Univerzita Hradec Králové
Fakulta informatiky a managementu

# Implementace kybernetické bezpečnosti a normy ISO 27000 ve státní správě

## Diplomová práce

Jan Píša duben 2015

Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

# Implementace kybernetické bezpečnosti a normy ISO 27000 ve státní správě
# Diplomová práce

Autor: Jan Píša
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové duben 2015

**Prohlášení:**

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne Jan Píša

**Poděkování:**
Děkuji vedoucímu práce Mgr. Josefu Horálkovi, Ph.D. za rady, připomínky, odbornou pomoc a poskytnutí podkladů k dokončení práce.

**Anotace**

Cílem diplomové práce je představit principy kybernetické bezpečnosti, vycházející z norem řady ISO 27000. Jelikož nabyl od 1. ledna 2015 účinnosti Zákon o kybernetické bezpečnosti, bude celá problematika řešena s ohledem na tento zákon. Výsledkem diplomové práce bude analýza zkoumaného prostředí s důrazem na fyzickou bezpečnost objektu a síťové infrastruktury. V návaznosti na analýzu bezpečnosti síťové infrastruktury bude navrženo a implementováno vybrané technické opatření pro ochranu fyzické a linkové vrstvy ISO/OSI modelu.

**Annotation**

**Title: Implementation of cybersecurity and ISO27000 standards in government**

The aim of Diploma thesis is to introduce the principles of cybersecurity, based on the standards of ISO 27000. Because of the new law aiming on cybersecurity, which came into effect on 1st January 2015, all the entire issue will be solved with regard to this law. The result of this thesis is the analysis of the examined enviroment, with emphasis on the physical security of the building and network infrastructure. Following the analysis of the network infrastructure security, there will be designed and implemented selected technical measures to protect the physical and data link layer of ISO/OSI model.

# Obsah

# Úvod

Dne 1. ledna 2015 vešel v platnost nový Zákon o kybernetické bezpečnosti, který se dotýká některých soukromých organizací, ale také organizací státní správy. Tyto subjekty mají za povinnost do konce roku 2015 splnit podmínky, které jim tento zákon nařizuje. Cílem této diplomové práce je provést analýzu povinností subjektů státní správy v souvislosti s tímto zákonem. Autor bude vycházet z informací a nařízení, která jsou zákonem předepsána, čerpat bude i z příslušných prováděcí právních předpisů (vyhlášek).

V teoretické části diplomové práce se autor zaměří na rodinu norem ISO/IEC 27000 a její jednotlivé části. Tyto normy jsou současným etalonem pro posuzování implementace ISMS a Zákon o kybernetické bezpečnosti z nich vychází. Podrobně budou analyzovány normy ISO/IEC 27000, 27001 a 27002. Dále autor vysvětlí principy frameworku COBIT, ze kterého tvůrci Zákona o kybernetické bezpečnosti také vycházeli. COBIT se na problematiku bezpečnosti zaměřuje z globálního hlediska organizace, proto autor shrne nejvíce patrné rozdíly mezi tímto frameworkem a ISO/IEC 27000. Následně bude autor analyzovat Zákon o kybernetické bezpečnosti. Bude představen důvod vzniku tohoto zákona, jeho historie a základní principy. Podrobněji budou vysvětleny důležité pojmy, které mají přesnou definici, a je tedy nezbytné jim porozumět. Budou vymezeny stěžejní body zákona, které musí všechny povinné subjekty dodržovat a budou představena bezpečnostní opatření dle jednotlivých paragrafů zákona.

V praktické části diplomové práce autor využije všech nabytých znalostí z teoretické části ke krátké analýze prostředí, ve kterém pracuje. Bude vysvětlena problematika fyzické bezpečnosti, základní pojmy a oblasti, které do ní spadají. Autor se pokusí odhalit slabá místa zabezpečení objektu organizace, ve které pracuje a navrhnout řešení, které přispěje ke zlepšení tohoto zabezpečení. Využívat bude znalostí, které nabyde studiem problematiky při psaní této práce a zkušeností, které doposud získal. Tyto využije také pro analýzu sítě, u které se zaměří na fyzickou a linkovou vrstvu modelu ISO/OSI. Nakonec práce navrhne možné opatření, které zvýší bezpečností sítě a bude splňovat požadavky Zákona o kybernetické bezpečnosti. Budou analyzovány silné a slabé stránky tohoto opatření, které budou zjištěny během jeho implementace a testovacího provozu, který by měl potvrdit znalosti a zkušenosti, které budou vypracováním této práce získány.

# 1 Řada norem ISO / IEC 27000 a ISMS

V této kapitole bude stručně představen pojem ISMS, historie řady norem ISO / IEC 27000. Dále budou představeny jednotlivé normy, důležité pojmy a principy.

## 1.1 ISMS

ISMS je zkratkou anglického slovního spojení Information Security Management System, což je do češtiny překládáno jako Systém řízení bezpečnosti informací. Jedná se o soubor nástrojů, požadavků a doporučení. Aby byla zajištěna informační bezpečnost všech hmotných či nehmotných aktiv, je nezbytné, aby všechny tyto nástroje byly správně využívány. Zároveň je nutné předem definovat úroveň bezpečnosti tak, aby byla přijatelná pro organizaci a odpovídala povaze aktiv a nákladům, které je organizace ochotna nebo musí na ochranu aktiv investovat. *(GiTy a.s., 2008)*

S postupným rozvojem informačních technologií se výrazným způsobem začala zkracovat doba, která je nezbytná pro předání informace. V současné době je možné obdržet jakoukoliv informaci prakticky okamžitě a to po celém světě a je tudíž nezbytné všechny cenné informace ochraňovat takovým způsobem, aby nebyly poskytnuty neoprávněným subjektům. Tato praxe nebyla v počátcích uplatňována, jelikož si nikdo neuvědomoval rizika, která jsou dána principy komunikace například po celosvětové síti Internet. Postupem času byly definovány postupy, jak s cennými informacemi zacházet a jak je chránit. Nezbytnou součástí začalo být monitorování prostředí, po kterém se aktiva přenášejí a také předem specifikovaný postup a reakce v případě, že dojde k narušení bezpečnosti aktiv. Také proto je ISMS často spojován hlavně s informačními technologiemi, přestože se se týká i dalších oblastí.

### 1.1.1 Informace

Informace představují aktivum, které je podstatné pro činnost organizace a vyžaduje odpovídající ochranu. Může být uchováváno v mnoha formách, a to v digitální formě, materiální formě nebo jako nevyjádřené informace ve formě znalostí zaměstnanců. Všechny způsoby, kterými mohou být informace přenášeny (např. elektronicky, kurýrem nebo verbálně), vyžadují vždy přiměřenou ochranu. *(ČSN ISO/IEC27000, 2014, s. 19)*

### 1.1.2 Bezpečnost informací

Mezi hlavní aspekty bezpečnosti informaci patří důvěrnost, dostupnost a integrita. Aby byly minimalizovány dopady incidentů na bezpečnost informací a byl tak zajištěn úspěch a kontinuita činnosti organizace, je nezbytné užití a řízení vhodných opatření bezpečnosti informací, které budou zahrnovat široký rozsah hrozeb. *(ČSN ISO/IEC27000, 2014, s. 19)*

### 1.1.3 Systém řízení

Systém řízení užívá k dosažení cílů organizace rámec zdrojů. Zahrnuje organizační strukturu, politiky, plánovací činnost, odpovědnosti, praktiky, postupy, procesy a zdroje. V oblasti bezpečnosti informací umožňuje systém řízení

a) uspokojovat požadavky zákazníků a dalších zúčastněných stran na bezpečnost informací
b) zlepšovat plány a činnosti organizace
c) splňovat cíle bezpečnosti informací organizace
d) vyhovovat předpisům, legislativě a oborovým normám
e) řídit informační aktiva organizovaně a tak usnadnit neustálé zlepšování a úpravy ve vztahu ke stávajícím cílům organizace

*(ČSN ISO/IEC27000, 2014, s. 19)*

### 1.1.4 Procesní přístup

Efektivní a účinné fungování organizací je možné zajistit pouze v případě, že bude identifikováno a řízeno mnoho činností. Aby byla umožněna přeměna vstupů na výstupy pomocí nějakého procesu, je nezbytné prováděnou činnost řídit. Řízením taktéž umožníme použití výstupu z jednoho procesu jako vstupu procesu druhého. Tuto aplikaci systému procesů uvnitř organizace nazýváme procesní přístup. *(ČSN ISO/IEC27000, 2014, s. 19)*

## 1.2 Historie ISO/IEC 27000

Jak již bylo v kapitole 2 vysvětleno, ISO / IEC 27000 není jedna norma, ale je to celá řada (soubor) norem, která se neustále rozrůstá a reviduje dle aktuálních praktik a doporučení. ISMS je úzce spjat s normami ISO / IEC 27001 a 27002. Tyto normy vznikly zhruba 13 let poté, co Britské Ministerstvo průmyslu a obchodu (DTI) vydalo

v roce 1992 „Kodex pro řízení bezpečnosti informací“. Tento kodex byl v roce 1995 revidován Britským Standardizačním Institutem (BSI) a vydán jako formální standard pod označením BS7799. Zanedlouho po vydání BS7799 se objevuje první nástroj – COBRA, který má umožnit podporu a dodržování tohoto standardu. Tento nástroj je neustále vyvíjen, ale v současné době prochází procesem kompletního přepracování a není dočasně k dispozici.

V roce 1998 vydává BSI další dokument – Specifikace systému řízení bezpečnosti informací – pod označením BS7799-2, původní dokument BS7799 je přeznačen jako BS7799-1. O rok později je zveřejněna první revize BS7799-1 a prvními certifikačními orgány se stávají BSI a LRQA (Lloyd's Register Quality Assurance). Rok 2000 je důležitým milníkem. Z britského standardu BS7799-1 vzniká norma ISO / IEC 17799, která je do roku 2005 několikrát revidována. Ve stejném roce je původní britský standard BS7799-2 převzat jako ISO / IEC 27001. V roce 2007 je přejmenována norma ISO / IEC 17799 na ISO / IEC 27002, aby bylo možné lépe sladit systém číslování této řady norem. Od tohoto roku dochází zároveň k postupnému vydávání norem řady ISO / IEC 27000, kterých je k době psaní této práce celkem 25 a dalších cca 11 je v přípravě. Na základě standardu “ISO Guide 83”, publikovaného v dubnu 2012, mají všechny standardy řady 27000 definovanou jednotnou strukturu a pravidla pro začlenění specifických požadavků. *(The ISO 27000 Directory, 2007)*

## 1.3 ISO/IEC 27000

Číslovací řada 27000 norem ISO/IEC byla rezervována pro záležitosti, které se týkají informační bezpečnosti. Tato celá řada byla vybrána z důvodu, aby vznikl ucelený soubor, obdobný s dalšími důležitými řadami norem, jako jsou například ISO 9000 pro řízení jakosti nebo ISO 14000 pro řízení ochrany životního prostředí. Pro úplnost informací je nezbytné ještě osvětlit zkratky ISO a IEC, které se vyskytují v názvu.

