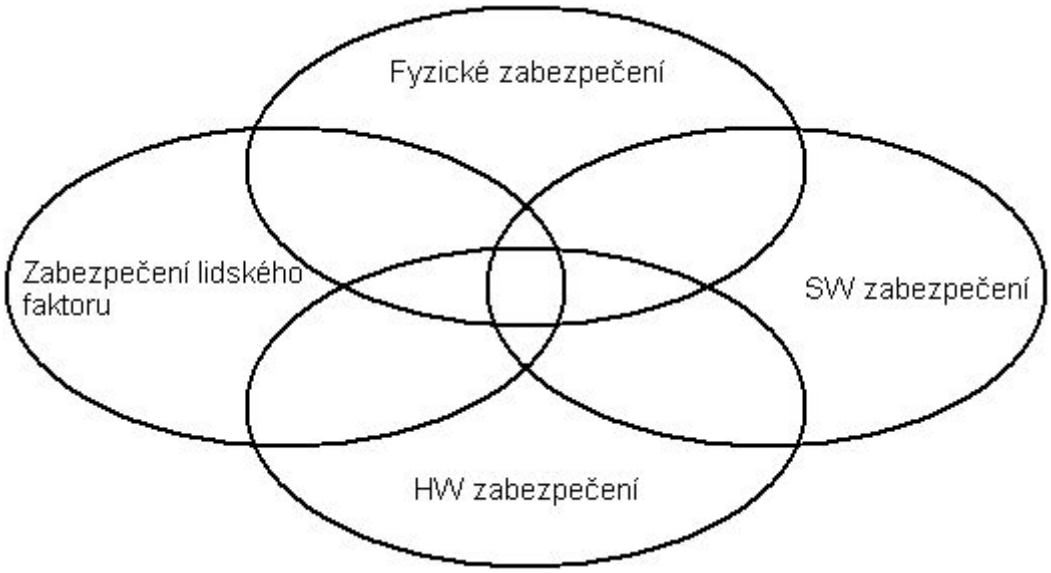
Při napadení systému může dojít ke vzniku mnoha rizikových situací. V základě je můžeme rozdělit na:

- Napadení serverů
- Napadení pracovních stanic
- Napadení síťové infrastruktury
- Napadení na úrovni aplikací
- Odcizení soukromých dat
- Nechtěný přenos dat
- Zablokování služeb

Všechny tyto škody mohou nastat systémovou chybou, ale i chybou člověka. Člověk je může páchat neúmyslně, kdy dochází k nedopatřením nebo chybám programátora, úmyslně nezlomyslně, kdy provádíme penetrační testy, nebo oportunisticky, kdy dochází ke zlomyslnému útoku za cílem poškodit organizaci nebo odcizit citlivé informace. [24]

Dále máme charakterizované bezpečnostní zásady, které:

- určující očekávané postupy,
- definují vhodné chování v systému,
- definují role jednotlivých skupin,
- popisují definice základních pojmů a myšlenek při zabezpečení na síti. [25]



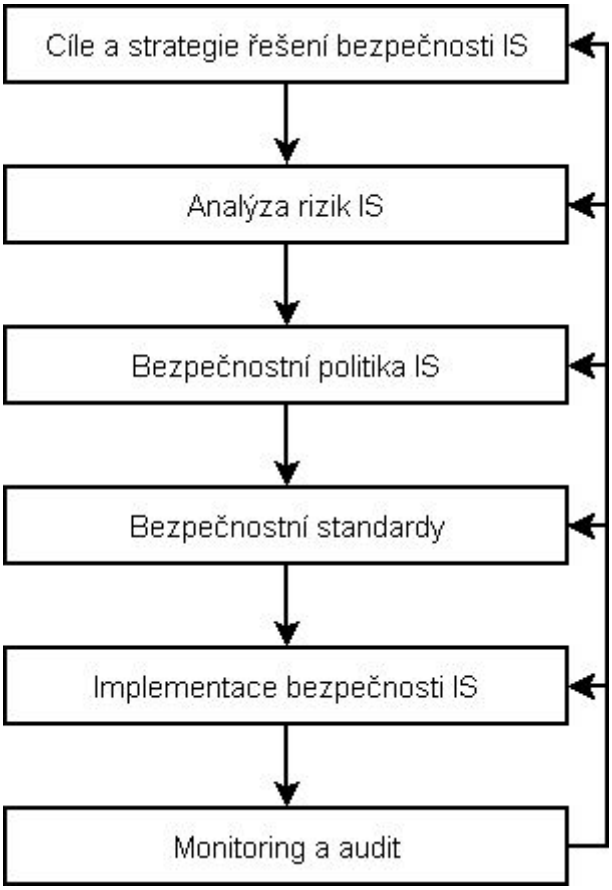
Obrázek 10 Schéma zabezpečení IKS [26]

Bezpečnost informačních a komunikačních systémů se skládá z:

- Počítačové a komunikační bezpečnosti
- Kryptografické ochrany
- Ochrany proti úniku kompromitujícího elektromagnetického vyzařování
- Administrativní bezpečnosti a organizačního opatření
- Personální bezpečnosti
- Fyzického zabezpečení

4.1 Řešení informační bezpečnosti

Základním a prvním krokem řešení bezpečnosti informačních systémů je určení cílů. V bezpečnosti je téměř nemožné riziko naprosto eliminovat, proto se rizika snažíme co nejvíce minimalizovat a zároveň tím minimalizovat následky. Proto naším cílem je minimalizovat přímé a nepřímé ztráty způsobené zneužitím, poškozením, zničením či nedostupností informací. Z tohoto důvodu musíme dodržet následující postup pro informační a komunikační bezpečnost systému.



Obrázek 11 Schéma informační bezpečnosti

Analýza rizik

V této fázi projektu určujeme nejen rizika, která hrozí našemu systému, ale i celé organizaci. I rizika s malou pravděpodobností mohou mít fatální důsledky na chod celého systému.

Pro analýzu rizik existuje mnoho postupů. Jedním z nich je, že si stanovíme aktiva, která chceme chránit a ohodnotíme je. Následně zjistíme hrozby, které hrozí na náš systém, a určíme jejich pravděpodobnost. Následně určíme pro jednotlivé aktivum zranitelnost dle dané hrozby. Výsledné riziko je spočítáno vynásobením určených hodnot.

Díky této analýze určíme, které aktiva jsou vysoce ohrožena a která nejsou v přímém ohrožení, tím pádem jim nemusíme věnovat takovou váhu při vytváření bezpečnostní politiky.

Vnitřní rizika na IKS

- Ztráta
- Modifikace
- Zničení
- Kompromitace dat
- Nedostupnost služeb způsobené lidskou chybou (náhodná/úmyslná)

Vnější rizika na IKS

- Ztráta
- Modifikace
- Zničení dat
- Nedostupnost služeb způsobené náhodnou nebo úmyslnou akcí neautorizovaných osob

Bezpečnostní politika

Díky analýze rizik jsme schopni vytvořit dokument bezpečnostní politiky, ve kterém určíme, jaké jsou naše cíle a jakým způsobem jich chceme dosáhnout. Jedná se o shrnutí chráněných aktiv, kdo za ně nese zodpovědnost a jakým způsobem budou daná aktiva chráněna.

Tento dokument může být v rozsahu několika stránek až po velmi rozsáhlé studie. Vše záleží na organizaci a daném informačním systému, kde mohou být požadavky na bezpečnost velmi rozdílné.

Bezpečnostní standardy

V bezpečnostní politice jsme si určili obecné cíle, kterých chceme dosáhnout. Následně vytváříme bezpečnostní standardy, které přímo specifikují jednotlivé procedury a postupy.

Zde jsou uvedeny jak postupy pro technické a informační zabezpečení, tak fyzickou, organizační a personální bezpečnost.

Bezpečnostních standardů je několik druhů a vždy se odvíjí od organizace. Příkladem jsou například standardy logického přístupu, administrace systému, záložní postupy a postup obnovy, řízení změn, atd. [27]

Implementace bezpečnosti

Jedná se o fázi projektu, kdy bezpečnostní politiku a standardy zavádíme do přímého provozu. S tím je spojeno i proškolení a uvědomění zaměstnanců s danými postupy, které se jich týkají.

Monitoring a audit

I když je bezpečnost daného systému již v provozu, tak pořád musíme provádět kontrolní činnost, zda veškeré postupy fungují tak, jak mají. Některá bezpečnostní rizika mohou být dlouhodobého charakteru, a proto se nemusí vyskytnout ihned po zavedení bezpečnostní politiky. Kontrolní činnost se provádí pravidelně minimálně jednou za rok, ale zároveň je doporučeno dělat nepravidelné namátkové kontroly bezpečnosti.

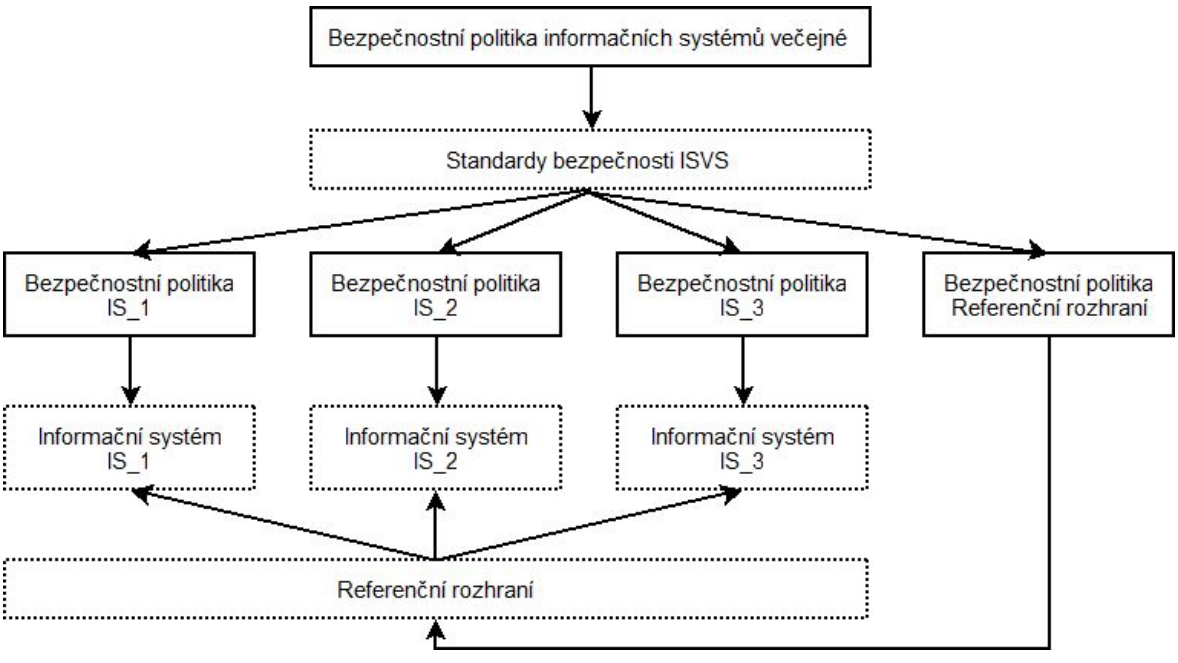
Některé kroky mohou být v praxi prováděny současně nebo v jiném pořadí, proto budeme dané schéma považovat pouze za obecné.

5 BEZPEČNOSTNÍ POLITIKA ISVS

Bezpečnostní politika je dokument, který patří k základům každé společnosti. Součástí tohoto dokumentu je samozřejmě i bezpečnostní politika informačního systému. Tento dokument musí být písemně daný. V jiném případě ztrácí na striktnosti a dochází k modifikaci politiky. V tomto dokumentu máme přesně stanoveno co, proč a jak chceme chránit. Zároveň je specifikováno ověřování dodržování politiky a postupy při vzniku nežádoucí situace. [28]

Bezpečnostní politika ISVS je obsažena v Informační koncepci ISVS a nadále rozvinuta v Provozní dokumentaci ISVS. Bezpečnostní politika ISVS se vytváří pouze tehdy, když ISVS je napojen na jiný ISVS nebo orgán VS není správcem tohoto systému, ale pouze provozovatelem nebo uživatelem.

Jako u všech rozsáhlejších systémů, tak i v systémech veřejné správy musíme rozlišovat soustavu ISVS od jednotlivého systému. Je to z důvodu, že bezpečnostní politika se vytváří na celou soustavu ISVS a zároveň i na jednotlivé subsystémy a referenční rozhraní. Samozřejmě vytváření jednotlivých politik není pravidlem. U malých systémů lze vytvořit jednotnou bezpečnostní politiku a požadavky na jednotlivé subsystémy specifikovat v bezpečnostních směrnicích.



Obrázek 12 Bezpečnostní politika ISVCS

Dále vytváříme bezpečnostní směrnice pro činnost bezpečnostního správce systému, kde podrobně popisujeme veškeré bezpečnostní funkce systému, které správce využívá.