IEC je mezinárodní elektrotechnická komise. Jedná se o neziskovou organizaci, sídlící v Ženevě, která vyvíjí a publikuje standardy, které se týkají elektrických technologií. Její standardy jsou dodržovány ve více než 150 zemích světa. Jedná se o přední světovou standardizační organizaci, která ve svém oboru hraje klíčovou úlohu při koordinaci snahy

jednotlivých zemí o sjednocení měření a standardizace moderní formy metrického systému. *(ANSI, ©2015a)*

ISO je mezinárodní organizace pro normalizaci. Stejně jako u IEC se jedná o neziskovou organizaci. ISO vyvíjí a publikuje standardy širokého spektra zaměření. Počínaje normami pro dynamiku tekutin, přes normy pro informační technologie, konče normami pro jadernou energii. Sídlo organizace je taktéž v Ženevě, ale celá organizace se skládá ze 162 členů, z nichž každý je výhradní zástupce pro zemi, ve které sídlí. ISO je největší vývojář a vydavatel norem na světě a plní tak zásadní úlohu sprostředkovatele dohod mezi jednotlivými vývojáři standardů. *(ANSI, ©2015b)*

Společně tvoří ISO a IEC specializovaný systém celosvětové organizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících národních orgánů.

ISO/IEC 27001 vypracovala společná technická komise ISO/IEC JTC1 Informační technologie, subkomise SC 27 IT Bezpečnostní techniky.

*(ISO 27000, 2014, s. 5)*

Řada mezinárodních norem, která má pomoci organizacím se zavedením a provozem ISMS sestává z konkrétních norem, uvedených v následující tabulce:

**Tabulka 1 - rodina norem ISO27000 (zdroj: zpracováno dle (RAC s r.o.))**

| | |
|---|---|
| ISO 27000 | Definuje pojmy a terminologický slovník pro všechny ostatní normy z této série. |
| ISO 27001 | hlavní norma pro Systém řízení bezpečnosti informací (ISMS), dříve známá jako BS7799 část 2, podle které jsou systémy certifikovány. Poslední revize normy byla publikována v říjnu 2013. |
| ISO 27002 | norma byla prvně publikována v červnu 2005 jako ISO/IEC 17799:2005. V červenci 2007 došlo k jejímu přejmenování na ISO/IEC 27002:2005, kdy obsah předchozí normy byl zachován. Poslední revize normy byla vydána v říjnu 2013. |
| ISO 27003 | návod pro návrh a zavedení ISMS v souladu s ISO 27001. |
| ISO 27004 | - norma byla publikována v prosinci 2009 pod názvem "Information technology - Security techniques - Information security management - Measurement". Normu přeložila společnost Risk Analysis Consultants. |
| ISO 27005 | norma byla publikována v červnu 2008 pod názvem "Information technology - Security techniques - Information security risk management" a následně v červnu 2011 revidována. |
| ISO 27006 | norma byla poprvé publikována v březnu 2007 pod názvem “Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems”. |
| ISO 27007 | norma byla publikována v listopadu 2011 pod názvem "Information technology — Security techniques — Guidelines for information security management systems auditing". |
| ISO 27008 | norma byla publikována v listopadu 2011 pod názvem "Information technology — Security techniques — Guidelines for auditors on information security management systems controls". Obsahuje doporučení auditorům ISMS a doplňuje ISO 27007. |
| ISO 27010 | norma byla publikována v dubnu 2012 pod názvem "ISO/IEC 27010:2012 Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications". Poskytuje doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci. |
| ISO 27011 | norma byla publikována v roce 2008 pod názvem "ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002". Obahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů. |
| ISO 27013 | norma byla publikována v říjnu 2012 pod názvem "ISO/IEC 27013:2012 — Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1". Norma poskytuje doporučení pro implementaci ISO/IEC 20000 a ISO/IEC 27001. |
| ISO 27014 | norma byla publikována v první polovině roku 2013 pod názvem "ITU-T Recommendation X.1054 & ISO/IEC 27014:2013 Information technology — |

| | |
|---|---|
| | Security techniques — Governance of information security". Norma organizacím poskytuje doporučení při návrhu Information Security Governance. |
| ISO 27015 | norma byla publikována v listopadu 2012 pod názvem "ISO/IEC TR 27015:2012 Information technology — Security techniques — Information security management guidelines for financial services". Obsahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí finančních institucí (banky, pojišťovny apod.). |
| ISO 27016 | norma byla publikována v roce 2014 jako technická zpráva (Technical Report) pod názvem ISO/IEC TR 27016:2014 — IT Security — Security techniques — Information security management – Organizational economics. Poskytuje doporučení pro nastavení bezpečnostního programu s ohledem na předpokládané finanční výsledky. |
| ISO 27018 | norma byla publikována v srpnu 2014 pod názvem ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors. Poskytovatelům cloudových služeb dává vhodná bezpečnostní opatření pro zabezpečení soukromí zákazníků. |
| ISO 27019 | norma byla publikována jako Technická zpráva (Technical Report) pod názvem "ISO/IEC TR 27019:2013 — Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry". Norma pomáhá organizacím v energetickém průmyslu interpretovat a aplikovat normu ISO/IEC 27002, aby byla zajištěna bezpečnost jejich systémů pro elektronické řízení procesů. |
| ISO 27031 | norma byla publikována v březnu 2011 pod názvem "ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity".Obsahuje doporučení pro zajištění kontinuity činností organizace (business continuity). |
| ISO 27032 | norma pod označením "Guidelines for cybersecurity" vyšla v červnu 2012, obsahuje bezpečnostní doporučení týkající se kyberprostoru. |
| ISO 27033 | soustava norem poskytující doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí. Prozatím bylo vydáno pět částí normy. |
| ISO 27034 | soustava norem poskytující doporučení pro tvorbu, implementaci a užívání aplikačního softwaru. Byla vydána první část normy. |
| ISO 27035 | norma byla publikována v roce 2011 pod názvem "Information security incident management". Norma se věnuje řízení incidentů bezpečnosti informací. |
| ISO 27036 | soubor norem "Information security for supplier relationships" bude obsahovat doporučení organizacím pro hodnocení a snižování rizik týkajících se outsourcovaných služeb. Prozatím byly vydány první tři části. |
| ISO 27037 | norma byla publikována v říjnu 2012 pod názvem "ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence". |

| | |
|---|---|
| | Norma obsahuje doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů. |
| ISO 27038 | norma byla publikována v roce 2014 pod názvem "ISO/IEC 27038:2014 — Information technology — Security techniques — Specification for digital redaction". Norma obsahuje doporučení pro publikování digitálních dokumentů. |
| ISO 27799 | doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních. |

Následující podkapitoly využívají přesných definicí normy ISO/IEC 27000 z důvodu, aby nedošlo ke změně zamýšleného významu autorem.

### 1.3.1 Předmět normy ISO/IEC 27000

Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací a definuje související termíny, které jsou běžně používané v ISMS. Použitelná je pro všechny typy i velikosti organizací, od drobných podniků až po vládní úřady. *(ISO 27000, 2014, s. 8)*

### 1.3.2 Některé termíny a definice (řazeno dle normy ISO 27000)

- **Řízení přístupu** (2.1 - access control) jsou prostředky zajišťující, aby přístup k aktivům byl autorizován a omezen na základě obchodních a bezpečnostních požadavků.
- **Útok** (2.3 - attack) je pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti, zcizení aktiva nebo získání neoprávněného přístupu k aktivu nebo uskutečnění neoprávněného použití aktiva.
- **Audit** (2.5 - audit) je systematický, nezávislý a dokumentovaný proces k získání důkazů z auditu, a jejich objektivní ohodnocení, aby se určil rozsah, v jakém jsou auditní kritéria splněna.
- **Autentizace** (2.7 - authentication) je poskytnutí záruky, že prohlašovaná charakteristika entity je správná.
- **Autenticita** (2.8 - authenticity) je vlastnost vyjadřující, že entita je tím, za co se vydává.
- **Dostupnost** (2.9 - availability) je přístupnost a použitelnost na žádost oprávněné entity.

- **Kompetence** (2.11 - competence) je schopnost použít znalosti a dovednosti k dosažení zamýšlených výsledků.
- **Důvěrnost** (2.12 - confidentiality) je splnění požadavku.
- **Následek** (2.14 - consequence) je výsledek události působící na cíle
- **Opatření** (2.16 - control) je prostředek modifikující riziko.
- **Událost** (2.25 - event.) je výskyt nebo změna určité množiny oolností
- **Bezpečnost informací** (2.33 - information security) je zachování důvěrnosti, integrity a dostupnosti informací.
- **Incident bezpečnosti informací** (2.36 - information security incident) je jednotlivá nežádoucí nebo neočekávaná událost bezpečnosti informací nebo série nežádoucích nebo neočekávaných událostí bezpečnosti informací, které mohou s významnou pravděpodobností vyvolat kompromitování operací souvisejících s činností organizace a ohrožení bezpečnosti informací.
- **Informační systém** (2.39 - information system) jsou aplikace, služby, aktiva informační technologie nebo další komponenty zacházející s informacemi.
- **Integrita** (2.40 - integrity) je vlastnost přesnosti a úplnosti.
- **Stupeň rizika** (2.44 - level of risk) je velikost rizika vyjádřená jako kombinace následků a jejich pravděpodobnost
- **Systém řízení** (2.46 - management system) je soubor vzájemně propojených nebo vzájemně na sebe působících prvků organizace k ustavení politik, cílů a procesů k dosažení těchto cílů
- **Cíl** (2.56 - objective) je výsledek, kterého má být dosaženo.
- **Organizace** (2.57 - organization) je osoba nebo skupina osob, které mají své vlastní funkce s odpovědnostmi, pravomocemi a vztahy, pomocí nichž mohou dosáhnout svých cílů.
- **Politika** (2.60 - policy) je celkový záměr a směřování organizace, formálně vyjádřené jejím vrcholovým vedením.
- **Proces** (2.61 - process) je soubor aktivit majících vzájemný vztah nebo vzájemně na sebe působících a přeměňujících vstupy na výstupy.
- **Požadavek** (2.63 - requirement) je potřeba nebo očekávání, které jsou stanovené, obecně předpokládané nebo závazné.
- **Zbytkové riziko** (2.64 - residual risk) riziko zbývající po ošetření rizika.

- **Riziko** (2.68 - risk) je účinek nejistoty na dosažení cílů. Riziko bezpečnosti informací je spojeno s možností, že hrozby využijí zranitelností informačního aktiva nebo skupiny informačních aktiv a tak způsobí organizaci škodu.
- **Hrozba** (2.83 - threat) je potencionální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.
- **Vrcholový management** (2.84 - top management) je osoba nebo skupina lidí, kteří řídí a kontrolují organizaci na nejvyšší úrovni.
- **Zranitelnost** (2.89 - vulnerability) je slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami.

*(ISO 27000, 2014, s. 8-18)*

### 1.3.3 ISO/IEC 27000 v souvislostech

Norma ISO/IEC27000 slouží jako obecný přehled o problematice systémů pro řízení bezpečnosti informací (ISMS). Je úvodem do řady norem ISO/IEC27000, definuje základní pojmy a vymezuje důležité termíny. Certifikací ISO/IEC 27001 subjekty prokazují vysokou úroveň bezpečnosti vzhledem k informacím. ISO/IEC27000 navazuje na další řady norem – například na Systém managementu jakosti (ISO 9000), které umožňují prokázat daným organizacím schopnost výroby či distribuci produktů v souladu se všemi nezbytnými předpisy a potřebami zákazníka.

## 1.4 ISO/IEC 27001

V této kapitole bude představena norma ISO/IEC27001, která je velmi důležitou ve vztahu k zákonu o kybernetické bezpečnosti, který z ní vychází. Podkapitoly opět využívají přesných definic normy, aby nedošlo k nepřesné interpretaci.

### 1.4.1 Předmět normy ISO/IEC 27001

Tato mezinárodní norma specifikuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací v kontextu organizace. Tato mezinárodní norma také zahrnuje požadavky na posuzování a ošetření rizik bezpečnosti informací, přizpůsobené potřebám organizace. Požadavky této normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. Vyloučení jakýchkoli požadavků obsažených v následujících

sedmi kapitolách je nepřijatelné, pokud chce organizace dosáhnout shody s touto normou. *(ISO 27001, 2014, s. 7)*

### 1.4.2 Kontext organizace

#### Porozumění organizaci a jejímu kontextu

Organizace musí určit externí a interní aspekt, který je významný pro její záměry a který ovlivňuje její schopnost dosáhnout zamýšleného výstupu (výstupů) systému řízení bezpečnosti informací organizace.

#### Porozumění potřebám a očekáváním zainteresovaných stran

Organizace musí dále určit:

a) zainteresované strany, které mají vztah k systému řízení bezpečnosti informací;
b) požadavky těchto zainteresovaných stran, které jsou relevantní k bezpečnosti informací.

#### Stanovení rozsahu systému řízení bezpečnosti informací (ISMS)

Pro stanovení rozsahu musí organizace určit hranice a aplikovatelnost systému řízení bezpečnosti informací. Při určování tohoto rozsahu musí organizace zvážit:

a) externí a interní aspekt (viz. „Porozumění organizaci a jejímu kontextu“);
b) požadavky zainteresovaných stran (viz. „Porozumění potřebám a očekáváním zainteresovaných stran“);
c) propojení a závislosti mezi činnostmi prováděnými organizací a těmi činnostmi, které jsou prováděné jinými organizacemi.

Rozsah systému řízení bezpečnosti informací musí být dostupný jako dokumentovaná informace.

#### Systém řízení bezpečnosti informací

Organizace musí ustavit, implementovat, udržovat a neustále zlepšovat systém řízení bezpečnosti informací v souladu s požadavky této mezinárodní normy. *(ISO 27001, 2014, s. 7)*

### 1.4.3 Vůdčí role

#### Vůdčí role a závazek

Vrcholové vedení organizace musí s ohledem na systém řízení bezpečnosti informací demonstrovat vůdčí roli a závazek tím, že:

a) zajistí stanovení politiky bezpečnosti informací a cílů bezpečnosti informací slučitelných se strategickým směrováním organizace;
b) zajistí integraci požadavků systému řízení bezpečnosti informací do procesů organizace;
c) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací;
d) komunikuje význam efektivního řízení bezpečnosti informací a význam dosažení shody s požadavky systému řízení bezpečnosti informací;
e) zajistí dosažení zamýšlených výstupů systému řízení bezpečnosti informací organizace;
f) směřuje a podporuje osoby k přispívání efektivnosti systému řízení bezpečnosti informací;
g) prosazuje neustálé zlepšování;
h) podporuje ostatní relevantní řídící role k prokázání jejich vůdčí role v oblastech jejich odpovědnosti.

#### Politika

Vrcholové vedení organizace musí stanovit politiku bezpečnosti informací, která:

a) je přiměřená záměrům organizace;
b) zahrnuje cíle bezpečnosti informací nebo poskytuje rámec pro nastavení cílů bezpečnosti informací
c) zahrnuje závazek ke splnění aplikovatelných požadavků týkajících se bezpečnosti informací.
d) zahrnuje závazek k neustálému zlepšování systému řízení bezpečnosti informací

Politika bezpečnosti informací musí:

e) být dostupná jako dokument;
f) být komunikována v rámci organizace;

g) být přiměřeně dostupná zainteresovaným stranám.

#### Role, odpovědnosti a pravomoci organizace

Vrcholové vedení organizace musí zajistit, že odpovědnosti a pravomoci pro role relevantní bezpečnosti informací jsou přiřazeny a komunikovány.

Vrcholové vedení organizace musí přiřadit odpovědnosti a pravomoci pro:

a) zajištění, že systém řízení bezpečnosti informací je ve shodě s požadavky této mezinárodní normy;
b) podávání zpráv o výkonnosti systému řízení bezpečnosti informací vrcholovému vedení organizace.

*(ISO 27001, 2014, s. 8)*

### 1.4.4 Plánování

#### Opatření zaměřená na rizika a příležitosti

Při plánování systému řízení bezpečnosti informací musí organizace zvážit aspekt a požadavky zainteresovaných stran a určit rizika, na které se potřebuje zaměřit pro:

a) zajištění, že systém řízení bezpečnosti informací organizace může dosáhnout zamýšlených výstupů;
b) předcházení nebo snížení nežádoucích následků;
c) dosažení neustálého zlepšování.

Organizace musí plánovat:

d) opatření zaměřená na tato rizika a příležitosti;
e) jak
    1) integrovat a implementovat tato opatření do procesů ISMS;
    2) vyhodnocovat efektivnost těchto opatření.

#### Posuzování rizik bezpečnosti informací

Organizace musí definovat a aplikovat proces posuzování rizik bezpečnosti informací, který:

a) stanoví a udržuje kritéria rizik bezpečnosti informací, která zahrnují:
    1) kritéria akceptace rizik;

2) kritéria pro provádění posouzení rizik bezpečnosti informací;

b) zajistí, že opakovaná posouzení rizik bezpečnosti informací produkují konzistentní, opodstatněné a porovnatelné výsledky;

c) identifikuje rizika bezpečnosti informací:

1) používá proces posuzování rizik bezpečnosti informací k identifikaci rizik spojených se ztrátou důvěrnosti, integrity a dostupnosti informací v rozsahu systému řízení bezpečnosti informací;

2) identifikuje vlastníky rizik;

d) analyzuje rizika bezpečnosti informací:

1) posuzuje potencionální následky, které by nastaly, pokud by se realizovala rizika identifikovaná v c) 1);

2) posuzuje reálnou pravděpodobnost výskytu rizik identifikovaných v c) 1);

3) určuje úroveň rizik;

e) hodnotí rizika bezpečnosti informací:

1) porovnává výsledky analýzy rizik s kritérii rizik stanovených v a);

2) stanovuje priority analyzovaných rizik pro ošetření rizika.

Organizace musí uchovávat dokumentované informace o procesu posuzování rizik bezpečnosti informací.

### Ošetření rizik bezpečnosti informací

Organizace musí definovat a používat proces ošetření rizik bezpečnosti informací pro:

a) výběr vhodných variant pro ošetření rizika bezpečnosti informací s ohledem na výsledky posuzování rizik;

b) určení všech opatření nezbytných k implementaci vybrané varianty pro ošetření rizika bezpečnosti informací;

c) porovnání opatření určených v bodě b) s opatřeními pro verifikaci, že žádné nezbytné opatření nebylo vynecháno;

d) vytvoření Prohlášení o aplikovatelnosti, které obsahuje nezbytná opatření (viz. b) a c)) a zdůvodnění pro jejich zahrnutí, ať už jsou nebo nejsou implementována, a zdůvodnění pro vyloučení opatření pro verifikaci (viz. příloha A normy ISO/IEC 27001).

e) formulaci plánu ošetření rizik bezpečnosti informací;
f) získání souhlasu vlastníků rizik ohledně plánu ošetření rizik bezpečnosti informací a přijetí zbytkových rizik bezpečnosti informací.

Organizace musí uchovávat dokumenty o procesu ošetření rizik bezpečnosti informací.

#### Cíle bezpečnosti informací a plánování jejich dosažení

Organizace musí stanovit cíle bezpečnosti informací relevantní jednotlivým funkcím a úrovním řízení. Cíle bezpečnosti informací musí:

a) být konzistentní s politikou bezpečnosti informací;
b) být měřitelné, pokud je to proveditelné;
c) vzít v úvahu aplikovatelné požadavky bezpečnosti informací a výsledky z posuzování rizik a ošetření rizik;
d) být komunikovány;
e) být dle potřeby aktualizovány.

Organizace musí uchovávat dokumentované informace o cílech bezpečnosti informací. Při plánování jak dosáhnout cílů bezpečnosti informací musí organizace určit:

f) co bude vykonáno;
g) jaké zdroje budou vyžadovány;
h) kdo bude odpovědný;
i) kdy to bude dokončeno;
j) jak budou výsledky vyhodnoceny.

*(ISO 27001, 2014, s. 8-10)*

### 1.4.5 Podpora

#### Zdroje

Organizace musí určit a zajistit zdroje potřebné pro ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací.

### Kompetence

Organizace musí:

a) určit nezbytné kompetence osoby nebo osob vykonávajících pro organizaci práci, která má vliv na výkonnost bezpečnosti informací;
b) zajistit, že tyto osoby jsou kompetentní na základě odpovídajícího vzdělání, školení nebo zkušeností;
c) tam, kde je to aplikovatelné, přijmout opatření k získání nezbytné kompetence a vyhodnocovat efektivnost těchto přijatých opatření;
d) uchovávat odpovídající dokumentované informace jako důkazy o kompetenci.

### Povědomí

Osoby pracující pro organizaci si musí být vědomy:

a) politiky bezpečnosti informací;
b) svého přínosu k efektivnosti systému řízení bezpečnosti informací, včetně výhod zlepšené výkonnosti bezpečnosti informací;
c) důsledků nepřizpůsobení se požadavkům systému řízení bezpečnosti informací.

### Komunikace

Organizace musí ve vztahu k systému řízení bezpečnosti informací určit potřebu pro interní a externí komunikaci, která zahrnuje:

a) o čem komunikovat;
b) kdy komunikovat;
c) s kým komunikovat;
d) kdo musí komunikovat;
e) procesy, kterými musí být komunikace realizována.

### Dokumentované informace - obecně

Systém řízení bezpečnosti informací musí zahrnovat:

a) dokumentované informace požadované touto mezinárodní normou
b) dokumentované informace určené organizací za nezbytné pro efektivnost systému řízení bezpečnosti informací.

### Vytváření a aktualizace dokumentovaných informací

Při vytváření a aktualizaci dokumentovaných informací musí organizace zajistit odpovídající:

a) identifikaci a popis (např. název, datum, autor nebo číslo jednací);
b) formát (např. jazyk, verze softwaru, grafika) a média (např. papírové, elektronické);
c) přezkoumání a schválení vhodnosti a přiměřenosti.