5.1 Základní struktura dokumentů bezpečnostní politiky

1. Charakteristika politizovaného systému vycházející z popisu systému uvedeného v informační koncepci, vymezení systému z hlediska funkčnosti a bezpečnosti v návaznosti na cíle dlouhodobého řízení ISVS.
2. Současný stav bezpečnosti vycházející z výsledků analýzy rizik systému, v rámci které byla provedena identifikace aktiv, hrozeb, zranitelností a stanovena rizika.
3. Vazby bezpečnostní politiky na management orgánů veřejné správy, platnost bezpečnostní politiky a její závaznost.
4. Pravidla organizace bezpečnosti v oblastech rolí a odpovědností, schvalovacích procesů, spolupráce s úřady a odbornými skupinami, bezpečnosti v otázce externích přístupů.
5. Klasifikace a řízení aktiv, jejich evidence v návaznosti na vlastnictví informačních prvků a celků.
6. Bezpečnosti lidských zdrojů v rozlišení na aktuální, zrušené a nové uživatele.
7. Fyzická bezpečnost a zabezpečení prostředí.
8. Management komunikace spočívající v řízení dodávek včetně řízení akceptace z pohledu bezpečnosti.
9. Řízení provozu, především pak ochrana proti škodlivým kódům, zálohování, správa sítě, výměna informací s jinými systémy a monitorování.
10. Řízení přístupu, evidence uživatelů, stanovení pravidel a odpovědností pro přístupy, řízení přístupu k síti a k předmětnému systému.
11. Nákup, vývoj a údržba informačního systému s důrazem na bezpečnost.
12. Management bezpečnostních incidentů
13. Soulad systému s požadavky plynoucích z platné interní/externí legislativy, soulad se standardy bezpečnosti a z hlediska provádění auditu systému. [29]

5.2 Vytváření bezpečnostní politiky ISVS

Při vytváření bezpečnostní politiky ISVS musíme dbát základních postupů a nesmíme opomenout jediný aspekt hrozeb či možných následků.

Stanovení dlouhodobých cílů v oblasti řízení bezpečnosti ISVS:

V každém informačním systému, tak i v ISVS musíme určit dlouhodobé cíle. Ty nám určují, čeho chceme v IS a jeho bezpečnosti dosáhnout. Jsou určeny obecné cíle, jejich řešením se musíme při vytváření bezpečnostní politiky bezpodmínečně zabývat. [30]

V oblasti řízení rizik pro ISVS jsou to vždy tyto cíle:

- Bezpečnost dat, která jsou v daném systému zpracovávána.
- Bezpečnost technických a programových prostředků.
- Bezpečnost služeb, které jsou daným systémem poskytovány.

Na základě určených dlouhodobých cílů určujeme konkrétní požadavky na bezpečnostní politiku orgánu veřejné správy a jejich následné kontrolování a vyhodnocování. [30]

Popis současného stavu ISVS

Jak informační technologie, tak i požadavky uživatelů se stále zvyšují. V našem případě, pokud se jedná o ISVS, tak se jedná hlavně o fyzické a právnické osoby, které chtějí mít své požadavky na veřejnou správu rychle a bezproblémově vyřešeny. Za tímto účelem musíme systém neustále vylepšovat a propojovat s dalšími systémy.

Abychom mohli náš systém vylepšit, či připojit na další ISVS, potřebujeme znát současný stav našeho informačního systému. Tento dokument se netvoří za účelem popisu, jak „skvělý“ máme systém, ale abychom popsali jeho slabé stránky.

Příklady slabých stránek informačního systému:

- Neexistence koncepčního řešení
- IS se bere pouze jako prostředek pro ukládání dat
- Nekoordinované zavádění IS
- Neúplnost, či nepřítomnost bezpečnostních směrnic
- Nesoulad systému s danou legislativou
- Neprovázanost programů dílčích agend
- Nedostatečné využívání nových technologií
- Neproškolení či neodborné proškolení pracovníků [31]

5.3 Organizační řízení bezpečnosti ISVS

Každá organizace musím mít stanovené organizační postupy s ohledem na bezpečnost informací. Musí mít stanovené povinnosti pro jednotlivé pracovníky, kancelář, oddělení a úseky vzhledem k ochraně informací. Zároveň jsou jednoznačně definovány i odpovědnosti jednotlivých zaměstnanců.

V rámci organizační bezpečnosti musíme určit jeden celek v rámci organizace, který bude zodpovídat za zajištění bezpečnosti informací. Tento celek musí být určitého charakteru a splňovat následující náležitosti.

- Musíme určit pravomoci s ostatními organizačními celky. Převážně svrchovanost nad celky informačních technologií, interního auditu a personálního úseku.
- Pracovníci musí být řádně proškolení
- Je zodpovědný za přípravu, schvalování, zavádění a modernizaci postupů a systému. Zároveň organizace práce s dalšími celky, které se podílí, ať již nepřímo, na bezpečnosti informací.
- Je zodpovědný za přípravu, schvalování, zavádění a novelizaci interních předpisů a dokumentů. Tyto dokumenty jsou součástí administrativního řízení a kontroly

bezpečnosti informací za účelem vytvoření interních směrnic organizace. Rozlišujeme směrnice pro standardní a nestandardní situace v organizaci.

- Definujeme správu výjimek z bezpečnostní politiky, pro nestandardní situace.

5.3.1 Předpisy a normy

Pro každou část organizace jsou vytvořeny dokumenty pro určení práv a povinností, případně postupů v případě nestandardní situace. Tyto dokumenty musí být vypracovány v jednotné formě a každý zaměstnanec je s nimi seznámen.

Je zde určena platnost dokumentu, odpovědné celky nebo jednotliví zaměstnanci, kterých se dokument týká, kdo ho vypracovával a kdo je určen jako odpovědný správce pro splnění požadavků dokumentu.

Za aktuálnost, správnost a udržování seznamu všech dokumentů je zodpovědný bezpečnostní celek organizace.

Zároveň jsou určeny předpisy pro správu instalovaných zařízení, které jsou většinou součástí dokumentace od dodavatele. Součástí těchto předpisů jsou i pravidelné kontroly zařízení.

5.3.2 Organizační členění

V případě využívání systému můžeme definovat několik základních skupin osob, které se zabývají jak správou, tak i užíváním systému. Všechny tyto osoby musí mít definována svá práva a povinnosti. Důležité je, aby ani jedna vedoucí skupina osob nebyla svrchována nad jinou, ale aby pracovaly společně. Tím se myslí určení vedoucích pracovníků skupin a jejich zástupců, kteří vytvoří bezpečnostní komisi. V některých případech se může stát, že více funkcí bude zastoupeno jednou osobou. V případě menšího systému to nemůžeme brát jako bezpečnostní riziko, nicméně se nemůže stát, že by jedna osoba měla převahu nad bezpečnostní komisí.

V některých případech využíváme i externí pracovníky, nejen jako dodavatele systému, ale i pro účel servisních zásahů a někdy například i jako provozovatele systému. V tomto případě musí vedoucí zaměstnanci striktně dohlížet na dodržování bezpečnostních postupů

pro manipulaci s informacemi a zároveň musí být smluvně uvedeny i sankce zneužití pravomocí a informací. Tyto sankce jsou samozřejmě uvedeny pro všechny zaměstnance naší organizace. Nicméně striktní dohled je důležitý i pro naše zaměstnance, protože „nespokojený“ zaměstnanec představuje mnohdy několikanásobně větší riziko.

Vedoucí zaměstnanci jsou odpovědni za:

- vytváření bezpečnostní politiky ISVS
- znalost aktiv jim svěřených
- znalost bezpečnostních předpisů a norem
- zajištění využití všech zařízení pouze pro účely jim povolené
- přidělovaní pravomocí a přístupů k aktivům
- proškolení zaměstnanců v oblasti bezpečnosti informací
- zajišťování kontrolní funkce a dodržování nařízených pravidel
- včasnou reakci na nestandardní situace (zneužití informací, zničení aktiv)
- vypracovávání a schvalování místních bezpečnostních politik

Správci IS jsou odpovědni za:

- posouzení hodnoty aktiv jim svěřeným
- účast na procesu hodnocení rizik
- klasifikaci informací
- povolování přístupu k informacím
- dohled nad využíváním systému uživateli a dodavateli
- určování provozovatelů IS
- zajištění bezproblémového chodu systému
- zajištění zálohování systému
- zajištění implementace ochrany dat uložených v systému

- upozornění vedoucích pracovníků na nestandardní situaci, ohrožení bezpečnosti nebo zneužití informací

Provozovatelé IS jsou odpovědni za:

- předávání, ukládání, zpracování a vytváření informací
- respektování požadavku vlastníka informací
- zajištění dostupnosti informací
- zajištění vazeb mezi jednotlivými provozovateli pro sjednocení systému
- zajištění bezpečnosti informací jim svěřených
- upozornění správce IS na nestandardní situaci, ohrožení bezpečnosti nebo zneužití informací

Uživatelé informací jsou odpovědni za:

- dodržování zásad bezpečnosti informací jim svěřených
- využívání informací a aktiv pouze k účelům výkonu povolání
- odpovědnost za přístup informací a pracování pod jeho uživatelskými přístupy
- dodržování bezpečnostních směrnic (pravidelná změna hesla)
- dodržení důvěryhodnosti informací (neprozrazení žádné, ať již nepatrné informace dalším nezainteresovaným stranám)
- upozornění provozovatele, správce, nebo vedoucího pracovníka na nestandardní situaci, ohrožení bezpečnosti nebo zneužití informací

Externí pracovníci (jako dodavatelé informačních technologií) jsou odpovědni za:

- řízení bezpečnosti informačních aktiv a systémů dle pravomocí určených vlastníkem systému
- zajištění správy přístupu k aktivům

- zajištění správy fyzických, technologických a procesních opatření
- informování správců a uživatelů o bezpečnostních postupech a případných změnách
- zajištění autorizovaných přístupů do systému
- upozornění správce IS na nestandardní situaci, ohrožení bezpečnosti nebo zneužití informací

5.3.3 Organizace bezpečnostního řízení

Jako každý systém i informační systém veřejné správy potřebuje řídit, kontrolovat a vykonávat jednotlivé postupy. Proto musíme vyčlenit jednotlivé celky, které se budou touto problematikou zabývat.

Bezpečnostní řízení bude složeno ze složky řídící, kontrolní a výkonné. Složka řídící a kontrolní náleží pro vrcholový management organizace, zato výkonná složka je určena pro administraci informačních systému.

Řízení a kontrola:

Jak jsme již zmiňovali, tak řízení a kontrola je určena převážně pro vrcholový management. V našem případě se jedná o vedoucí pracovníky a správce systému, nicméně v mnoha případech se může stát, že využijeme outsourcing a dle smlouvy zadáme tyto úkoly externí firmě, která vrcholový management informuje o výsledcích, navrhuje a zpracovává změny v bezpečnostní politice.

Řízení bezpečnosti vychází z analýzy rizik. Díky tomu můžeme stanovit jednotlivé postupy pro zajištění bezpečnosti a můžeme eliminovat případné hrozby.

Kontrola se zabývá interním auditem systému. Tento audit rozdělujeme na audit informačních technologií a audit postupů organizace.

Za účelem řízení a kontroly systému se vytváří tzv. bezpečnostní komise, která dohlíží komplexně na celou bezpečnost systému. Bezpečnostní komise je v našem případě nejčastěji složena vrcholovým managerem, bezpečnostním managerem, který je většinou předsedou komise, správcem systému a dalšími zástupci nižších pozic, zainteresovaných

v bezpečnostní politice IS. Členové komise zároveň určují své zástupce, z důvodu nepřítomnosti při vzniku nestandardní situace, nebo ohrožení bezpečnosti organizace.

Výkonná složka:

Tato složka slouží k administraci informačních technologií. Zde striktně oddělujeme odpovědnosti za správu systému a správu bezpečnosti. Je to z toho důvodu, aby nedocházelo ke zbytečnému zatížení jednotlivých pracovníků úkoly, které nejsou jejich povinností a tím pádem i k degradaci výsledného efektu bezpečnosti ISVS. Proto musíme v naší organizaci přesně určit funkci správce systému, bezpečnostního správce a administrátora databáze.

5.4 Systémové řízení bezpečnosti ISVS

Systémové řízeni bezpečnosti můžeme rozdělit na několik základních složek. Jedná se o fyzickou bezpečnost, administrativní bezpečnost, bezpečnost technických zařízení a personální bezpečnost. Každá složka obsahuje souhrn postupů, které jsou pro danou problematiku nejlepší. Většina postupů vychází z dokumentu Národní strategie informační bezpečnosti ČR. Tento dokument má sloužit jako příručka pro oblast bezpečnosti IKS. Většina doporučených postupů má vycházet z tzv. Best practices. Jedná se o nejlepší zkušenosti z praxe, které jsou osvědčeny a využívány v oblasti bezpečnosti IKS. [32]

5.4.1 Fyzická bezpečnost

Informační bezpečnost je pro jakýkoliv systém nezbytnou součástí, z toho důvodu, abychom minimalizovali rizika. Ale pokud nemáme zavedenou fyzickou bezpečnost, která je velmi často zanedbávána, i když je její implementace snadná, tak je náš systém velmi zranitelný.