### Řízení dokumentovaných informací

Dokumentované informace vyžadované systémem řízení bezpečnosti informací a touto mezinárodní normou musí být řízeny, aby bylo zajištěno následující:

a) dokumentované informace jsou dostupné a vhodné pro použití, a to kdekoliv a kdykoliv je to potřebné;
b) dokumentované informace jsou odpovídajícím způsobem chráněny (např. před prozrazením, nevhodným použitím nebo ztrátou integrity).

Pro řízení dokumentovaných informací musí organizace věnovat pozornost následujícím činnostem, pokud jsou aplikovatelné:

c) distribuci, přístupu, vyhledání a použití;
d) ukládání a zachování, včetně zachování čitelnosti;
e) řízení změn (např. řízení verzí);
f) uchování a likvidace.

Dokumentované informace externího původu, které organizace určí jako nezbytné pro plánování a provozování systému řízení bezpečnosti informací, musí být dle potřeby identifikovány a řízeny.

*(ISO 27001, 2014, s. 10-11)*

## 1.4.6 Provozování

### Plánování a řízení provozu

Organizace musí plánovat, implementovat a řídit procesy potřebné ke splnění požadavků bezpečnosti informací a implementovat opatření určená v kapitole 1.4.4.

Organizace musí také implementovat plány k dosažení cílů bezpečnosti informací určených v 1.4.4.

Organizace musí udržovat dokumentované informace v nezbytném rozsahu, aby měla jistotu, že procesy byly prováděny, jak bylo plánováno.

Organizace musí řídit plánované změny a přezkoumávat následky neúmyslných změn přijímáním opatření ke snížení jakýchkoliv nepříznivých dopadů, pokud je to nezbytné.

Organizace musí zajistit, že jsou outsourcované procesy určeny a řízeny.

#### Posuzování rizik bezpečnosti informací

Organizace musí posuzovat rizika bezpečnosti informací v pravidelných intervalech, nebo pokud jsou plánovány nebo nastanou významné změny, a to s ohledem na kritéria stanovená v podkapitole 1.4.4. Organizace musí uchovávat dokumentované informace o výsledcích posuzování rizik bezpečnosti informací.

#### Ošetření rizik bezpečnosti informací

Organizace musí implementovat plán ošetření rizik bezpečnosti informací. Organizace musí uchovávat dokumentované informace o výsledcích ošetření rizik bezpečnosti informací. *(ISO 27001, 2014, s. 11-12)*

### 1.4.7 Hodnocení výkonnosti

#### Monitorování, měření, analýza a hodnocení

Organizace musí vyhodnocovat výkonnost bezpečnosti informací a efektivnost systému řízení bezpečnosti informací.

Organizace musí určit:

a) co je třeba monitorovat a měřit, včetně procesů a opatření bezpečnosti informací;
b) použitelné metody monitorování, měření, analýzy a hodnocení k zajištění platných výsledků;
c) kdy musí být monitorování a měření prováděno;
d) kdo bude monitorovat a měřit;

e) kdy budou výsledky z monitorování a měření analyzovány a vyhodnoceny;
f) kdo bude analyzovat a vyhodnocovat výsledky.

Organizace musí uchovávat odpovídající dokumentované informace jako důkazy o výsledcích monitorování a měření.

### Interní audit

Organizace musí v plánovaných intervalech provádět interní audity k získání informací o tom, zda systém řízení bezpečnosti informací:

a) vyhovuje:
    1) vlastním požadavkům organizace na systém řízení bezpečnosti informací;
    2) požadavkům této mezinárodní normy;
b) je efektivně implementován a udržován.

Organizace musí:

c) plánovat, ustavit, implementovat a udržovat auditní program (programy), včetně četnosti, metod, odpovědností, plánování požadavků a podávání zpráv. Auditní program musí vzít v úvahu význam příslušných procesů a výsledků předchozích auditů;
d) definovat kritéria auditu a rozsah každého auditu;
e) vybrat auditory a provádět audity při zajištění objektivity a nestrannosti procesu auditu;
f) zajistit, aby byly výsledky auditů předkládány relevantním vedoucím pracovníkům;
g) uchovávat dokumentované informace jako důkaz o programu a výsledcích auditů.

### Přezkoumání vedením organizace

Vrcholové vedení organizace musí v plánovaných intervalech přezkoumávat systém řízení bezpečnosti informací organizace pro zajištění jeho neustálé vhodnosti, přiměřenosti a efektivnosti. Přezkoumání vedením organizace musí vzít v úvahu:

a) stav opatření z předchozích přezkoumání vedením organizace;

b) změny v externím a interním aspektu, které jsou relevantní pro systém řízení bezpečnosti informací;
c) zpětnou vazbu na výkonnost bezpečnosti informací, včetně trendů ohledně:
    1) neshod a nápravných opatření;
    2) výsledků monitorování a měření;
    3) výsledků auditů;
    4) naplnění cílů bezpečnosti informací;
d) zpětnou vazbu od zainteresovaných stran;
e) výsledky posuzování rizik a stav plánu ošetření rizika;
f) příležitosti pro neustálé zlepšování.

Výstupy z přezkoumání vedením organizace musí zahrnovat rozhodnutí vztahující se k příležitostem neustálého zlepšování a k jakýmkoliv potřebám pro změny v systému řízení bezpečnosti informací. Organizace musí uchovávat dokumentované informace jako důkazy o výsledcích přezkoumávání vedení organizace.

*(ISO 27001, 2014, s. 12-13)*

### 1.4.8 Zlepšování

#### Neshody a nápravná opatření

Při výskytu neshody musí organizace:

a) reagovat na neshodu, a pokud je to aplikovatelné:
    1) přijmout opatření k řízení a nápravě neshody;
    2) zabývat se následky;
b) vyhodnotit potřebu pro opatření k odstranění příčin neshody, aby se nehoda znovu nevyskytla, prostřednictvím:
    1) přezkoumání neshody;
    2) určení příčin neshody;
    3) určení, zda existují podobné neshody nebo by se mohly potencionálně vyskytnout;
c) implementovat jakákoliv potřebná opatření;
d) přezkoumat efektivnost každého přijatého nápravného opatření;
e) provést změny v systému řízení bezpečnosti informací, pokud je to nezbytné;

Nápravná opatření musí být přiměřená dopadům neshod, kterým čelí.

Organizace musí uchovávat dokumentované informace jako důkaz o:

f) podstatě neshod a každého následného přijatého opatření;
g) výsledcích každého nápravného opatření.

**Neustálé zlepšování**

Organizace musí neustále zlepšovat vhodnost, přiměřenost a efektivnost systému řízení bezpečnosti informací. *(ISO 27001, 2014, s. 13)*

### 1.4.9 ISO/IEC 27001 v souvislostech

ISO/IEC 27001 vymezuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování ISMS. Rozvádí tím normu ISO/IEC27000. Určuje, jak nakládat s aktivy organizace a jak se vypořádat s riziky. Důležitou částí ISO/IEC27001 je část, ve které je vysvětleno, jak vytvořit politiku bezpečnosti informací. Další normy řadu ISO/IEC27000 využívají její aspekty a dále je rozvádějí. Mezi klíčová slova normy patří „interní audit“ a „neustálé zlepšování“.

## 1.5 ISO/IEC 27002

V této kapitole bude představena norma ISO/IEC27002. Spolu s normou ISO/27001 tvoří nejdůležitější části, které se objevují v Zákoně o kybernetické bezpečnosti, který bude podrobněji popsán v kapitole 3.

### 1.5.1 Předmět normy ISO/IEC 27002

ISO/IEC 27002 poskytuje seznam obecně akceptovaných cílů opatření a opatření pro doporučené postupy, které mají být použity jako návod k implementaci při výběru a provádění opatření, jejichž cílem je dosáhnout bezpečnosti informací. *(ISO 27001, 2014, s. 25)*

### 1.5.2 ISO/IEC 27002 v souvislostech

Tato norma obsahuje už konkrétní typy opatření. Vzhledem ke vhodnosti a použitelnosti je možné provést výběr některých opatření (případně všech) v rámci procesu zavádění ISMS, které popisuje norma ISO/IEC 27001. Tyto opatření bezpečnosti informací je možné popsat v rámci doporučených metodik.

Jako dvě z vhodných metodik pro odhalování zranitelností systému i opakovatelnou kontrolu správnosti nasazení opatření, zmiňuje norma SWOT analýzu a penetrační testování.

## 1.6 Další normy řady ISO/IEC 27000

### 1.6.1 ISO/IEC 27003

ISO/IEC 27003 poskytuje praktický návod pro implementaci a informace pro ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování ISMS dle ISO/IEC 27001. *(ISO 27001, 2014, s. 25)*

### 1.6.2 ISO/IEC 27004

ISO/IEC 27004 poskytuje návod a doporučení pro vývoj a použití měření, aby se posoudila efektivnost ISMS, cílů opatření a opatření použitých k implementaci a řízení bezpečnosti informací podle specifikace ISO/IEC 27001. *(ISO 27001, 2014, s. 25)*

### 1.6.3 ISO/IEC 27005

ISO/IEC 27005 poskytuje směrnice pro řízení rizik bezpečnosti informací. Přístup popsaný v této mezinárodní normě podporuje obecná pojetí specifikovaná v ISO/IEC 27001. *(ISO 27001, 2014, s. 26)*

## 1.7 Shrnutí norem ISO/IEC 27000

Předcházející kapitoly se podrobně věnovaly normám řady ISO/IEC27000, které jsou důležité v návaznosti na nový Zákon o kybernetické bezpečnosti. Norma ISO/IEC27000 poskytuje přehled důležitých termínů, které se používají i v dalších normách této řady. Součástí normy ISO/IEC27000 je rovněž detailně vysvětlen pojem ISMS, kterému autor věnoval kapitolu 1.1 a její podkapitoly.

Kapitola 1.4 navazuje a věnuje se podrobně normě ISO/IEC27001, která specifikuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací v kontextu organizace. Pokud chce organizace dosáhnout shody s touto normou, nesmí být vyloučeny požadavky v podkapitolách 1.4.2 – 1.4.8.

V kapitole 1.5 je představena norma ISO/IEC27002. Jelikož Zákon o kybernetické bezpečnosti a příslušná jeho vyhláška čerpají převážně z této normy, není v této kapitole

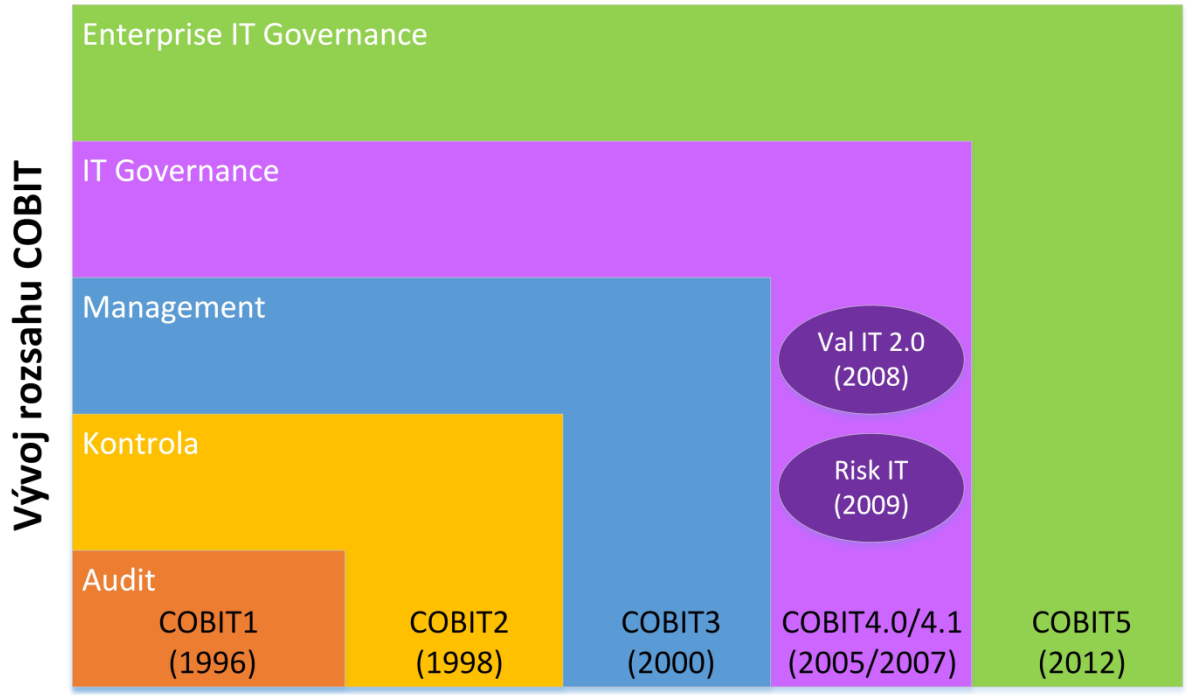
zacházeno do detailů. Ty jsou, včetně podrobných informací a analýz vysvětleny v samostatné kapitole 3, věnované Zákonu o kybernetické bezpečnosti.

V kapitole 1.6 a jejích podkapitolách jsou uvedeny i další normy z řady ISO/IEC27000 – konkrétně ISO/IEC 27003, ISO/IEC 27004 a ISO/IEC 27005. Informace obsažené v těchto normách přesahují rámec Zákona o kybernetické bezpečnosti, proto jsou zmíněny pouze okrajově s informacemi o jejich obsahu.

# 2 COBIT

## 2.1 Historie COBIT

COBIT (**C**ontrol **OB**jectives for **I**nformationand related **T**echnology) je metodika, která tvoří ucelený, veřejně dostupný rámec (framework), formulující doporučení pro implementaci IT procesů, postupy jejich hodnocení a to vše v návaznosti na celkovou podnikovou strategii *(Bernard, 2012)*. Veřejná dostupnost této metodiky znamená, že její publikace je možné zakoupit a neomezeně využívat. První revize této metodiky byla vydána společností ISACA již v roce 1996 a byla zaměřena převážně na provádění auditu podnikových informačních technologií. Od verze COBIT2 přebírá iniciativu společnost ITGI. COBIT2, která vznikla v roce 2008, přidává vrstvu „Řízení". V roce 2000 následovala metodika COBIT3 s vrstvou „Pokyny řízení". Všechny tyto metodiky byly poprvé publikované online v roce 2003. COBIT4.0 a COBIT4.1, které vznikly v roce 2005, respektive 2007 přidávají vrstvu „IT governance". COBIT4.1 je také výrazně zaměřen na procesy.




**Obrázek 1 - vývoj COBITu (zdroj: zpracováno dle (ISACA, 2012))**

Procesní model COBIT4.1 se dělí na 4 základní domény – „Plánování a organizace", „Akvizice a implementace", „Dodávka a podpora", „Sledování a hodnocení" a 34 procesů,

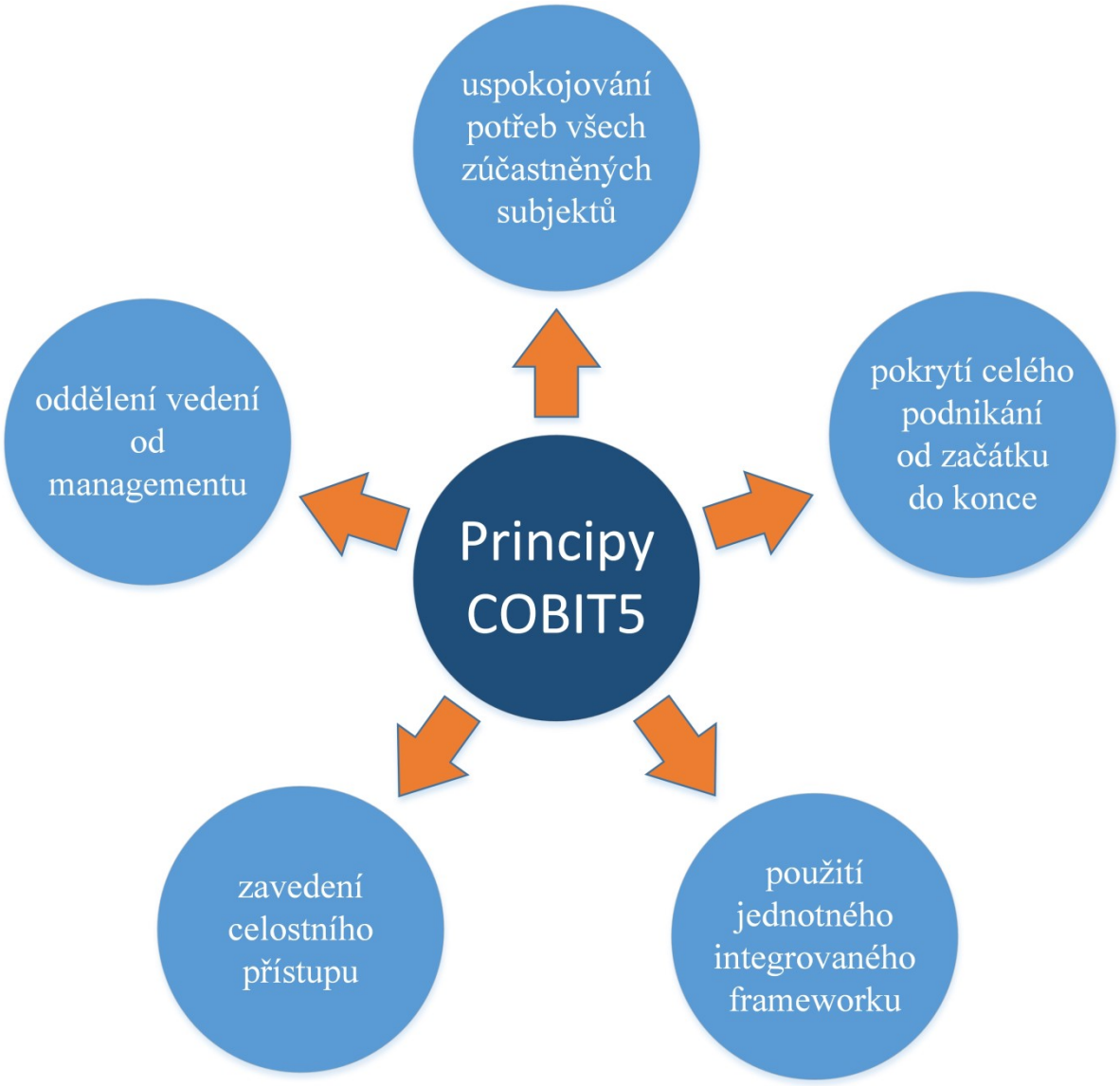
které jsou v souladu s těmito doménami. Zatím poslední vydanou verzí je verze COBIT5, kterou společně vydaly v červnu roku 2012 společnosti ISACA a ITGI. Oproti verzi 4.1 došlo k celkové změně v organizaci metodiky. Metodika se více zaměřuje na všechny zúčastněné objekty, tedy například i na externí subjekty, který mají nějaký význam pro celý podnik. COBIT5 zahrnuje COBIT4.1 a sdružuje s ním dříve oddělené metodiky Val IT 2.0 a Risk IT, tedy metodiky pro řízení a hodnocení investic a IT rizik. Díky tomu se COBIT5 přiblížil jiným metodikám, mezi které patří například ITIL nebo ISO/IEC20000. *(ISACA, 2012)*

## 2.2 Hlavní principy COBIT5

Jak již bylo naznačeno v minulé kapitole, vychází COBIT5 ze starší verze COBIT4.1. I proto nadále platí, že informace jsou jedním z klíčových aktiv každého podniku. Jakákoliv práce s informacemi je dnes závislá na informačních technologiích, které díky své sofistikovanosti vyžadují, aby byly spravovány odborníky v oblasti IT a nikoliv vrcholovým managementem podniku. IT technologie jsou tedy dnes jednou ze zásadních částí podniku a to nejen proto, že zasahují do všech hledisek jeho existence. Pokud jsou procesy okolo IT správně implementovány, umožňují generování přidané hodnoty v oblasti IT investic, usnadňují rozhodování v obchodních záležitostech a tím zjednodušují dosažení strategických cílů podniku. *(Harmer, 2014)* COBIT5 v sobě zahrnuje podporu rizikových analýz. Jedná se o více než 100 scénářů přehledně rozdělených do 20 kategorií v části nazvané „COBIT5 for Risk“. Každý scénář obsahuje detailní pokyny, jak se zachovat v případě události, která by například mohla ohrozit obchodní hodnotu společnosti nebo poškodit její dobrou pověst. *(ISACA, 2015)*

Metodika COBIT5 se skládá z 5 principů:

- uspokojování potřeb všech zúčastněných subjektů (Meeting Stakeholder Needs)
- pokrytí celého podnikání od začátku do konce (Covering the Enterprise End-to-End)
- použití jednotného integrovaného frameworku (Applying Single Integrated Framework)
- zavedení celostního přístupu (Enabling a Holistic Approach)
- oddělení vedení od managementu (Separating Governance From Management)




**Obrázek 2 - hlavní principy COBIT5 (zdroj: zpracováno dle (ISACA))**

## 2.3 Rozdíl mezi COBIT a ISO/IEC 27000

COBIT i řada norem ISO27000 se řadí mezi standardy. Každý z nich se však zaměřuje na jinou problematiku, zároveň se však nevylučují. Zatímco normy ISO27000 úzce cílí na IT bezpečnost, COBIT se na celou problematiku dívá ze širšího měřítka – z pohledu celé společnosti a subjektů, na kterých je společnost závislá. I COBIT v sobě zahrnuje prvky bezpečnosti, ale pouze povrchně. Můžeme v něm najít informace a návody, jaké bezpečnostní opatření je potřeba zavést, ale již není nikde napsáno, jak to máme udělat. Na druhou stranu v normách řady ISO27000 nenalezneme informace, jak

zapracovat tato bezpečnostní opatření do širšího kontextu podnikové strategie. Základní rozdíly zobrazuje názorně následující tabulka.