Pod slovem fyzická bezpečnost si můžeme představit spoustu významů. V našem případě se jedná o technické zabezpečení objektu. Toto zabezpečení využívá:

- mechanické zábranné systémy (MZS)

- poplachové zabezpečovací a tísňové systémy (PZTS)
- přístupové systémy (ACS)
- uzavřené televizní okruhy (CCTV)
- elektronické požární systémy (EPS)

Cílem fyzické bezpečnosti je zamezení přístupů nepovolaných osob (útočníků) do námi označených rizikových prostor. V současné době je již zavedeným standardem, že servery a důležitá zařízení jsou v oddělených místnostech, ale osobní počítače a jejich HW vybavení jsou neustále umístěny v kancelářích, do kterých má přístup většinou více zaměstnanců. [26]

Proto definujeme chráněné zóny objektu, které můžeme rozdělit na veřejné prostory, jako jsou například chodby a kanceláře výkonných pracovníků, místa s přístupem pouze pro zaměstnance organizace a místa s omezeným přístupem. Zón můžeme samozřejmě vytvořit nespočetně mnoho, jsme omezeni pouze limitem zabezpečovacího systému, ale v případě rozsáhlejšího systému můžeme klidně přiřadit každé místnosti vlastní zónu.

Pro systém veřejné správy se jedná hlavně o vytvoření bezpečných perimetrů kolem místností se servery, datovými úložišti a hlavními rozvody.

I v tomto případě platí, že systém je tak silný, jako jeho nejslabší článek. Proto musíme dodržovat jistá pravidla:

- mít odpovídající plášťovou ochranu (mříže, odolné dveře, atd.)
- vhodně umístěné prvky PZTS (maximalizovat spolehlivost systému, minimalizovat vznik planých poplachů)
- vstup do vybraných prostor pomocí ACS systémů
- 24hodinové monitorování vybraných veřejných i neveřejných prostor CCTV systémem se záznamem

Jak již bylo zmíněno, fyzická bezpečnost je velmi důležitou částí bezpečnosti ISVS. Pro pachatele je mnohem snazší projít přes obyčejné zamčené dveře než přes firewally, které chrání náš IS. Proto na fyzickou bezpečnost nesmíme zapomínat.

5.4.2 Administrativní bezpečnost

Jedná se o zabezpečení vstupu a pohybu osob v objektu. Jedná se o rozdělení objektu alespoň na tři základní oblasti:

- Veřejné prostory
    - Tyto prostory jsou přístupny pro všechny osoby bez jakékoliv kontroly a to většinou jen v pracovní době zaměstnanců.
- Zaměstnanecké prostory
    - Jsou přístupny pouze zaměstnancům. Ostatní osoby (návštěvy, servisní a jiné služby) mají přístup pouze v doprovodu autorizované osoby. Většinou jsou tyto prostory spojeny se služebním vchodem pro zaměstnance.
- Prostory s omezeným přístupem
    - Jedná se o prostory, kde mohou vstupovat jen autorizované osoby. Ostatní, ať zaměstnanci nebo jiné osoby, mají přístup pouze výjimečně a v doprovodu těchto osob. Převážně se jedná o servisní služby.

Ve většině případů toto základní rozdělení vyhovuje požadavkům.

Výjimku tvoří zaměstnanci bezpečnostních, servisních a úklidových služeb, kteří se většinou mohou pohybovat po celém objektu, kromě prostor s omezeným přístupem, bez doprovodu. Naneštěstí se v dnešní době všechny tyto služby řeší komplexně pomocí jednoho autorizovaného dodavatele, který smluvně ručí za prověření svých zaměstnanců, a zároveň jsou stanoveny sankce v případě jakéhokoliv porušení bezpečnostních směrnic.

Jak z daného textu vyplývá, administrativní bezpečnost je úzce spojena s fyzickou bezpečností, kde fyzická bezpečnost v provedení ACS systémů zabezpečuje identifikaci, autentizaci a autorizaci přístupu povolaných osob do daných prostor.

5.4.3 Bezpečnost technických zařízení

Pod pojmem bezpečnost technických zařízení si představujeme zabezpečení hmotných aktiv, a tím pádem i zabezpečení nehmotných aktiv informačního systému.

Hlavním cílem zabezpečení je předejít ztrátě, poškození nebo degradaci informací uložených v našem sytému.

Bezpečnost technických zařízení je úzce spjata s fyzickým technologickým zabezpečením. Technická zařízení musí být umístěná odděleně na místech s omezeným přístupem, kde jsou chráněna proti vnějším vlivům a hrozbám. Zároveň musí být vhodně chráněna informačními prostředky, jako jsou firewally a antiviry, kde předcházíme hrozbám přetížení systému DOS útoky, napadení systému viry a hackery, čímž minimalizujeme případné napadení a výpadky systému.

Důležitá technická zařízení, jako jsou servery a datová úložiště, musí být chráněny proti výpadku proudu. To je zajištěno záložními napájecími zdroji.

Hlavní elektrické a komunikační rozvody musí být vedeny ve zdech a v podzemí, kde zamezíme snadnému přerušení a odposlechu případným pachatelem. Ostatní komunikační rozvody by neměli vést přes veřejné prostory a v případě potřeby opatřeny pancéřováním.

Důležitou součástí je i zamezení interference mezi elektrickými a komunikačními rozvody, které zajistíme potřebným odstíněním.

U všech technických zařízení musí probíhat pravidelný servis, který může odhalit případné škody, ale zároveň i nežádoucí zařízení připojená na náš systém.

Při výměně, rozšiřování, nebo modernizaci systému musíme dbát na výběr kompatibilních prvků.

Likvidace zastaralého nebo poškozeného zařízení musí probíhat v souladu s ohledem na maximální zabezpečení informací. V případě vyřazování zastaralých diskových polí musíme zajistit permanentní a dokonalé odstranění všech uložených informací.

Pro testování bezpečnosti našich zařízení je vhodné využívat penetrační testy, prováděné externí, nezainteresovanou organizací pro zjištění případného narušení bezpečnosti.

5.4.4 Personální bezpečnost

Personální bezpečnost tkví ve výběru vhodného pracovníka na danou pozici. V našem případě se jedná o výběr pracovníka s odpovídajícími zkušenostmi, který je trestně bezúhonný a důvěryhodný.

V případě obsazování nižších pozic můžeme pracovníka omezit přístupovými právy do systému tak, abychom co nejvíce omezili možnost zneužití citlivých informací.

V případě pozice provozovatele nebo správce systému jsou možnosti omezení přístupu poměrně složitější. Proto musíme více dbát na důvěryhodnost dané osoby. Vhodným kandidátem je například pracovník informačního oddělení s několikaletou praxí v oblasti, u kterého se nevyskytlo žádné podezření na zneužití jakýchkoliv informací. Nicméně i v tomto případě musíme vyhodnotit, zda je pro nás pracovník důvěryhodný. Nejlepším způsobem je získání referencí od několika zaměstnanců, prověřit si, zda uvedené odborné vzdělání opravdu souhlasí, zda nebyl někdy v minulosti žadatel závislý na návykových látkách, atd.

S personální bezpečností je spojeno i vhodné školení pracovníků. Každý zaměstnanec musí přesně znát svá práva a povinnosti. Zároveň musí znát bezpečnostní směrnice, které se týkají výkonu jeho povolání a zároveň musí být i autoritou pro své podřízené.

Školení pracovníků musí probíhat vhodným způsobem, aby každý zaměstnanec přesně znal bezpečnostní politiku systému, možné hrozby a následky. Zároveň se učí, nejlépe formou interaktivního školení, jak reagovat v případě nestandardní situace.

Každý zaměstnanec musí v případě jakéhokoliv náznaku ohrožení systému, i v případě ohrožení sytému vlastní chybou, vhodně reagovat a neprodleně informovat svého nadřízeného, který je pro tyto účely jmenován.

Školení musí probíhat i pro práci s citlivými informacemi, které nesmí být nijak zdiskreditovány nebo prozrazeny. Pracovníci jsou proškoleni ohledně technické bezpečnosti těchto informací, ale zároveň i proti tzv. sociálnímu inženýrství.

Zaměstnanci musí být motivováni k výkonu svého povolání. Pokud dochází k napětí na pracovišti, stresovým situacím či neshodám mezi pracovníky, tak musí nadřízený pracovník vhodně reagovat a situaci uklidnit. V opačném případě by mohl vzniknout tzv. syndrom nespokojeného zaměstnance, který může být hrozbou pro náš systém.

O všech právech a povinnostech jsou všichni zaměstnanci vhodně poučeni a toto poučení smluvně stvrzují.

Vhodnou „motivací“ pro zaměstnance je případné udělení sankcí za porušení bezpečnosti a vhodné informování o případném trestním stíhání v případě zneužití citlivých informací.

5.4.5 Komunikační bezpečnost

Bezpečný přenos informací je nezbytnou součástí ISVS. Komunikační přenos informací můžeme rozdělit na několik úrovní. Základní rozdělení je přenos informací uvnitř organizace a komunikace s vnějším prostředím.

Komunikace uvnitř organizace by měla probíhat pomocí uzavřené komunikační infrastruktury. I v případě neveřejné sítě musíme dodržovat pravidla bezpečnostní politiky pro přenos citlivých informací pomocí šifrování a vhodných certifikátů, které vydává certifikační autorita, v našem případě správce systému.

Komunikace s vnějším prostředím můžeme rozlišit na běžnou komunikaci, která nepodléhá přísné bezpečnostní kontrole, ale minimální zabezpečení musí být zavedeno.

Každý jednotný systém komunikuje s vnějším prostředím pomocí referenčního rozhraní, které je součásti každého ISVS. Správcem referenčního rozhraní je Ministerstvo vnitra. Viz 3.6 Referenční rozhraní.

Komunikace mezi ISVS probíhá přes komunikační infrastrukturu veřejné správy (KISV). Tato síť je spravována Ministerstvem vnitra, které dohlíží na její bezpečný a bezporuchový provoz. Viz 3.2.1 Komunikační infrastruktura veřejné správy.

Komunikace systému ISVS se systémem základních registrů probíhá přes KISV, která je doplněna několika bezpečnostními prvky. Viz 3.2.2 Základní registry veřejné správy.

Celý systém musí být vhodně strukturován a vybaven technickým vybavením, které určuje Ministerstvo vnitra formou dokumentu Katalogových listů KIVS. Tento dokument je vydáván usnesením vlády o Koncepci nákupu datových a hlasových služeb KIVS.

II. PRAKTICKÁ ČÁST

6 MODEL ISVS PRO MĚSTSKÝ ÚŘAD

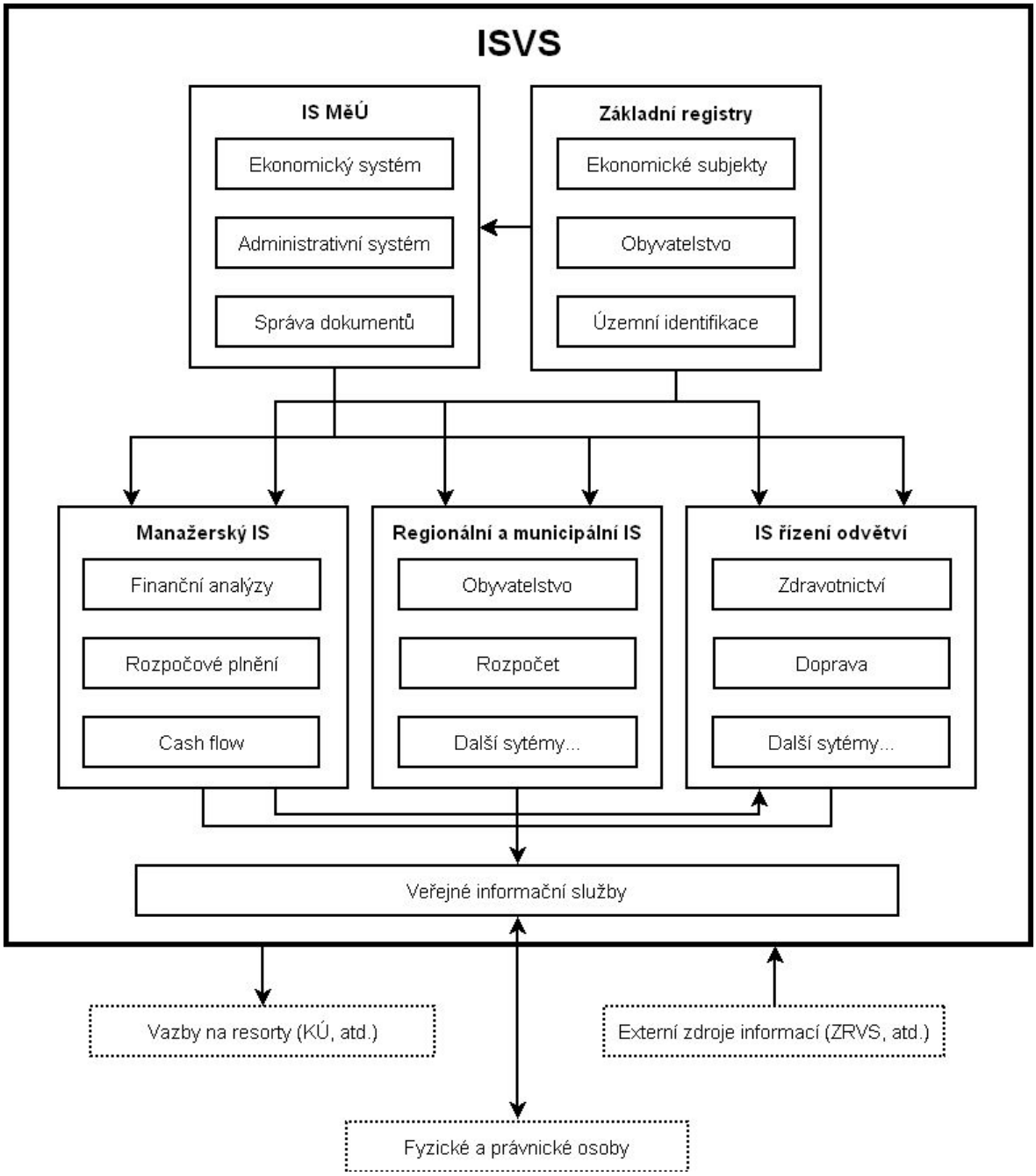
Pro vytvoření bezpečnostní politiky pro ISVS musíme mít strukturu IS. Proto si vytvoříme smyšlený model ISVS pro městský úřad s rozšířenou působností. Náš systém bude tvořen několika ISVS a provozními agendami s vazbou na jiný ISVS.

Pořizovatelem a správcem ISVS je náš MěÚ, který financoval jeho vybudování z vlastních zdrojů. Náklady na provoz a údržbu jsou taktéž hrazeny z finančních zdrojů úřadu.

Správcem systému je vedoucí oddělení informatiky. Ten se stará o bezproblémový chod systému.

Náš informační systém je složen z několika subsystémů:

- Ekonomický systém
- Administrativní systém
- Správa dokumentů
- Regionální a municipální IS
- Manažerský IS
- IS pro řízení odvětví
- Základní registry
- Veřejné informační služby
- Další subsystémy…



Obrázek 13 Struktura ISVS pro MěÚ

Systém je napojen pomocí referenčního rozraní a KIVS na různé resorty pro předávání důležitých informací. Jedná se o subsystémy, tzv agendy, které jsou napojeny na další ISVS.

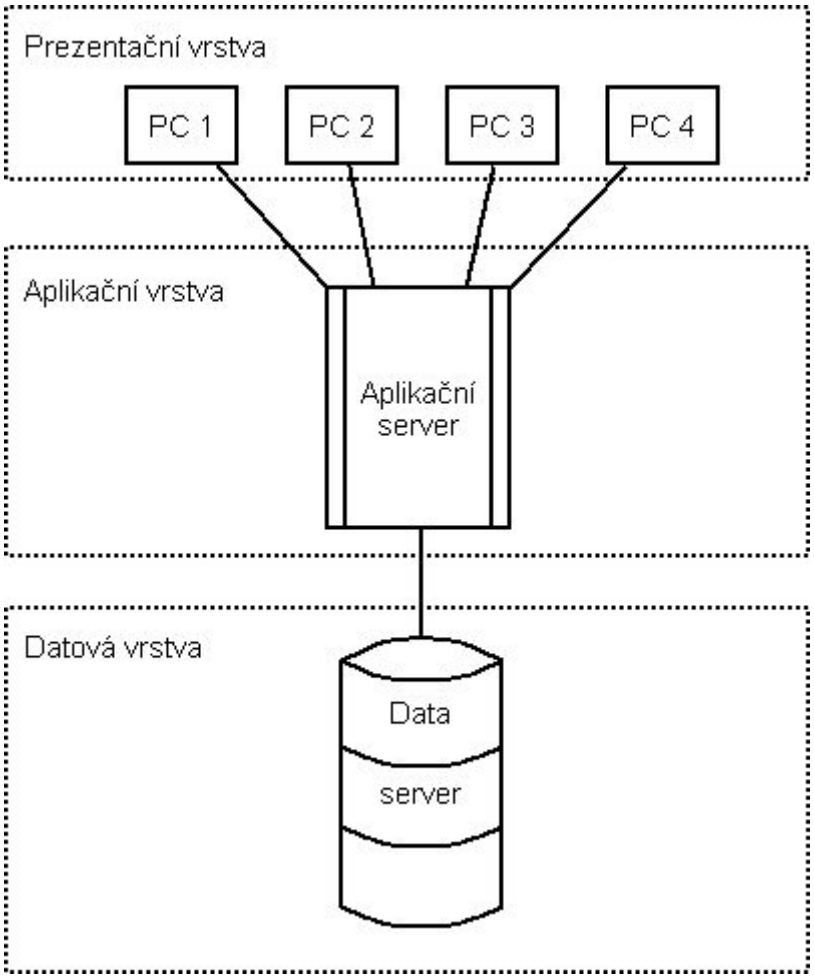
Agendy s vazbou na další ISVS:

- Účetnictví (předávání finančních výkazů krajskému úřadu)

- Účetní výkaznictví (předávání finančních výkazů krajskému úřadu)
- Mzdy

Protože na našem serveru běží agendy s vazbou na další ISVS, jsme povinni mít pro daný systém vypracovanou informační koncepci a provozní dokumentaci. Součástí provozní dokumentace je i bezpečnostní politika, kterou musíme mít vypracovanou pro náš IS, a která je nezbytná pro získání atestu.

Celý systém je postaven na třívrstvé architektuře. Uživatelé využívají prezentační vrstvu pro zadávání svých požadavků a získávání výsledku ze strany serveru. Strana serveru je tvořená aplikační vrstvou pro vyhodnocování požadavku a datová vrstva, kde dochází k veškerým procesům práce s daty.



Obrázek 14 Třívrstvá architektura IS

Protože náš ISVS funguje jako nezávislý IS s vazbou na další ISVS jsme povinni získat dodržovat pravidla pro vytváření, užívání a provozování ISVS. Z toho důvodu potřebujeme získat atestaci na IS. Pro získání atestace musíme předložit několik dokumentů, kde jedním z nich je Bezpečnostní politika ISVS.

7 NÁVRH BEZPEČNOSTNÍ POLITIKY PRO MODEL ISVS

Vzhledem k tomu, že jsme udělali bezpečnostní audit stávajícího systému a zhodnotili rizika, tak jsme schopni vytvořit bezpečnostní politiku.

V tomto dokumentu určíme následující:

- Bezpečnostní cíle ISVS
- Organizační bezpečnost
- Bezpečnostní opatření

7.1 Bezpečnostní cíle ISVS

Cílem naší bezpečnostní politiky je zajištění činností a stavů, které jsou nezbytné pro každý IS. Tyto činnosti a stavy jsou:

- Zajištění ochrany dat a prostředků IS
- Trvalé a kvalitní zajištění dostupnosti, důvěryhodnosti, integrity a autentizace dat
- Zajištění bezpečné komunikace s vnějším prostředím

7.1.1 Požadavky na bezpečnost ISVS

V požadavcích na bezpečnost uvádíme konkrétní informace na dosažení bezpečnostních cílů IS.

Zajištění ochrany dat a prostředků

- Personální bezpečnost
- Zajištění fyzické bezpečnosti ISVS
- Systém antivirové ochrany
- Bezpečností směrnice pro:
    - Vnitřní hrozby (bezpečnostní pravidla pro uživatele)

  - Vnější hrozby (bezpečnostní opatření proti napadení útočníkem, přírodní katastrofou, neúmyslným zaviněním)

- Ustanovení správce ISVS
- Ustanovení bezpečnostního správce ISVS

Trvalé a kvalitní zajištění dostupnosti, důvěryhodnosti, integrity a autentizace dat

- Identifikace a autentizace oprávněných uživatelů (přístup k informacím na základě funkčního zařazení)
- Ochrana soukromí uživatelů (zajištění bezpečnosti osobních údajů před jinými uživateli a cizími osobami)
- Pravidelné zálohování a archivace dat

Zajištění bezpečné komunikace s vnějším prostředím

- Bezpečná komunikace mezi MěÚ a dalšími subjekty (veřejné subjekty, státní správa)
- Využívání bezpečných komunikačních cest

7.2 Organizační bezpečnost ISVS

Náš IS pro MěÚ spadá do provozní problematiky úřadu. Tím pádem realizaci bezpečnostní politiky a personálního zabezpečení včetně stanovení rolí a odpovědností schvaluje tajemník úřadu.

Pro organizační bezpečnost jsou definována následující opatření:

- Bezpečnostní komise, včetně pravomocí a odpovědností
- Bezpečnostní správce, včetně pravomocí a odpovědností
- Definování povinností uživatelů ISVS MěÚ

7.2.1 Bezpečností komise ISVS

Bezpečnostní komise je složena z:

- Vedoucího oddělení informatiky – předseda komise
- Zástupce odboru tajemníka MěÚ
- Zástupce odboru správy MěÚ

Pravomoci a odpovědnosti bezpečnostní komise jsou:

- Formuluje zásady bezpečnostní politiky IS
- Zodpovídá za řízení přístupu k informačním systémům a informačním aktivům
- Koordinuje implementaci opatření v oblasti bezpečnosti IS MěÚ
- Zodpovídá za průběžné monitorování a ověřování funkčnosti zavedených bezpečnostních opatření
- Navrhuje a podporuje iniciativy týkající se bezpečnosti IS MěÚ
- Prosazuje, aby podpora bezpečnostní politiky ze strany vedení byla viditelná v celém úřadě
- Definuje bezpečnostní cíle a sleduje jejich zavádění
- Navrhuje hlavní kroky vedoucí ke zvýšení bezpečnosti dat a prostředků v IS MěÚ,
- Navrhuje specifické role a odpovědnosti v oblasti bezpečnosti IS v rámci celého úřadu,
- Navrhuje metody a postupy v oblasti bezpečnosti
- Kontroluje, aby bezpečnost byla součástí procesu plánování v oblasti informatiky
- Prosazuje zvyšování bezpečnostního uvědomění uživatelů IS MěÚ
- Definuje potřebné požadavky na lidské znalosti a na finanční náklady
- Řeší disciplinární problémy vůči bezpečnosti
- Hodnotí účinnost bezpečnostní politiky

7.2.2 Bezpečnostní správce ISVS

Jedná se o pověřenou osobu, která dohlíží na bezpečnost celého systému.

Pravomoci a odpovědnosti bezpečnostního správce jsou:

- Zodpovídá za dodržování bezpečnosti IS MěÚ
- Spolupracuje s bezpečnostní komisí a správcem IS MěÚ
- Řídí zavádění bezpečnostních opatření podle definovaných bezpečnostních cílů
- Průběžně monitoruje bezpečnostní incidenty a účinnost bezpečnostní politiky a ověřuje funkčnost zavedených bezpečnostních opatření
- Podílí se na zvyšování bezpečnostního uvědomění uživatelů IS MěÚ
- Zodpovídá za to, aby bezpečnostní politika byla součástí plánování v oblasti informatiky
- Navrhuje hlavní kroky vedoucí ke zvýšení bezpečnosti dat a prostředků v IS
- Navrhuje specifické role a odpovědnosti v oblasti bezpečnosti IS MěÚ v rámci celého úřadu
- Navrhuje metody a postupy v oblasti bezpečnosti IS MěÚ
- Zajišťuje, aby dodavatelé služeb IT dodržovali bezpečnostní politiku úřadu a ostatní relevantní vnitřní předpisy

7.2.3 Uživatelé ISVS

Uživateli jsou zaměstnanci, kteří mají práva pracovat s IS MeÚ.

Povinnosti uživatelů IS jsou:

- Řídit se provozním řádem IS MěÚ
- Využívat výpočetní techniku pouze pro výkon svého povolání
- Řídit se pokyny oddělení informatiky MěÚ
- Zajistit svěřenou výpočetní techniku proti přístupu neoprávněných osob

Uživatelům IS je zakázáno:

- Jakkoliv měnit konfiguraci přidělené výpočetní techniky
- Provádět jakékoliv technické zásahy do přidělené výpočetní techniky

7.3 Identifikace aktiv - analýza bezpečnostních rizik

Určíme si hmotná a nehmotná aktiva naší organizace.

Vnější rizika mohou být přírodního nebo fyzického původu. Rizika přírodního původu jsou méně pravděpodobná, nicméně v případě, že taková situace nastane, může mít drtivý dopad na celý systém a tím pádem i na celou organizaci.

Po určení aktiv našeho systému jsme pro analýzu rizik využili demoverzi programu Ranit 5. Tento program slouží jako nástroj pro analýzu rizik na informační systémy. Program nám přehledně určil rizika pro dané aktiva. (viz Příloha č. II)

Při vniku jakékoliv situace může nastat hrozba, kterou nesmíme ignorovat. Proto musíme znát i možné následky na informační systém.