**Tabulka 2 - rozdíly mezi COBIT a ISO27001 (zdroj: zpracováno dle (Varun Arora, 2010, s. 8 ))**

| | **COBIT** | **ISO27001** |
|---|---|---|
| **Zaměření** | Obchodní zaměření a IT governance v plném rozsahu | Provádění bezpečnostních kontrol, důraz na přístup k řízení rizik |
| **Model** | Plánování IT procesů | Systém řízení bezpečnosti informací |
| **Rozsah** | Kompletní správa IT governance organizace, včetně plánování zabezpečení. Jedná se o integrované řešení. | Pouze pokyny pro zabezpečení |
| **Struktura** | 34 IT procesů rozdělených do 4 domén | 11 sekcí, 36 cílů, které jsou dále děleny na dílčí cíle |
| **Organizační model** | Všechny zúčastněné strany | Management, IT oddělení |
| **Certifikace** | Ne | Ano |

Tabulka přináší pouze strohé porovnání, pro jednodušší pochopení rozdílů slouží následující odstavce, které se zaměří na jednotlivé řádky tabulky.

Zaměření – COBIT, který je aktuálně platný ve verzi COBIT5 se na celou problematiku subjektu dívá jako na celek. To znamená, že se snaží svým souhrnem „nejlepších praktik“ o dosažení hlavních cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizací IT rizik. Je především určen pro vrcholový management a pro auditory. Vzhledem k informačním a komunikačním technologiím (ICT) je určen primárně pro posuzování jejich fungování a také pro provádění auditu systému řízení, nezabíhá příliš do detailů, které se ICT týkají. COBIT neposkytuje přesné pokyny, jak dosáhnout kontrolních cílů. ISO27001 je řada standardů, které výhradně týkají bezpečnosti informací včetně její implementace a dopodrobna tuto problematiku dále rozebírají.

Model – COBIT se zaměřuje na plánování celofiremních procesů a to i v oblasti IT, ISO27001 cílí detailně na Systém řízení bezpečnosti informací bez bližší vazby na další firemní procesy.

Rozsah – Již z předchozích dvou bodů je možné odvodit, že COBIT zahrnuje plánování procesů v celé organizaci, zaměřuje se i na dodavatele, které zahrnuje mezi aktiva, celé řešení je integrovaný celek, poskytující globální pohled. ISO27001 pouze detailně vymezuje pokyny pro zabezpečení.

Organizační model – COBIT zahrnuje všechny zúčastněné strany, tedy i dodavatele, odběratele a všechny vlastní zaměstnance. ISO27001 je úzce zaměřen pouze na IT oddělení a IT management.

Certifikace – ISO27001 certifikace doslova říká, že společnost, která postupuje dle této řady norem, splňuje úroveň bezpečnosti, která je normou dána. Tato certifikace může být použita pro zjednodušení procesu naplnění podmínek zákona o kybernetické bezpečnosti, jelikož z ní zmíněný zákon vychází. COBIT certifikaci neposkytuje, protože exaktně neurčuje, jak dosáhnout cílů, pouze poskytuje souhrn praktik, které k tomu mohou dopomoci. Navíc každá korporace může mít cíle rozdílné nebo odlišné postupy, jak jich dosáhnout a tak by se těžko určovalo, zda certifikaci udělit, či nikoliv.

Který standard nebo standardy tedy implementovat a v jakém pořadí? Tato otázka nemůže být jednoduše zodpovězena, jelikož každá společnost je v podstatě unikát. Navíc je velice obtížné rozpoznat, které cíle jsou pro oba standardy totožné, i když jsou popsány jinými slovy a stejně těžké je rozpoznat cíle, které vypadají stejně, ale jsou díky drobným rozdílům ve formulaci diametrálně odlišné. Proto je při výběru také důležité zaměřit se například na následující body:

- sladění frameworku/standardu s cíli organizace
- vztahy s jinými společnostmi, které mají implementovány stejné standardy
- schopnost dosáhnout cílů s existující infrastrukturou, ale menšími náklady
- posouzení a řízení rizik
- školení zaměstnanců

I když jsou mezi COBIT a ISO27000 zásadní rozdíly, můžeme nalézt aspekty, ve kterých si jsou oba standardy blízké nebo se v nich dokonce překrývají. Pro příklad je možné uvést požadavky na ochranu dat. V obou standardech se jedná o společný cíl, ale ISO27001 vznáší další požadavky, které v COBIT nejsou požadovány. V tomto případě

ISO nad rámec toho, co je v COBIT požaduje off-site zálohování, tedy přenesení záloh na jiné místo mimo organizaci nebo do jiné pobočky společnosti, která je umístěna geograficky jinde. Tento požadavek s sebou samozřejmě přináší vyšší náklady a úsilí ze strany organizace.

# 3 Zákon o kybernetické bezpečnosti

V této kapitole bude podrobněji nový zákon č. 181/2014 Sb., tedy Zákon o Kybernetické Bezpečnosti (ZoKB). Autor práce se pokusí analyzovat požadavky prováděcí vyhlášky k ZoKB, týkající se bezpečnostních opatření pro Kritickou Informační Infrastrukturu (KII) a Významné Informační Systémy (VIS).

## 3.1 Důvod vzniku ZoKB

S neustálým rozvojem informačních technologií, provázaností klíčových počítačových systémů a rozšiřováním celosvětové sítě internet se výrazně zvyšuje i riziko elektronického útoku. Na rychlé datové sítě jsou dnes připojeny prakticky všechny důležité složky, které mají za úkol zajišťovat bezchybný a bezpečný chod státu. Na počítačových systémech dnes závisí doprava, ekonomika, energetika a například i integrovaný záchranný systém. Proto v únoru 2013 představila Evropská unie směrnici, podle níž by měly všechny členské státy zvýšit svoji odolnost proti případným kybernetickým útokům. Důležitost tohoto rozhodnutí pocítily v roce 2013 některé české zpravodajské servery a banky, které se ocitly pod masivním DDOS (přehlcení napadeného objektu velkým množstvím požadavků) útokem *(ITBiz.cz, 2014)*. Obdobných útoků každoročně přibývá a škody, které jsou těmito útoky způsobené, narůstají do závratných výšin.

V České republice došlo již v roce 2011 k pověření Národního bezpečnostního úřadu (NBÚ) k výkonu dozoru nad národní kybernetickou bezpečností. Hlavní povinností NBÚ bylo předložení návrhu legislativní úpravy v oblasti kybernetické bezpečnosti a vybudování Národního centra kybernetické bezpečnosti. Toto centrum by mělo zastávat funkci vládního CERT, což je zkratka anglického Cyber Emergency Response Team. Všechna tato opatření mají za úkol ochraňovat kritické informační systémy, které jsou nezbytné pro fungování státu. Jedná se hlavně o informačních systémy zajišťující práci státní správy a samosprávy a také o kritickou informační infrastrukturu, čímž se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva. Zatímco ochranu systémů veřejné správy je možnost zajistit prostřednictvím nařízení vlády, správci kritické infrastruktury mohou být ve velké míře i soukromé subjekty. Dle Ústavy ČR je možné ukládat povinnosti soukromým osobám pouze

prostřednictvím zákona, proto je třeba tuto úpravu provést přijetím nové legislativní normy na této úrovni – zákona o kybernetické bezpečnosti. *(MENIER s.r.o., 2013)*

## 3.2 Historie

Práce na návrhu věcného záměru zákona začaly již v roce 2011. Po rozsáhlých konzultacích s odbornou i širokou veřejností byl vládou přijat v květnu 2012. Prakticky okamžitě začaly práce na samotném zákonu *(ČIMIB, 2013)*. Zákon samotný je veden pod číslem 181/2014 Sb., byl schválen oběma komorami Parlamentu, podepsán presidentem ČR a ve sbírce zákona vyšel 29. srpna 2014. V současné době je již zákon v platnosti a to s účinností od 1. ledna 2015. Nezbytnou součástí, která musela být před nabytím účinnosti zákona vypracována, jsou tzv. prováděcí předpisy *(Peterka, 2014)*. Byly vypracovány tři předpisy:

- Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- Vyhláška, stanovující významné informační systémy a jejich určující kritéria
- Novela nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Vyhláška o kybernetické bezpečnosti zejména naplňuje a rozvádí první pilíř zákona o kybernetické bezpečnosti - bezpečnostní opatření, neboli požadavky na standardizaci kritické informační infrastruktury a významných informačních systémů. Vyhláška byla vypracována NBÚ.

Vyhláška, stanovující významné informační systémy a jejich určující kritéria, vyjmenovává konkrétní významné informační systémy včetně určujících kritérií, jejichž správci budou podléhat povinnostem podle zákona o kybernetické bezpečnosti. Z oblasti významných informačních systémů jsou přímo vyhláškou vyloučeny informační systémy obcí a informační systémy hlavního města Prahy, pokud jsou používány při výkonu jeho vlastní působnosti. Vyhláška byla vypracována ve spolupráci NBÚ a Ministerstva vnitra.

Novela nařízení vlády č. 432/2010 Sb. stanoví odvětvová kritéria pro určení prvku kritické infrastruktury v oblasti kybernetické bezpečnosti. Na tvorbě části novely se podílel NBÚ, novela jako celek je v gesci Ministerstva vnitra *(NBÚ, 2014)*.

## 3.3 Základní principy ZoKB

Zákon o kybernetické bezpečnosti vychází z několika principů. Hlavní úkol je sjednocení elektronické dokumentace a to jak ve státní, tak i v soukromé sféře. Aby byla komunikace mezi státem a soukromou sférou efektivní, je stanoven i způsob vzájemného dorozumívání a to tak, aby ze strany státu nedocházelo k přílišnému zasahování do práv soukromoprávních subjektů. Mělo by také dojít k postupnému sjednocení pasivní počítačové ochrany, ale zároveň by se neměla opomíjet i ochrana aktivní, aby bylo možné přímo a aktivně s útoky na elektronické úrovni bojovat *(BUREAU VERITAS CZECH REPUBLIC, spol. s r.o., 2014)*. Za ochranu informačních systémů je zodpovědný jejich provozovatel, prováděcí předpisy, které budou vycházet zejména z řady norem ISO27000, bude vydávat NBÚ. Kontrolní a exekutivní pravomoc vykonává Národní centrum kybernetické bezpečnosti CERT (pro soukromou sféru) a NBÚ (pro státní instituce a kritickou informační infrastrukturu). Funkci Národního centra kybernetické bezpečnosti CERT v současnosti vykonává sdružení CZ NIC.

Povinnosti správců jednotlivých subjektů jsou závislé na důležitosti spravovaných informačních systémů. Největší povinnosti tak budou mít správci kritické informační infrastruktury (KII), kteří budou mít za úkol především oznamovat bezpečnostní incidenty a také správci významných informačních systémů veřejné správy. Zvláštní povinnosti jsou pro ostatní subjekty určeny pouze v případě vyhlášení stavu kybernetického nebezpečí, tedy v případě masívního kybernetického útoku, jenž by ohrožoval fungování České republiky.

*(www.nbu.cz)*

## 3.4 ZoKB podrobněji

V předchozích třech kapitolách autor shrnul základní charakteristiky zákona, důvod jeho vzniku a historii. Následující kapitoly přinesou hlubší pohled na zákon tak, jak byl

schválen, budou vysvětleny důležité pojmy a doporučená opatření v oblasti technické i organizační.