Tabulka 1 Příklady rizik vnějšího prostředí

Hrozby	Následky
Živelná pohroma	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW
Požár	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW

Zaplavení (povodně, vodovodní potrubí)	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW
Přerušení elektrické energie	úplný výpadek systému částečný výpadek systému ztráta nezálohovaných dat
Napadení IS hackerem	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW krádež citlivých informací
Napadení IS virem	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW krádež citlivých informací

Vnitřní rizika jsou pro náš systém pravděpodobnější a ve většině případů je pro nás mnohem jednoduší se proti těmto rizikům bránit.

Tabulka 2 Příklady rizik vnitřního prostředí

Hrozby	Následky
Poruchy HW	úplný výpadek systému částečný výpadek systému

	ztráta dat poškození HW krádež citlivých informací
Poruchy sítě	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW krádež citlivých informací
Nestandardní chování SW	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW krádež citlivých informací
Zneužití identity uživatele neoprávněnou osobou	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW krádež citlivých informací
Vyzrazení/krádež citlivých informací (nespokojený zaměstnanec)	úplný výpadek systému částečný výpadek systému ztráta dat poškození HW krádež citlivých informací

Výsledkem analýzy jsme zjistili míru rizika pro jednotlivá aktiva a taky jsme si určili míru zranitelnosti. Ta nám vyjadřuje, jak dlouho bude trvat obnovení systému do původního stavu.

Tabulka 3 Analýza rizik hmotných aktiv

Hmotná aktiva	**Míra rizika**	**Míra zranitelnosti**
Síťový server	3	Týdny
Databázový server	3	Týdny
Centrální prvky sítě	3	Týdny
Centrální kabelové rozvody	2	Dny
Osobní počítače	1	Hodiny
Ostatní HW	1	Hodiny

Tabulka 4 Analýza rizik nehmotných aktiv

Nehmotná aktiva	**Míra rizika**	**Míra zranitelnosti**
Operační systém - server	3	Týdny
Operační systém - osobní počítače	1	Hodiny
MS Exchange	3	Dny
MS SQL Server	3	Dny
Zoner antivirus	3	Dny
InterBase Firebird	2	Dny
Účetnictví	3	Dny
Rozpočet	3	Dny
Účetní výkaznictví	2	Dny

Pohledávky	3	Dny
E-spisy	3	Dny
GIS	3	Dny
Evidence majetku	3	Dny
Mzdy	3	Dny
Přestupky	2	Dny
Matrika	3	Dny
Volby	2	Dny
Registr obyvatel	2	Dny
připojení do sítě MV ČR	3	Dny
připojení na ZR	3	Dny
Připojení do sítě Internet	2	Dny

Příklad analýzy pro síťový server je uveden příloze.

7.4 Bezpečnostní opatření

7.4.1 Systémové zabezpečení

V systémovém zabezpečení hledíme na důslednost a bezpečné používání informačních technologii a dalších jejich prostředků, kterými jsou:

- Bezpečné nastavení přístupu k datům
- Dostatečná délka hesel (15 znaků a více)
- Firewall
- Antivirové programy (pravidelné aktualizace)
- Využívání jen administrativních prostředků k výkonu povolání (daný operační systém, daný SW)
- Zabezpečení pracoviště při odchodu

- Použití šifrovacích prostředků pro přenos informací po vnější síti
- Zaznamenávání provozu serverů
- Monitorování a zaznamenávání přístupu k citlivým informacím
- ACS pro přístup do neveřejných prostor
- Kontrola komunikačních cest
- Evidence poruch

7.4.2 Fyzické zabezpečení

Z důvodu zabezpečení budovy MěÚ je v prostorech instalován elektronický zabezpečovací systém. Dále jsou vyhrazeny prostory s přístupem pouze pro povolané osoby. V našem případě, prostory s prostředky IS, kde se nalézají síťové servery a centrální aktivní prvky kabelových rozvodů, jsou přístupny pouze pro správce systému a zástupce vedení úřadu či v jejich doprovodu.

Centrální kabelové rozvody jsou vedeny skrytě uvnitř stěn, aby nebylo možné je snadno poškodit, nebo se na ně napojit.

Síťové a zálohovací servery jsou umístěny v místnosti s nezávislou klimatizací. Jsou připojeny na záložní napájecí zdroj UPS pro případ výpadku elektrického proudu.

Všechna výpočetní technika smí být používána jen v prostorách MěÚ. Výjimkou jsou notebooky a tablety sloužící pro vedení MěÚ.

PC stanice jsou uzamčeny proti nedovolené manipulaci s HW vybavením a síťové prvky, které tvoří např. routery a switche jsou umístěny v uzamčených skříních.

Celkové fyzické zabezpečení budovy a prostor je tvořeno:

- MZS systém
    - Mříže na oknech v přízemí budovy
    - Dveře bezpečnostní třídy 3 pro vchod do budovy a vyhrazených prostor
- PZTS systém
    - Umístění PIR detektorů v celé budově
    - Siréna na plášti budovy

- Napojení na PCO Policie ČR

- ACS systém
  - Docházkový systém pomocí bezkontaktních karet
  - Vyhrazení práv přístupu do jednotlivých prostor MěÚ dle povolání
  - Vyhrazené prostory s prostředky IS přístupné pouze s bezkontaktní kartou a pinem, který je jedinečný pro každou pověřenou osobu

- CCTV systém
  - Kamery umístěny ve vstupní hale, u jednotlivých přepážek a vstupů do vyhrazených prostor
  - Kamery umístěny v prostorech s prostředky IS z důvodu případného dohledání neoprávněné manipulace s vybavením

- EPS
  - V budově jsou rozmístěny požární hlásiče
  - Jedná se o detektory kouře a tlačítkové hlásiče

7.4.3 Personální a organizační zabezpečení

Jsou stanovena pravidla, kompetence a odpovědnosti pro bezpečnost informačních technologií MěÚ, která jsou zakotvena v interních bezpečnostních směrnicích. S těmito nařízeními je seznámen každý zaměstnanec úřadu a jejich dodržování stvrzuje vlastnoručním podpisem. V případě jejich porušení jsou definovány sankce pro zaměstnance.

Pro každého uživatele IS je určeno programové vybavení a přístup k datům dle jejich vykonávané funkce. Tato oprávnění uděluje bezpečnostní správce systému po konzultaci s vedoucím daného oddělení.

Jsou uděleny povinnosti určených uživatelů, kteří ručí za správnost a aktuálnost dat, která jsou vládána do systému.

Každý zaměstnanec pracující s IS MěÚ je řádně proškolen se způsobem práce se systémem. Zároveň je povinen hlásit jakékoliv poruchy systému či podezření na porušení bezpečnostních směrnic bezpečnostnímu správci IS.

O celém systému se vedou provozní deníky, kde jsou evidovány veškeré události o porušení bezpečnostních směrnic, poruchách či výpadcích systému. Za vedení provozních deníků je zodpovědný bezpečnostní správce systému.

V případě, že nastane nestandardní situace a nejsou přítomny kompetentní osoby odpovědné za chod systému, je pověřen kompetentní zástupce, který bude schopen danou situaci řešit.

7.5 Kontrola ISVS

Kontrola celého systému se provádí formou prověrek a testů minimálně jednou ročně. Celý proces řídí bezpečnostní správce ve spolupráci se správcem systému. Pokyn ke kontrole podává bezpečnostní správce, ale může být vykonána i na pokyn bezpečnostní komise.

Při kontrole prověřujeme a testujeme:

- Dodržování bezpečnostních směrnic
- Kontrolu provozních deníků
- Kontrolu přístupových práv
- Testy funkčnosti systému
- Penetrační testy (pokus o neoprávněný přístup)

7.6 Komunikace s ZRVS

Komunikace bude realizována po síti veřejné správy KIVS. Pro komunikaci jsou využity služby vnějšího rozhraní publikované v UDDI registru. Přenos informací probíhá zabezpečeným protokolem HTTPS s ověřením klienta. Pro přístup do systému bude potřeba získat klientský certifikát od certifikační autority, která bude provozována Informačním systémem základních registrů (ISZR).

- Autentizace – pomocí klientského certifikátu
- Autorizace – pomocí identifikátoru agendy, ke které budou přiřazeny práva v registru práv a povinností (RPP)
- Důvěryhodnost – pomocí šifrovaného spojení HTTPS

Veškerá komunikace a kontrola oprávnění přístupu je zprostředkována pomocí ISZR.

8 OBECNÁ DOPORUČENÍ PRO ŘÍZENÍ RIZIK

Pod pojmem řízení rizik si představujeme doporučené postupy pro řešení nestandardních situací.

Tyto situace jsou např.:

- Krátkodobý výpadek systému
- Dlouhodobý výpadek systému
- Selhání bezpečnosti
- Napadení systému (hackerem, virem)
- Únik citlivých informací (vyzrazení, krádež)
- Poškození systému (ne\úmyslné)

Žádný systém není dokonale bezpečný a žádná zavedená bezpečnostní politika nám nemůže zaručit striktní dodržování bezpečnostních pravidel. Z toho důvodu provádíme řízení rizik. K tomuto řízení nám napomáhá několik metod a procesů, které se musí v rámci bezpečnosti aplikovat na náš IS.

8.1 Monitoring

Je nejdůležitějším východiskem pro zvládání rizik. Průběžným monitorováním systému získáváme cenné informace o chování systému.

Výsledky monitoringu jsou sledovány a analyzovány bezpečnostním správcem systému, který je následně schopný vytvářet bezpečnostní opatření pro zvýšení komplexní bezpečnosti celého systému. Pro zvýšení účinnosti monitoringu by měly být výsledné analýzy zhodnoceny nestrannými odborníky, kteří zhodnotí, zda jsou daná bezpečnostní opatření vhodná a účinná. V případě nesouhlasu interpretují své výsledky bezpečnostnímu správci IS, který vyvodí patřičné závěry.

8.2 Bezpečnostní audit

Nezávislý audit klíčových částí systému a celkové bezpečnosti slouží k ověření komplexního způsobu zabezpečení IS. Bezpečnostní audit by měl probíhat v pravidelných intervalech, ale i jako namátkové kontroly. Auditorem může být zaměstnanec organizace nebo externí pracovník. Důležité je předložení výsledků vedení organizace, porovnávání výsledků s předchozími audity. Díky tomu získáme přehled o stavu bezpečnosti našeho systému a zároveň můžeme provádět prognózy budoucích stavů.

8.3 Revize

Každý informační systém se vyvíjí a tím zároveň vznikají nové hrozby a nutnosti protiopatření proti vzniku krizové situace. Revize slouží k zjištění vhodnosti bezpečnostní politiky na daný IS. Zároveň se bezpečnostní opatření porovnávají s novými trendy.

Provádí se minimálně jednou ročně. Je vhodné využít služeb externí organizace, která s námi bude konzultovat veškeré poznatky.

Tabulka 5 Řízení rizik dle organizace [33]

Proces	**Malá organizace**	**Střední organizace**	**Velká organizace**
Monitoring	Namátkový monitoring IS, vyhodnocování záznamů událostí a logů do systému. Testování zranitelností systémů připojených do veřejné sítě.	Pravidelný monitoring IS, vyhodnocování záznamů událostí a logů do systému. Testování zranitelností systémů připojených do veřejné sítě a k dalším stranám.	Centralizovaný automatický monitoring IS, vyhodnocování záznamů událostí a logů do systému. Pravidelné testování zranitelností, podpořené penetračními testy. Bezpečnostní analýza klíčových prvků systému.

Bezpečnostní audit	Audit opatření dle dokumentace a plánu auditu. Iniciátorem je vedoucí organizace. Auditorem je pracovník organizace. Namátková interní kontrola stavu opatření.	Audit opatření dle dokumentace a plánu auditu. Bezpečnostně technický audit klíčových systémů Namátková interní kontrola stavu opatření.	Pravidelná kontrola a audit bezpečnostních opatření dle směrnic a nařízení. Průběžný bezpečnostně technický audit celého systému.
Revize	Rámcová revize a vyhodnocení aktuálnosti, efektivnosti a adekvátnosti opatření.	Roční podrobná revize a stavu opatření s využitím externího konzultanta. Porovnávání opatření s novými postupy a vývojem hrozeb a zranitelností.	Srovnávací audit stavu IS s normou. Průběžné přehodnocování hrozeb a zranitelností dle cílů organizace.

8.4 Penetrační testy

Jedná se o testování zranitelných míst systémů za účelem odhalení slabých míst systému. Při penetračních testech se díváme na celý systém i na jeho části z pohledu hackera, který má zájem poškodit náš systém, a tím i celou organizaci.

Penetrační testy provádíme pravidelně, pokud možno bez vědomí řadových zaměstnanců, kteří sami, ať už vědomě či nevědomě, mohou porušovat zásady bezpečnostní politiky.

Vhodné, i když poměrně nákladné, je využití externí organizace, která nestranně vyhodnotí odolnost našeho systému proti útokům. Po provedení penetračních testů dostaneme doporučení pro zvýšení bezpečnosti.

8.5 Havarijní plány

Pro všechny situace bychom měli mít připravené havarijní plány, kde budou sepsány jednotlivé postupy a procesy s tím spojené. Tyto plány musí být pravidelně aktualizovány a přizpůsobeny pro náš systém. S procesem zvládání rizik souvisí i pravidelné cvičení, kde se testuje reakce zúčastněných osob a schopnost uvedení systému do normálního režimu.

Před vytvořením havarijních plánů musíme být schopni pochopit rizika, která hrozí. U každého rizika určujeme možnou pravděpodobnost, s jakou může daná situace nastat a jaké budou její dopady. Pro určení rizik si určíme priority na základě identifikace kritických částí systému a procesů systému.

Při určování možných dopadů bychom měli být schopni sdružovat podobné incidenty a vytvářet taková opatření a postupy, které budou univerzální a použitelnými jak v malých případech, tak i ve velkých případech narušení bezpečnosti.

Při vytváření havarijních plánů vycházíme z analýzy rizik, kde jsme určili důležité části systému a hrozby a rizika, jež na ně působí. Díky tomu jsme schopni určit obnovitelnost jednotlivých částí systému. Obnovitelnost rozdělujeme do třech základních složek. Části systému, které jsme schopni obnovit v řádu hodin, v řádu dní a v řádu týdnů.

8.6 Plány obnovy

Nezbytnou součástí každého IS je vytvoření plánu obnovy. Plán slouží pro obnovení systému do normálního provozu. Jsou vypracovány tak, aby co nejefektivněji a v co nejkratším časovém období vyřešily škody vzniklé rizikovou událostí v našem IS.

9 VÝVOJ BEZPEČNOSTI ISVS

Informační systémy veřejné správy a jejich bezpečnost se vyvíjí každým dnem, a to hlavně díky OECD a účasti České republiky a na celosvětovém projektu e-Governmentu. Můžeme říct, že vývoj bezpečnosti ISVS přímo souvisí s vytvářením, rozšiřováním a vzájemným propojování ISVS.

Příkladem je tomu i vznik základních registrů veřejné správy, na které by měly být v budoucnu připojeny všechny orgány VS, a tím zabezpečit rychlý a bezproblémový přístup k informacím. Dalším příkladem je vznik KIVS a její neustálé rozšiřování a upravování legislativy s ní související za účelem zaručení větší bezpečnosti přenosu informací.

V budoucnu by měl být zaveden čtyřvrstvý model sdílení služeb veřejné správy tvořený službami pro VS, službami informační společnosti, službami IKT platforem a službami pro datovou komunikační infrastrukturu. Služby veřejné správy budou zajišťovat procesy a služby veřejné správy v rámci legislativy. Služby informační společnosti budou poskytovat rozmanité služby v rámci všech systémů veřejné správy. Služby informačních a komunikačních technologií budou definovat národní provozní standardy, včetně krizové infrastruktury státu. Služby datové komunikační infrastruktury budou definovat národní komunikační standardy, včetně krizové komunikační infrastruktury. Každá tato vrstva bude mít vlastní správu a tím pádem i své požadavky na legislativu a vytváření, implementování a řízení bezpečnostní politiky.

V budoucnu by ISVS, např. pro MěÚ, mohl sloužit pouze a jen jako administrativní systém, kde stávající systémy nahradí agendové systémy připojené přes KIVS a Portál veřejné správy na jednotný systém veřejné správy. Díky tomu bychom dosáhli centralizace informací sloužící pro efektivnější fungování veřejné správy a snadnému přístupu k potřebným informacím pro fyzické a právnické osoby.

Vývoj bezpečnosti ISVS spočívá ve vytvoření jednotného systému pro zpracování, přenos a uložení informací, využívající kompatibilní prvky, které by ručily za minimalizaci chyb v informačním cyklu a zároveň vytvoření jednotných norem a standardů pro vytváření, implementaci, a řízení bezpečnosti ISVS. Tyto normy a standardy by byly specifikovány dle úrovní orgánů veřejné správy a každý orgán by byl povinen tato nařízení dodržovat.

ZÁVĚR

Cílem diplomové práce bylo navrhnout implementaci bezpečnostní politiky v informačním a komunikačním systém veřejné správy, kde jsem využil své znalosti z problematiky bezpečnosti a informačních systémů.

Při vytváření bezpečnostní politiky pro jakýkoliv informační systém je nutné znát základní postupy pro řešení informační bezpečnosti. V oblasti informačních a komunikačních systémů veřejné správy je nutné rozšířit znalosti o legislativní požadavky na tyto systémy, které jsou z důvodu přehlednosti a ucelenosti vymezeny v metodických pokynech vydávaných Ministerstvem vnitra ČR.

Základem bezpečnostní politiky je určení cílů, kterých chceme dosáhnout. Důležité je zjištění aktiv organizace a provedení analýzy rizik, od které odvíjíme celý proces vytváření návrhu. Po dokončení návrhu nastupuje implementace politiky do systému a jeho následné sledování. Tento krok nazýváme řízení rizik, kde monitorujeme, testujeme a odhalujeme případná další rizika na systém.

V práci jsou uvedeny postupy pro vytváření bezpečnostní politiky informačních a komunikačních systémů veřejné správy. Jsou zde uvedeny případy propojení systémů s dalšími subjekty a agendovými systémy, které jsou součástí informačních systémů pod správou Ministerstva vnitra.

Návrh implementace bezpečnostní politiky je tvořen uvedením cílů informačního sytému, organizační bezpečností, identifikací aktiv, analýzy rizik a bezpečnostními opatřeními. Tato opatření dělíme na systémová, fyzická, personální a organizační. Součástí bezpečnosti informací je i pravidelná kontrola zavedených postupů. Podrobné metody a postupy jsou následně určeny v bezpečnostních směrnicích organizace.

Veškeré tyto metody a postupy jsme implementovali na fiktivní model městského úřadu, který je napojen na agendové systémy veřejné správy. Implementací jsme docílili vytvoření dokumentu, který můžeme využít pro získání atestu pro náš informační systém.

Nakonec jsme určili obecná doporučení pro systém řízení rizik v informačních systémech, kde jsme uvedli procesy a způsoby jejich provádění a budoucí vývoj informačních systémů veřejné správy.

ZÁVĚR V ANGLIČTINĚ

The aim of this thesis was to design security policy implementation in the information and communication system of public administration, where I used my knowledge of security issues and information system.

During the creation of a security policy for any information system is necessary to know the basic procedures for information security solutions. In the field of information and communication systems of public administration it is necessary to broaden the knowledge of legislative requirements for these systems, which are defined to the methodological guidelines issued by the Ministry of Interior for clarity and consistency.

The basis of security policy is to determine the targets, which we want to achieve. It is important to identify assets of the organization and risk analysis, from which we unfold the entire design process. After completing the design, we are going to implementation of policy in the system and monitor the system. This step is called risk management, where the system is monitored, tested and any additional risk to the system is detected.

The paper describes the procedures for creating security policies for information and communication systems of public administration. There are cases describing system interconnectivity with other subjects and agenda systems, which are part of the information systems under the administration of the Ministry of Interior.

Design implementation security policy is made by stating the objectives of the information system, organizational security, asset identification, risk analysis and security measures. These measures are divided into systemic, physical, personnel and organization. The part of information security is the regular inspection of established procedures. Detailed methods and procedures are identified by the safety guidelines of the organization.

All these methods and procedures are implemented to fictitious model of municipality, which is connected to agendas governance systems. By implementation, we achieved a document that we can use to get clearance for our information system. Finally, we determined the general recommendations for risk management system in information systems, where we put the processes and methods for their implementation and future development of the information systems of public administration.

SEZNAM POUŽITÉ LITERATURY

[1] HROMÁDKA, Matěj. *Veřejná správa a její organizace*. Praha, 2008. Dostupné z: http://www.vsrr.cz/kestazeni/predmety/vs.pdf. Učební text. Vysoká škola regionálního rozvoje, s.r.o.

[2] ŠPAČEK, David. *Moderní principy veřejné správy a vyhodnocování její elektronizace*. Brno, 2007. Dostupné z: http://is.muni.cz/th/77120/esf_d/. Disertační práce. Masarykova univerzita, Ekonomicko-správní fakulta. Vedoucí práce Doc. JUDr. Ivan Malý, CSc.

[3] HALÁSKOVÁ, Matina. *Veřejná správa*. Ostrava, 2007. Dostupné z: http://projekty.osu.cz/pvsos/doc/verejna_sprava.pdf. Učební text. Ostravská univerzita, Pedagogická fakulta.

[3] HRONEK, Jiří. *Informační systémy*. Olomouc, 2007. Dostupné z: http://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf. Učební text. Univerzita Palackého, Přírodovědecká fakulta, Katedra informatiky.

[4] KUČEROVÁ, Helena. *Projektování informačních systémů*. 2007. Dostupné z: web.sks.cz/users/ku/DOKUMENTY/pri_syl.pdf. Sylaby ke kurzu. Vyšší odborná škola informačních služeb.

[5] *Informační systémy* [online]. Brno, 2009 [cit. 2013-06-01]. Dostupné z: https://akela.mendelu.cz/~rybicka/#prvni. Učební text. Mendelova univerzita v Brně.

[6] SVOBODA, Kamil. *Projektování informačních systémů* [online]. Hradec Králové, 2012 [cit. 2013-06-01]. Dostupné z: http://edu.uhk.cz/~simkomo1/OMO1/4/03_projektovani_tisk.pdf. Učební text. Univerzita Hradec Králové, Fakulta informatiky a managementu.

[7] ZIKMUND, Martin. *INFORMAČNÍ SYSTÉMY VE VEŘEJNÉ SPRÁVĚ* [online]. 2004[cit. 2013-06-01]. Dostupné z: http://www.parlament-vlada.cz/modules.php?name=News&file=article&sid=493

[8] ŠMÍD, Vladimír. *Informační systém veřejné správy a jeho vztah k ostatním informačním systémům* [online]. 2002[cit. 2013-06-01]. Dostupné z: http://www.fi.muni.cz/~smid

[9] E-Government – KIVS (6. díl) E-Government – KIVS (6. díl). ADVICE.CZ S.R.O. *www.ISVS.CZ* [online]. 2001 [cit. 2013-06-01]. Dostupné z: http://www.isvs.cz/e-government-kivs-6-dil/

[10] OECD. *The e-Government Imperative*. Francie, Paříž: OECD PUBLICATIONS, 2003. ISBN 92-64-10117-9.

[11] EGON jako symbol eGovernmentu - moderního, přátelského a efektivního úřadu. MINISTERSTVO VNITRA ČR. *Http://www.mvcr.cz* [online]. 2010 [cit. 2013-06-01]. Dostupné z: http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu-moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx?q=Y2hudW09Mg%3d%3d

[12] Komunikační infrastruktura veřejné správy. MINISTERSTVO VNITRA ČR. *Http://www.mvcr.cz* [online]. 2010 [cit. 2013-06-01]. Dostupné z: http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-komunikacni-infrastruktura-verejne-spravy.aspx

[13] DETAILNÍ ARCHITEKTURA ARES. In: *Integrace ARES se systémem ZR cz.1.06/1.1.00/07.06406*. 2011. Dostupné z: http://www2012.mfcr.cz/cps/rde/xbcr/mfcr/2011_Integrace_ARES_se_systemem_ZR-DA_pdf.pdf

[14] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy. MINISTERSTVO VNITRA ČR. *Http://www.mvcr.cz* [online]. 2010 [cit. 2013-06-01]. Dostupné z: http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx

[15] E-Government – Jak je to s legislativou? (2. díl). ADVICE.CZ S.R.O. *Www.ISVS.CZ* [online]. 2001 [cit. 2013-06-01]. Dostupné z: http://www.isvs.cz/e-government-jak-je-to-s-legislativou-2-dil/

[16] Co je a co není informační systém veřejné správy. In: *Komentář k zákonu č. 365/2000 Sb.* 2009. Dostupné z: http://www.mvcr.cz/soubor/co-je-a-co-neni-isvs.aspx

[17] VAŠÁKOVÁ, Lenka. *Dlouhodobé řízení ISVS*. Hradec Králové, 2013. Dostupné z: http://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C

DEQFjAA&url=http%3A%2F%2Fportal.kr-plzensky.cz%2Ffile.asp%3Fname%3D1004792070212173700.ppt%26folder%3D799&ei=-EmpUYXuF6eG4gS0q4HwBQ&usg=AFQjCNFkL8pS1ZxNZht-vFcUmc-IeQJM7g&sig2=1btKd-P7ODQljsDthgsaZA&bvm=bv.47244034,d.bGE&cad=rja. Legislativní opora. Ministerstvo informatiky České republiky.

[18] Metodický pokyn: Dlouhodobé řízení ISVS. In: *vyhl. č .529/2006*. 2007. Dostupné z: http://www.relsie.cz/stredisko/cenik/IO-MP-302-365-529-FIN-080423.pdf

[19] E-Government – Referenční rozhraní (5. díl). ADVICE.CZ S.R.O. *Www.ISVS.CZ* [online]. 2001 [cit. 2013-06-01]. Dostupné z: http://www.isvs.cz/e-government-referencni-rozhrani-5-dil/

[20] Atestace ISVS. EQUICA, a.s. *Www.equica.cz* [online]. 2013 [cit. 2013-06-01]. Dostupné z: http://www.equica.cz/atestace-isvs

[21] Atestační podmínky a postupy atestačního střediska při provádění atestací způsobilosti k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní. In: ELEKTROTECHNICKÝ ZKUŠEBNÍ ÚSTAV, 2008. Dostupné z: http://www.ezu.cz/file.php?type=file&disk_filename=file_126_GENERAL.pdf&filename=atestacni_postupy_ref_rozhrani.pdf&filetype=application/pdf

[22] Atestační podmínky a postupy atestačního střediska při provádění atestací dlouhodobého řízení informačních systémů veřejné správy. In: ELEKTROTECHNICKÝ ZKUŠEBNÍ ÚSTAV, 2009. Dostupné z: http://www.ezu.cz/file.php?type=file&disk_filename=file_335_GENERAL.pdf&filename=atestacni_postupy_dlouhodobe_rizeni.pdf&filetype=application/pdf

[23] JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2006, 140 s. ISBN 80-7318-456-7.