### 3.4.1 Důležité pojmy

Aby dávaly následující kapitoly smysl, je nezbytné osvětlit několik pojmů, které se v ZoKB vyskytují.

a) **Významný informační systém (VIS).** Významný informační systém je takový informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Požadavky posuzování rizik jsou zúženy na oblast identifikace a ohodnocení primárních aktiv, která jsou důležitá pro postižení bezpečnostních atributů. Identifikace podpůrných aktiv, která mohou ovlivňovat vlastní rizika, není vyžadována, protože je možné akceptovat riziko spojené s méně formálním postižením vnitřních souvislostí.

   Významné informační systémy jsou, stejně jako KII, upraveny vyhláškou k ZoKB a i v tomto případě bylo čerpáno v řadě norem ISO/IEC27000. NBÚ provedl minimalistickou regulaci vyžadující pouze nejzákladnější bezpečnostní opatření.

b) **Kritická informační infrastruktura (KII).** Částečně byl tento pojem vysvětlen v kapitole 3.1. Jedná se o prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti. Tyto prvky jsou určovány na základě nařízení vlády nebo opatřením obecné povahy. Opatření obecné povahy má konkrétně vymezený předmět, je určeno pro obecně určené adresáty a slouží ke konkretizaci již existujících povinností vyplívajících ze zákona. Pro jednodušší představu, jak opatření obecné povahy může vypadat, lze odkázat například na územní plán, návštěvní řád národního parku nebo i na obecnou amnestii prezidenta.

   Aby mohla KII fungovat dle požadavků zákona, je nezbytné nasazení efektivních bezpečnostních opatření. Jejich nasazení se musí pravidelně vyhodnocovat a v případě potřeby dále optimalizovat. Neméně důležitým faktorem KII je řízení rizik, jehož požadavky pro KII na rozdíl od požadavků pro VIS

obsahují i činnosti spojené s identifikací podpůrných aktiv. Jinými slovy výsledky posouzení rizik u KII budou přesnější, neboť musí být identifikována i aktiva, která jsou určující pro stanovení míry zranitelností. Pro správnou praktickou realizaci je nezbytné vypracovat dokumentaci, dle které bude postupováno.

Kritickou informační infrastrukturu upravuje vyhláška k ZoKB. Bylo primárně vycházeno z norem ISO/IEC27001 a ISO/IEC27002. Oproti normám ISO však došlo na základě výběru pouze podstatných požadavků k velké, ale rozumné regulaci.

c) **Kybernetický prostor.** Jedná se o virtuální oblast, kde pracují, případně spolu prostřednictvím elektronických komunikací komunikují informační systémy, jednotlivé počítače i počítačové sítě. V kybernetickém prostoru jsou zpracovávány a vyměňovány informace a ukládána, sdílena či přenášena data v elektronické podobě.
d) **Bezpečnost informací.** Znamená zajištění důvěrnosti, integrity a dostupnosti informací. To znamená, že informace je dostupná v požadovaném čase, v požadovaném rozsahu a požadovaným (oprávněným) uživatelům. Je chráněná před neoprávněným přístupem a je v úplné (správné), celistvé a nezměněné podobě.

e) **Správce informačního systému.** Zákon určuje, že správcem může být osoba, nebo orgán, které určují účel zpracování informací a podmínky provozování informačního systému.

f) **Správce komunikačního systému.** Stejně jako v případě správce IS, je i správcem KS osoba nebo orgán, které určují účel komunikačního systému a podmínky jeho provozování.

g) **Významná síť.** Významnou sítí je síť elektronických komunikací, která zajišťuje přímé zahraniční propojení do veřejných komunikačních sítí nebo síť, zajišťující přímé připojení ke kritické informační infrastruktuře.

Další důležité pojmy vymezuje vyhláška k ZoKB. Jedná se pouze o pojmy, které jsou pro vyhlášku zásadní, nebo je jejich výklad pro vyhlášku specifický. Pokud některý z pojmů není ve vyhlášce vysvětlen, doporučuje NBÚ využít publikaci „Výkladový slovník kybernetické bezpečnosti“, který vznikal ve spolupráci společnosti AFCEA a NBÚ. Tato publikace je volně dostupná ke stažení v elektronické podobě ze stránek Národního centra kybernetické bezpečnosti.

h) **Systém řízení bezpečnosti informací**. Systémem řízení bezpečnosti informací (ISMS) je část celkového systému řízení orgánu nebo osoby uvedené v ZoKB založené na přístupu daného orgánu nebo osoby k rizikům činností, která je zaměřena na činnosti, vztahující se k bezpečnosti informací. Mezi tyto činnosti patří ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování.

   Samostatně jsou stanoveny požadavky na kritickou informační infrastrukturu, které se ve většině shodují s požadavky stanovené normou ISO/IEC 27001 včetně ročního cyklu přehodnocení. U požadavků na významné informační systémy jsou pak omezeny především takové činnosti, které se váží na zpětnovazební prvky systému řízení bezpečnosti informací. Zpětná vazba je redukována na aktualizaci stanovených plánů v tříletém cyklu. Jedním z hlavních vodítek při výběru opatření pro řízení bezpečnosti informací byly modely vyzrálosti procesů.

i) **Aktivum (primární / podpůrné).** Aktiva jsou důvod, proč vznikl ZoKB. Je to cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu. Dělí se na aktiva primární – informace nebo služby a aktiva podpůrná – zaměstnanci a dodavatelé, kteří se podílejí na provozu nebo bezpečnosti.

j) **Riziko.** Riziko je možnost, že hrozba využije zranitelnost aktiva (KII nebo VIS) a způsobí negativní dopad. Rizika hodnotíme a určujeme jejich přijatelnou úroveň.

k) **Hrozba.** Hrozba je potenciální příčina nechtěné události. Výsledkem může být poškození systému nebo organizace.

l) **Zranitelnost.**.Úmyslná chyba nebo neúmyslný nedostatek v software nebo firmware zařízení komunikační infrastruktury, která může být zneužita potenciálním útočníkem pro škodlivou činnost. Zranitelnosti mohou být známé, ale výrobcem ještě neošetřené nebo skryté a neobjevené. V případě skrytých zranitelností je důležité, kým jsou objeveny dříve. Pokud je objeví dříve útočník, může jich využít k záškodnické činnosti. Pokud je objeví výrobce, bezpečnostní analytik, či uživatel, jsou tyto nedostatky obvykle ošetřeny dříve, než se je pokusí někdo zneužít. Bezpečnostní zranitelnosti jsou proto potenciálními bezpečnostními hrozbami.

m) **Bezpečnostní politika.** Je soubor zásad a pravidel, která zajišťují ochranu aktiv kritické informační infrastruktury a významných informačních systémů. Obvykle se jedná o dokument, který vymezuje bezpečnostní rizika, odpovědnosti za ochranu informací ve společnosti a její úroveň.

n) **Garant aktiva.** Garant aktiva je osoba, která je věcně odpovědná za aktivum KII a VIS a odpovídá za jeho bezpečnost.

o) **Uživatel / Administrátor.** Pojmem uživatel se rozumí každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací. Administrátor je zpravidla osoba, která je odpovědná za správu části informačního systému, pro kterou má zpravidla nejvyšší privilegia přístupu.

p) **Výbor pro řízení**. Skupina osob výkonně zodpovědných za vývoj, řízení a provoz KII a VIS. Měla by být výkonně nápomocna manažerovi kybernetické bezpečnosti v oblasti řízení bezpečnosti informací.

*(výkladový slovník kybernetické bezpečnosti, vyhláška k zákonu o kybernetické bezpečnosti)*

### 3.4.2 Tři základní pilíře zákona

Aby byla ochrana důležitých aktiv efektivní, muselo být zákonem vymezeno několik stěžejních bodů – pilířů, které je nezbytné dodržovat.

a) **Hlášení bezpečnostních incidentů CERT**. Představme si situaci, kdy dochází k útoku na nějakou část infrastruktury. Tento útok může být v lokálním hledisku zcela bezvýznamný. V globálním hledisku se však může jednat o velice nebezpečný jev ve chvíli, kdy by podobné útoky začaly probíhat na další částí infrastruktury. Pokud by první incident nebyl nikam nahlášen, nebylo by možné jej analyzovat a poskytnout tak důležitá data dalším subjektům, které by se mohly na podobný útok připravit a aktivně nebo pasivně se bránit.

b) **Povinnost zavedení bezpečnostních opatření.** Zavedením bezpečnostních opatření se rozumí úkony, které mají za cíl zajistit bezpečnost informací, jejich spolehlivost a dostupnost. Zákon rozlišuje dva typy bezpečnostních opatření - organizační a technická. Povinnost jejich zavedení a dodržování mají pouze subjekty KII a VIS. Na přijetí opatření mají lhůtu jeden rok od nabytí účinnosti zákona nebo od svého určení. Upřesnění bezpečnostních opatření je možné nalézt ve vyhlášce o kybernetické bezpečnosti. Jelikož tato vyhláška byla inspirována rodinou norem ISO/IEC27000, budou mít subjekty, které mají pro tyto normy certifikaci, možnost prokázat svoji připravenost příslušným certifikátem.

c) **Vytvoření legislativy pro případ stavu kybernetického nebezpečí.** Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací. Nastává ve chvíli, kdy je natolik ohrožena integrita či bezpečnost informací jednotlivých systémů v takové míře, že by mohlo dojít k ohrožení zájmů České republiky. O vyhlášení stavu kybernetického nebezpečí rozhoduje NBÚ a tento stav může trvat sedm až třicet dní.

### 3.4.3 Povinnosti jednotlivých správců

Povinnosti jednotlivých správců IS jsou zobrazeny v následující tabulce. Je patrné, že povinnosti jsou přímo úměrné důležitosti subjektu.

**Tabulka 3 - povinnosti správců jednotlivých IS (zdroj: zpracováno dle (AutoCont CZ a.s., 2014))**

| Subjekt/ povinnost | elektronické komunikace | | významné sítě | | informační systémy KII | | komunikační systémy KII | | významné IS (VIS) | |
|---|---|---|---|---|---|---|---|---|---|---|
| hlásit kontaktní údaje | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| detekovat kybernetické bezpečnostní události | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| hlásit kybernetické bezpečnostní incidenty | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| zpracovávat bezpečn. dokumentaci a zavádět bezpečnostní opatření | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| provádět opatření vydaná NBÚ | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

standardní stav | kybernetické nebezpečí

Aby byla předchozí tabulka srozumitelná i laikovi a zároveň nebyla příliš rozsáhlá, pokusí se níže autor práce uvést k jednotlivým subjektům konkrétní příklady.

**Elektronické komunikace** – Jedná se o poskytovatele služby elektronických komunikací nebo subjekty zajišťující síť elektronických komunikací. Mezi tyto subjekty patří například všichni poskytovatelé veřejného internetu, jejich seznam je možné nalézt na stránkách Českého telekomunikačního úřadu.

**Významné sítě** – pojem zahrnuje systémy, zařízení a prostředky pro přenos signálů a vysílání, užívané pro propojení kybernetického prostoru České republiky do zahraničí, nebo sítě, které zajišťují připojení kritické informační infrastruktury ke kybernetickému prostoru. Mezi subjekty, které mají tuto povinnost, patří například CESNET.