[24] LUDVÍK, Miroslav. *Teorie bezpečnosti počítačových sítí*. Praha: Computer Media, 2008. ISBN 80-86686-35-3.

[25] THOMAS, Thomas M. *Zabezpecení pocítacových sítí bez predchozích znalostí*. 1. vyd. Brno: CP Books, 2005. ISBN 80-251-0417-6.

[26] MALANÍK D., *Význam fyzického zabezpečení IT systémů*. Security Revue, 2010. ISSN 1336-9717.

[27] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 8073180952.

[28] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Praha: Computer Press, 2004. ISBN 8025101061.

[29] Provozní dokumentace ISVS: Pravidla provozní dokumentace. In: Městská část Praha 1, 2008. Dostupné z: http://www.praha1.cz/cps/media/P1_INFOK_Priloha_2.pdf

[30] Komentář k vyhlášce č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy Verze. In: Ministerstvo vnitra ČR, 2009. Dostupné z: http://www.mvcr.cz/soubor/komentar-k-vyhlasce-c-529-2006-sb-o-pozadavcich-na-strukturu-a-obsah-informacni-koncepce-a-provozni-dokumentace-a-o-pozadavcich-na-rizeni-bezpecnosti-a-kvality-informacnich-systemu-verejne-spravy.aspx

[31] VLČEK, Pavel. *NÁVRH INFORMAČNÍHO SYSTÉMU VEŘEJNÉ SPRÁVY*. Ostrava, 2004. Dostupné z: http://formular-ekf.vsb.cz/formulare/f01/tsw/getfile.php?prispevekid=745. Seminární práce. VŠB-TU Ostrava, Ekonomická fakulta, katedra informatiky v ekonomice.

[32] Národní strategie informační bezpečnosti ČR z pohledu veřejné. ADVICE.CZ S.R.O. *Www.ISVS.CZ* [online]. 2001 [cit. 2013-06-01]. Dostupné z: http://www.isvs.cz/narodni-strategie-informacni-bezpecnosti-cr-z-pohledu-verejne-spravy/

[33] BALCAR, Štěpán. *Bezpečnostní audit IS*. Brno, 2007. Dostupné z: http://formular-ekf.vsb.cz/formulare/f01/tsw/getfile.php?prispevekid=745. Diplomová práce. Masarykova univerzita, Fakulta informatiky.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Přístupové systémy
AIFO	Agendový identifikátor fyzické osoby
AIS	Agendový informační systém
ATS	Atestace
BP	Bezpečnostní politika
CCTV	Uzavřené televizní okruhy
DOS	Denial of service - Odmítnutí služby
DSS	Decision Support System
EDI	Electronic Data Interchange - Komunikace s okolím
EIS	Executive Information System - Strategické řízení podniku
EPS	Elektronické požární systémy
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IK	Informační koncepce
IKS	Informační a komunikační systém
IS	Informační systém
ISVS	Informační systém veřejné správy
ISZR	Informační systém základních registrů
KIVS	Komunikační infrastruktura veřejné správy
KMS	Knowledge Management System
KÚ	Krajský úřad
MěÚ	Městský úřad
MIS	Management Infromation System - Taktické řízení podniku
MV	Ministerstvo vnitra ČR

MZS	Mechanické zábranné systémy
OECD	The Organisation for Economic Co-operation and Development
OIS	Office Information System - Kancelářské systémy
ORG	Systém zajišťující ochranu osobních uložených v základních registrech.
PD	Provozní dokumentace
PZTS	Poplachové zabezpečovací a tísňové systémy
ROB	Základní registr obyvatel
ROS	Základní registr osob
RPP	Základní registr agend orgánů veřejné moci a některých práv a povinností
RUIAN	Základní registr územní identifikace, adres a nemovitostí
SW	Software
TPS	Trasaction Procesing Systém - Operativní řízení podniku
VS	Veřejná správa
ZIFO	Zdrojový identifikátor fyzické osoby

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ŽÁDOST O ATESTACI

Elektrotechnický zkušební ústav, s.p.
Atestační středisko pověřené Ministerstvem vnitra ČR
Registrační č. 02 ze dne 27.ledna 2009
Pod Lisem 129, 171 02 Praha 8 - Troja
tel.: 266104213, 266104111, fax: 284680070, 2846800037
e-mail: msedlacek@ezu.cz

ŽÁDOST O ATESTACI

1. **Název a adresa žadatele**:

   .....

   .....

   PSČ: .....

   Telefon č.: ..... Fax č.: .....

   IČO: ..... DIČ: .....

2. **Kontaktní osoba pro atestační řízení** / funkce:

   .....

   E-mail: ..... Telefon č.: .....

3. **Plný název předmětu atestace**:

   .....

   .....

4. **Stručný popis předmětu atestace a jeho účel:**

   .....

   .....

5. **Požadovaný druh atestace:**

   Stanovení shody dlouhodobého řízení informačních systémů veřejné správy s požadavky zákona č.365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

.....
Datum

.....
Podpis statutárního zástupce

PŘÍLOHA P II: ANALÝZA RIZIK – SÍŤOVÝ SERVER

Aktivum: : Síťový server
Hrozba: TH01 Chyba provozu
Dopad: Z08 Nedostupnost 1 T - A03 Nízká, hodnota 100 - 300 tis.Kč
Míra rizika: **Vysoká** (Úhrnná míra rizika = 3)
Účinnost stávajících protiopatření: C5 Výborná více než 90%
Protiopatření:
A.10 Řízení komunikací a řízení provozu
A.10.1 Provozní postupy a odpovědnosti
A.10.1.1 Dokumentace provozních postupů
A.10.1.1.1 Provozní postupy musí zahrnovat kompletní sadu provozních instrukcí pro každou aplikaci.
A.10.1.1.2 Provozní postupy musí zahrnovat postupy pro zacházení a hospodaření s médii.
A.10.1.1.3 Provozní postupy musí být rozděleny v souladu s pracovními funkcemi.
A.10.1.1.4 Provozní postupy musí být aktualizovány v souladu se změnami aplikací.
A.10.1.1.5 Popisy pracovních postupů mají být bezpečně uloženy.
A.10.1.1.6 Evidence zpracování musí být ukládána do trvalého souboru.
A.10.1.1.7 Má být zaznamenáván čas spuštění a ukončení činnosti systému.
A.10.1.1.8 Mají být zaznamenávány systémové chyby a činností, které byly učiněny při jejich nápravě.
A.10.1.1.9 Mají být zaznamenávána jména osob, které vstoupily do evidenčních záznamů.
A.10.1.1.10 Závady musí být zaznamenány a musí být provedeny činnosti vedoucí k jejich nápravě.
A.10.1.2 Řízení změn
A.10.1.2.1 Musí být identifikovány důležité změny IT zařízení .
A.10.1.2.2 Změny IT zařízení musí být zaznamenány do registru změn.
A.10.1.2.3 Pro navrhované změny ITmusí být získán souhlas.
A.10.1.2.4 Pro případ neúspěšné změny musí být zajištěna možnost návratu do původního stavu.
A.10.1.2.5 Musí být zkontrolováno, zda změny IT nemají dopad na bezpečnost.
A.10.1.3 Oddělení povinností
A.10.1.3.1 Pro minimalizaci příležitostí zneužití systému personálem má být provedeno udržování oddělení povinností.
A.10.1.3.7 Proti přítomnosti pouze jediného administrátora má být použito pravidlo "dvou osob".
A.10.1.3.8 Provozní činnost musí být monitorována.
A.10.1.4 Oddělení vývoje, testování a provozu
A.10.2 Řízení dodávek služeb třetích stran
A.10.2.1 Dodávky služeb
A.10.2.1.1 Pozornost má být věnována všem citlivým a kritickým aplikacím, které je bezpečnější udržovat vlastními prostředky.
A.10.2.1.2 Má být získán souhlas od garantů aplikací organizace.
A.10.2.1.3 Ve smlouvě se společností, která zajišťuje externí správu zařízení, mají být stanoveny bezpečnostní standardy.
A.10.2.1.4 Ve smlouvě mají být stanoveny procedury pro monitorování bezpečnostních činností.
A.10.2.1.5 Ve smlouvě o správě mají být jasně určeny termíny.

A.10.2.1.6 Pro stěhování nebo přesun zařízení mají být stanoveny přesné postupy .

A.10.2.1.7 Všechny práce v rámci správy mají být zdokumentovány.

A.10.2.1.8 Plánovaná údržba nemá zasahovat do ostrého zpracování.

A.10.2.1.9 Má být kontrolována vzdálená správa.

A.10.2.1.10 Nemá být povoleno odnášet žádné zařízení umožňující archivovat.

A.10.2.1.11 Vzdálená správa má být zakázána.

A.10.2.2 Monitorování a přezkoumávání služeb třetích stran

A.10.2.3 Řízení změn služeb poskytovaných třetími stranami

A.10.3 Plánování a přejímání systémů

A.10.3.1 Řízení kapacit

A.10.3.1.1 Má být analyzována přiměřená rychlost procesoru počítače.

A.10.3.1.2 Má být analyzováno odpovídající uložení dat.

A.10.3.1.3 Má být analyzováno používání V/V zařízení.

A.10.3.1.4 Má být analyzováno časové rozvržení transakcí.

A.10.3.1.5 Pro účtovací/auditní soubory má být zajištěn dostatečný prostor.

A.10.3.1.6 Mají být stanoveny trendy použití a růstu infrastruktury.

A.10.3.1.7 Musí být sledovány současné a odhadovány budoucí požadavky na personál.

A.10.3.1.8 Musí být sledovány současné a odhadovány budoucí požadavky na prostory.

A.10.3.1.9 Musí být sledovány současné a odhadovány budoucí požadavky na zařízení a zásoby.

A.10.3.1.10 Nástroje na monitorování systému mají sledovat využívání kapacity médií, CPU, vstupů/výstupů, kapacity sítě.

A.10.3.1.11 Nástroje na monitorování systému mají generovat přímé alarmy, které upozorní na možnost výskytu problémů při dosažení nebo překročení určené meze kapacity.

A.10.3.2 Přejímání systémů

A.10.3.2.1 Požadavky a kritéria akceptace nového systému mají být jednoznačně vymezena, odsouhlasena, zdokumentována a otestována.

A.10.3.2.2 Mají být stanoveny výkonnostní a kapacitní požadavky na bezpečnost systému, včetně odpovídajících testů.

A.10.3.2.3 Testy mají zahrnovat testování bezpečnostních funkcí.

A.10.3.2.4 Mají být stanoveny testy, určena data potřebná pro testy a odhadnuty předpokládané výsledky testů.

A.10.3.2.5 Mají být vytvořeny plány testování.

A.10.3.2.6 Testování má být prováděno podle sady standardních bezpečnostních testů.

A.10.3.2.7 Po uvedení systému do provozu mají být bezpečnostní kontroly prováděny nejméně jednou za šest měsíců.

A.10.3.2.8 Pro provádění kontroly mají být použity automatizované nástroje zaznamenávající stav a konfiguraci bezpečnostních funkcí.

A.10.6 Správa bezpečnosti sítě

A.10.6.1 Síťová opatření

A.10.6.1.1 Veškeré prvky sítě musí být zahrnuty mezi aktiva organizace.

A.10.6.1.2 Má být zdokumentována logická struktura sítě.

A.10.6.1.3 Použití systému správy sítě má být povoleno pouze autorizovanému personálu.

A.10.6.1.4 Stav sítě musí být aktivně řízen.

A.10.6.1.5 Mají být zaznamenávány síťové chyby.

A.10.6.1.6 Události mají být Inteligentně filtrovány.

A.10.6.1.7 Musí být udržována přesná evidence prvků sítě.

A.10.6.1.8 Síť musí být odolná vůči selhání jednotlivých komponent.

A.10.6.1.9 Má být navržena odolná sít.

A.10.6.1.10 Když není možné zajistit redundanci, mají být síťová zařízení osazena

prvky s vysokou odolností vůči selhání.

A.10.6.1.11 Dostupnost každého síťového zařízení má být monitorována.

A.10.6.1.12 Dostupnost každé síťové linky má být monitorována.

A.10.6.1.29 Odpovědnost za provoz sítě má být oddělena od provozu počítačů.

A.10.6.1.30 Mají být určeny odpovědnosti za správu zařízení, která se nenachází v prostorách organizace, a to včetně zařízení, která jsou umístěna u uživatelů.

A.10.6.1.31 Správa sítě má zahrnovat udržování nepoškozené kopie všech zpráv.

A.10.6.1.32 Správa sítě má zahrnovat ochranu řídicích dat sítě před poškozením.

A.10.6.1.33 Správa sítě má zahrnovat zajištění systému pro řízení sítě.

A.10.10 Monitorování

A.10.10.1 Pořizování auditních záznamů

A.10.10.1.1 Má být monitorována práce administrátora pomocí evidence (logování) činností v systému.

A.10.10.1.2 Provozní personál má být informován, že jeho činnost je monitorována.

A.10.10.1.3 Evidenční záznamy se mají soustavně monitorovat.

A.10.10.1.4 Rozsah zaznamenávaných dat musí být nastavitelný.

A.10.10.1.5 Mají se zaznamenávat všechny změny souborů.

A.10.10.1.6 Má se zaznamenávat časový údaj o prohlížení souborů.

A.10.10.1.7 Má se zaznamenávat každý tiskový výstup.

A.10.10.1.8 Mají být monitorovány známé skryté kanály.

A.10.10.2 Monitorování používání systému

A.10.10.2.1 Mají být monitorovány bezpečnostní incidenty a výjimky.

A.10.10.2.2 Kontrakt se smluvním poskytovatelem služeb musí vymezovat bezpečnostní parametry každé síťové služby.

A.10.10.2.3 Musí být pravidelně prováděny nezávislé audity a revize.

A.10.10.2.4 Mají být použity mechanismy pro detekci a hlášení závad sítě.

A.10.10.2.5 Má být veden záznam všech chyb v síti.

A.10.10.2.6 Všichni uživatelé elektronické pošty mají být seznámeni s tím, co je považováno za neautorizované použití elektronické pošty.

A.10.10.2.7 Elektronická pošta musí být prohledávána, zda nedochází k porušování pravidel pro její použití.

A.10.10.2.8 Má být udržován seznam neautorizovaných slov.

A.10.10.2.9 Uživatelé musí být informováni o možných nebezpečích spojených s použitím elektronické pošty a k ní připojených souborů.

A.10.10.2.10 Klienti elektronické pošty nemají automaticky otvírat připojené soubory.

A.10.10.2.11 Všichni uživatelé musí být informováni o tom, že prostředky pro prohlížení webových stránek musí být využívány pouze pro schválené účely.

A.10.10.2.12 Uživatelé musí být informováni, že prohlížení WWW může být monitorováno.

A.10.10.2.13 Má být jmenována osoba zodpovědná za kontrolu pokusů o přístup k webovým místům, která jsou vedena jako neautorizovaná.

A.10.10.2.14 Mají být stanoveny kázeňské postihy pro případy neautorizovaného použití prostředků pro prohlížení WWW.

A.10.10.2.15 Pro řízení chodu sítě mají být zaznamenávány postupy všech zásahů na síti.

A.10.10.2.16 Musí existovat dostatečné prostředky pro analýzu účtovacích záznamů.

A.10.10.3 Ochrana vytvořených záznamů

A.10.10.3.1 Přístupová práva k auditnímu deníku mají být nastavena tak, aby záznam směl měnit pouze bezpečnostní správce systému.

A.10.10.3.2 Přístupová práva k auditnímu deníku mají být nastavena tak, aby záznam směl prohlížet pouze bezpečnostní správce systému.

A.10.10.3.3 Z důvodů možného vyšetřování by musí být evidenční deník archivován.

A.10.10.3.4 Fyzický přístup ke kopii evidenčního deníku musí být omezen na osoby, kterým nejsou přidělena práva správy systému.

A.10.10.3.5 Systémová opatření pro kontrolu integrity musí zaručit úspěšnou archivaci evidenčního deníku.

A.10.10.3.6 Když účtovací záznam dosáhne 75% své maximální povolené velikosti, má být tento stav ohlášen.

A.10.10.3.7 Když je účtovací záznam plný, systém má být zastaven.

A.10.10.4 Administrátorský a operátorský deník

A.10.10.4.1 Systémové účtování musí být prováděno důvěryhodným zařízením.

A.10.10.4.2 Pro činnost správy se mají používat samostatné účty.

A.10.10.4.3 Všechny operace mají být účtovány.

A.10.10.4.4 Všechny pokusy o zásahy do účtovacích souborů (zápis, výmaz, změna) mají být zaznamenány.

A.10.10.4.5 Mají být zaznamenány všechny operace podléhající pravidlu "dvou osob".

A.10.10.5 Záznam selhání

A.10.10.5.1 Musí být monitorována intenzita síťového provozu.

A.10.10.5.2 Má být prováděno monitorování klíčových přepínačů/uzlů.

A.10.10.5.3 Musí být definovány události, které mají podléhat prošetřování.

A.10.10.5.4 Má být provedena analýza počtu neúspěšných přihlášení.

A.10.10.5.5 Má být provedena analýza přidělování privilegovaných účtů.

A.10.10.5.6 Má být provedena analýza odepření přístupu.

A.10.10.5.7 Má být provedena analýza trendu počtu úspěšných přihlášení.

A.10.10.5.8 Musí být stanovena časová perioda analýzy záznamu o účtu.

A.10.10.6 Synchronizace hodin

A.11 Řízení přístupu

A.11.2 Řízení přístupu uživatelů

A.11.2.2 Řízení privilegovaného přístupu

A.11.2.2.1 Mají být určeny kategorie personálu, kterým mají být privilegia přidělena.

A.11.2.2.2 Přidělování privilegií má být prováděno na základě zásady "oprávněné potřeby".

A.11.2.2.3 O všech privilegiích, která byla přidělena, musí být vedena evidence.

A.11.2.2.4 Řízení přístupu k účtům správce má zajišťovat, že znalost hesel účtů systémového správce bude omezena na autorizované správce systému.

A.11.2.2.5 Kopie hesel účtů systémového správce má být bezpečně uložena.

A.11.2.2.6 Heslo systémového správce má být měněno častěji než heslo obyčejného uživatele.

A.11.2.2.7 Při použití jednoho účtu systémového správce má být každý autorizovaný správce systému jednoznačně identifikován.

A.11.2.2.8 Znalost každého hesla systémového správce má být omezena na jedinou osobu.

A.11.2.2.9 Řízení přístupu k účtům správce má zajišťovat tisk nepřetržitého záznamu všech příkazů, které byly zadány z účtu systémového správce.

A.11.2.2.10 Volné použití "silných" systémových utilit má podléhat speciálnímu schválení.

A.11.4 Řízení přístupu k síti

A.11.4.1 Politika užívání síťových služeb

A.11.4.1.1 Identifikační a autentizační informace uživatele mají být šifrovány.

A.11.4.1.2 Informace musí být před přenosem zašifrovány.

A.11.4.1.3 Aplikace se musí systému identifikovat.

A.11.4.1.4 Pro každou aplikaci má být použit jedinečný identifikátor.

A.11.4.1.5 Aplikace se musí autentizovat "bezpečním procesem".

A.11.4.1.6 Musí být vytvořeny směrnice pro používání sítí a síťových služeb.

A.11.4.1.7 Směrnice mají vymezovat sítě a síťové služby, ke kterým je povolen přístup .

A.11.4.1.8 Mají být vypracovány autorizační postupy, které stanoví, komu je přístup k síti a síťovým službám povolen.

A.11.4.1.9 Pro ochranu přístupu k síťovým spojům mají být vytvořeny kontrolní opatření a procedury.

A.11.4.1.10 Koncoví uživatelé musí mít přístup jen k těm síťovým prostředkům, které potřebují pro svou práci.

A.11.4.1.11 Síť musí mít definované hranice a známé uživatele a služby.

A.11.4.1.12 Musí existovat pokyny pro řízení přístupu přes bezpečnostní brány.

A.11.4.1.13 Pro použití elektronické pošty musí být připravena jasná bezpečnostní politika.

A.11.4.1.14 Bezpečnostní politika má upozornit na ochranu souborů připojených ke zprávám elektronické pošty.

A.11.4.1.15 Bezpečnostní politika má obsahovat směrnice pro případy, kdy nelze využít elektronickou poštu.

A.11.4.1.16 Bezpečnostní politika má obsahovat požadavky na využití kryptografických technik pro ochranu důvěrnosti a integrity elektronických zpráv.

A.11.5.4 Použití systémových nástrojů

A.12 Akvizice, vývoj a údržba informačních systémů

A.12.5 Bezpečnost procesů vývoje a podpory

A.12.5.2 Technické přezkoumání aplikací po změnách operačního systému

A.12.5.2.1 Změny v operačním systému musí být autorizovány.

A.12.5.2.2 Změny v operačním systému mají procházet přes procedury řízení změn programového vybavení.

A.12.5.2.3 Pro autorizaci změn v operačním systému se má udržovat kontrola nad nástroji pro realizaci aktualizace programového vybavení.

A.12.5.2.4 Bezpečnostní dopad změny v operačním systému musí být analyzován.

A.12.6 Řízení technických zranitelností

A.12.6.1 Řízení, správa a kontrola technických zranitelností

A.12.6.1.1 Musí být kontrolována konfigurace síťových zařízení, zda neobsahuje zranitelná místa.

A.12.6.1.2 Měly by být vyhodnoceny informace o technických zranitelnostech informačních systémů.

A.12.6.1.3 Záplaty (opravné programové balíčky, patch) musí být otestovány a vyhodnoceny před jejich instalací.

A.12.6.1.4 Všechny modemy musí být autorizovány.

A.12.6.1.5 Mají být omezena uživatelská práva k instalování zařízení.

A.12.6.1.6 Má být kontrolována odchozí komunikace, zda neobsahuje známky neautorizované činnosti. (Může být nutné brát v úvahu šifrovanou komunikaci).

A.12.6.1.7 Když je zjištěna podezřelá událost, má být vyhlášen poplach.

A.12.6.1.8 Relace, v nichž se objeví podezřelé aktivity, mají být ukončeny, pokud není rozhodnuto, že budou pouze monitorovány.

A.12.6.1.9 Směrovače mají být nakonfigurovány tak, aby automaticky zablokovaly podezřelé činnosti, které překročily nastavené hodnoty.

A.12.6.1.10 Systém na detekci průniků má být schopen odhalit i útoky, které byly provedeny mírně modifikovaným postupem oproti známé metodě útoku.

A.12.6.1.11 Má být prováděna automatizovaná prověrka serverů, zda je není možné využít jako východisko pro škodlivé útoky nebo pro zavádění "trojských koní".

A.12.6.1.12 Pro detekci nelegálních aktivit a k jejich navádění mají být vytvořeny fiktivní podsítě.

A.14 Řízení kontinuity činností organizace

A.14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

A.14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace

A.14.1.1.1 Musí být připraveny plány zajištění nepřetržitosti provozu.

A.14.1.1.2 Musí být připraven plán krizového řízení.

A.14.1.1.3 V rámci krizového plánu musí být jmenována osoba, která je odpovědná za řízení při krizové situaci včetně odpovědností.

A.14.1.1.4 Krizový plán musí obsahovat popis činností, které musí být prováděny k rozpoznání krizové situace.

A.14.1.1.5 V rámci krizového plánu musí být jmenována osoba, která má pravomoc zahájit řízení podle krizového plánu.

A.14.1.1.6 Krizový plán musí obsahovat organizační schéma pro vydávání příkazů v době krizové situace.

A.14.1.1.7 Krizový plán musí obsahovat popis způsobu komunikace mezi lidmi, kteří se podílejí na zvládnutí krizové situace.

A.14.1.2 Kontinuita činností organizace a hodnocení rizik

A.14.1.2.1 Mají být identifikována rizika, která mohou způsobit narušení chodu organizace.

A.14.1.2.2 Má být provedeno ohodnocení dopadů jednotlivých rizik.

A.14.1.2.3 Ohodnocení rizik má zahrnovat všechny procesy organizace.

A.14.1.2.4 Strategie kontinuity na vysoké úrovni má být schválena vyšším managementem.

A.14.1.3 Vytváření a implementace plánů kontinuity

A.14.1.3.1 Plány mají identifikovat zapojení osob a jejich odpovědnost při procesu obnovy.

A.14.1.3.2 Nouzové procedury mají dovolit zotavení a obnovení chodu v požadovaném čase.

A.14.1.3.3 Mají být identifikovány vnější závislosti organizace.

A.14.1.3.4 Pro vnější závislosti organizace mají existovat smlouvy.

A.14.1.3.5 Nouzové procedury a procesy mají být zdokumentovány.

A.14.1.4 Systém plánování kontinuity činností organizace

A.14.1.5 Testování, udržování a přezkoumávání plánů kontinuity

A.14.1.5.1 Plány kontinuity činností organizace musí být předmětem pravidelných testů.

Legenda

Aktivum: cokoli, co má pro organizaci hodnotu
Hrozba: potenciální příčina nežádoucího incidentu
Dopad: následek nežádoucího incidentu
Riziko: potenciální možnost, že daná hrozba využije zranitelnosti a způsobí tak ztrátu
Protiopatření: praxe, postup, mechanismus, který snižuje riziko