**Informační systémy KII** – Do informačních systémů KII patří všechna datová centra (např. Casablanca, Greenhousing) nebo technologické prvky pro satelitní komunikaci (např. navigační systém GALILEO).

**Komunikační systémy KII** – Tato oblasti je obdobou Informačních systémů, pouze její zaměření je na přenos hlasu, videa, ale týká se i poštovních služeb. Jako příklad

subjektů spadajících do této kategorie je možné zmínit mobilní operátory, provozovatele radiových a televizních vysílačů nebo Českou Poštu, s.p.

**Významné IS** – Mezi významné informační systémy patří všechny IS, jejichž nefunkčnost by mohla mít negativní vliv například na fungování orgánu veřejné moci, ale nepatří mezi ně IS, jehož správcem je obec nebo městská část. Příkladem významného IS může být CzechPoint.

### 3.4.4 Hlášení kybernetických incidentů

Zákona o kybernetické bezpečnosti stanoví, jakým způsobem hlásit kybernetické bezpečnostní incidenty. Vznikla dvě pracoviště (vládní a národní CERT), která mají za povinnost informace o kybernetických bezpečnostních incidentech a také kontaktní informace daných subjektů uvedených v §3 ZoKB.

Provozovatelem vládního CERTu je Národní centrum kybernetické bezpečnosti, které je součástí Národního bezpečnostního úřadu. Centrum má za úkol koordinovat spolupráci na národní i mezinárodní úrovni při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům a při předcházení kybernetickým útokům.

Roli národní CERTu v současné době zastává tým CSIRT.CZ, který přijímá kontaktní údaje a hlášení kybernetických bezpečnostních incidentů od orgánů a osob uvedených v §3 ZoKB.

### 3.4.5 Bezpečnostní opatření

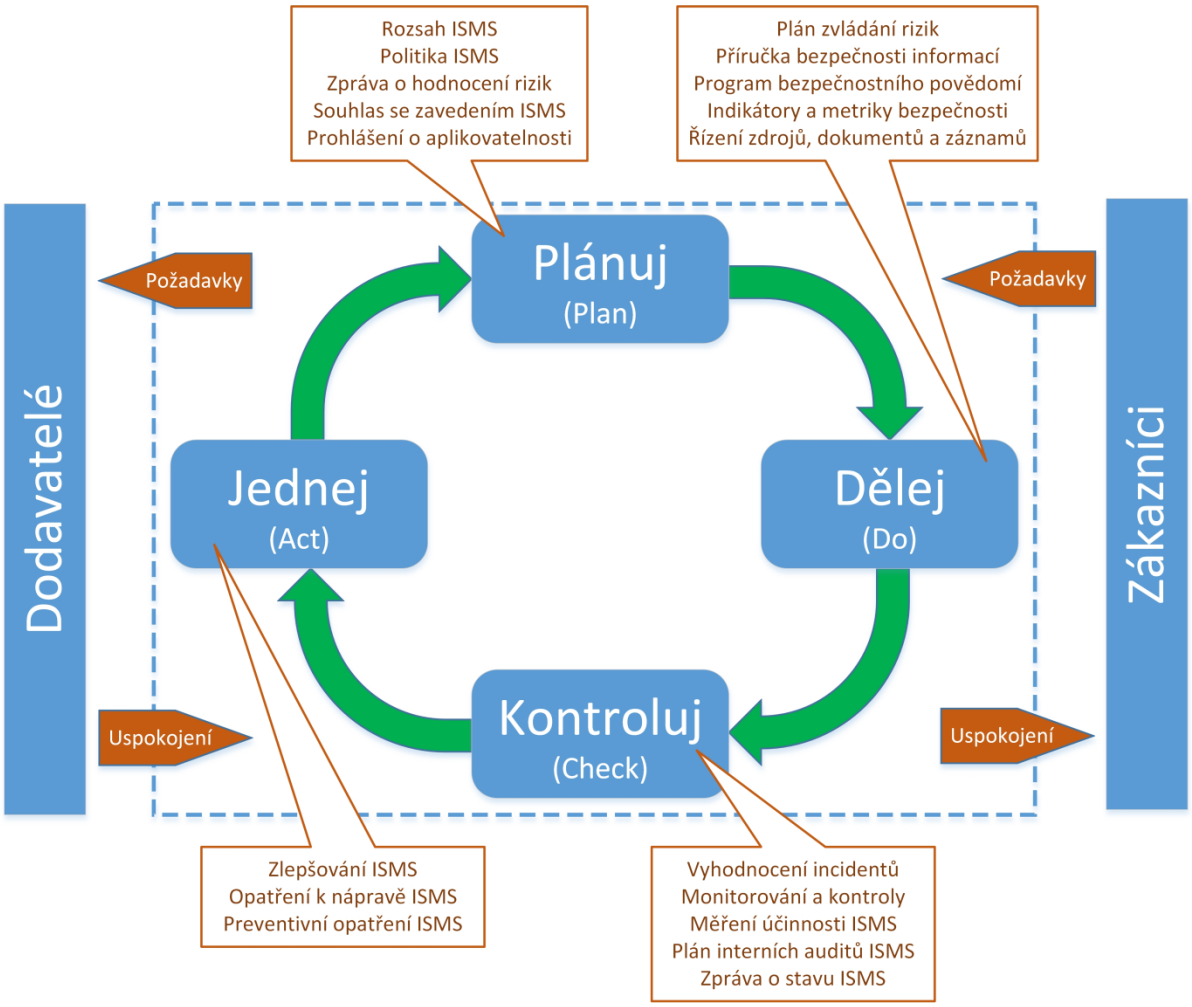
Bezpečnostní opatření jsou vyhláškou o kybernetickém zákonu rozdělena do dvou kategorií a týkají se subjektů KII a VIS. První skupinou jsou opatření organizační, kterých je 13 (jednotlivé paragrafy vyhlášky). Jedná se o procesy, které jsou spojeny s otázkou bezpečnostních rolí, administrativních záležitostí při přidělování oprávnění nebo se jedná o personální procesy.

- **Systém řízení bezpečnosti informací - ISMS (§3).** Požadavky vycházejí z tzv. Demingova cyklu, který se skládá za 4 částí – plánuj, dělej, kontroluj a jednej. Při jeho naplňování vycházelo NBÚ z cyklu, který je obsažen v normě ISO/IEC27001. Pro subjekty KII je požadován celý cyklus, subjekty

VIS byly vynechány některé úkony v oblasti zpětné vazby. Celý cyklus je znázorněn na obrázku 3.

Samotný cyklus, jak je již z obrázku patrné, má celkem čtyři hlavní části, které jsou propojeny do smyčky. Tato smyčka by měla poskytovat ideální techniku pro spojení dosud uvedených nástrojů pro řešení problémů kontinuálního zlepšování.

První fází je „Plánuj“, která zahrnuje plný výzkum problému při navržení změn, které povedou ke zlepšení. V této fázi je nezbytné identifikovat procesy, které mají největší vliv na zlepšování a promyslet plán na studium těchto vlivů. Nezbytné je založení týmu kvalifikovaných pracovníků, kteří tento plán připraví.




**Obrázek 3 - Demingův cyklus ISMS (zdroj: zpracováno dle (Přemysl Pazderka, 2014))**

Po naplánování příslušného zlepšení se celý proces posouvá do fáze „Dělej“. V této fázi by měly být nejprve testovány a posléze i implementovány změny, které byly navrženy ve fázi „Plánuj“. Je nepřípustné provádět změny, které nebyly dokumentovány, výstupy, které vzniknou zaváděním změn, je třeba zaznamenávat, včetně případných neobvyklých událostí.

Ve fázi „Kontroluj“ dochází k analýze dat, sesbíraných v předchozí fázi. Data se analyzují z hlediska stability a schopnosti.

Fáze „Jednej“ je finální fázi jednoho Demingova cyklu. Na základě analýzy výsledků a hodnocení předcházejícího testu se buď:

- přijmou navržené a projednané změny a celý cyklus se za účelem dalšího zlepšování opakuje. Všechny potřebné změny se zavedou do procesů nebo systému

- původní změny se korigují ve fázi plánuj a celý cyklus probíhá nanovo

- **Řízení rizik (§4)**. V rámci zajištění kybernetické bezpečnosti požaduje NBÚ zavést procesy řízení rizik, při kterých jsou identifikována a vyhodnocována rizika, týkající se aktiv KII a primárních aktiv VIS. Následně jsou určena a schválena zbytková rizika, která se popíší ve zprávě o hodnocení rizik. Uvedená opatření musí být uvedena v prohlášení o aplikovatelnosti, termíny realizací a odpovědné osoby jsou součástí plánu zvládání rizik. V tomto paragrafu je také uveden minimální výčet hrozeb a zranitelností, aby bylo možné rizika pro KII a VIS vypočítat.

- **Bezpečnostní politika (§5).** Dokumentace bezpečnostní politiky by v organizaci měla být tak obsáhlá, aby odpovídala počtu řešených oblastí kybernetické bezpečnosti. Pro VIS i KII se jedná o politiky pro 14 základních oblastí, KII obsahuje dalších 7 oblastí, mezi které patří např. technické zranitelnosti nebo mobilní zařízení.

- **Organizační bezpečnost (§6).** Pro KII i VIS je vyhláškou vyžadováno určení bezpečnostních rolí a výboru pro řízení bezpečnosti ICT, pro kritickou infrastrukturu jsou navíc předepsány následující 4 role – manažer bezpečnosti ICT, architekt bezpečnosti ICT, auditor bezpečnosti ICT a garant aktiva. Vyhláška dále stanoví požadavky na kvalifikaci jednotlivých osob. V současnosti je stanovena podmínka řádného vyškolení určených pracovníků a tři roky praxe v oboru.

- **Stanovení bezpečnostních požadavků pro dodavatele (§7).** Jelikož je stále více externích dodavatelů zapojováno do provozu a bezpečnosti ICT u subjektů veřejné správy, je nezbytné, aby s těmito dodavateli byla uzavřena řádná písemná smlouva. Pokud se externí dodavatel podílí nějakým způsobem na správě VIS (provoz, zajištění bezpečnosti), musí písemná smlouva navíc obsahovat ujednání o bezpečnosti informací. Pro KII je navíc vyžadována dohoda o úrovni dodávaných služeb (SLA) doplněna o pravidelné hodnocení rizik. Samozřejmostí je pravidelná kontrola této úrovně služeb včetně odstraňování zjištěných nedostatků.

- **Řízení aktiv (§8).** V kapitole 3.4.1 – Důležité pojmy ZoKB bylo vysvětleno slovo aktivum a to i v souvislosti s VIS a KII. Jelikož byla většina státních agend transformována do prostředí ICT a u dalších je plánována stejný změna, je nezbytné tato aktiva adekvátně chránit a efektivně spravovat. S přesunem těchto aktiv do prostředí ICT narůstá počet hrozeb a zranitelností, kterým jsou vystavena. Řízení aktiv pro objekty KII a VIS dle vyhlášky spočívá v identifikaci a ohodnocení primárních aktiv a určení jejich garanta. Pro KII navíc vyhláška také vyžaduje identifikaci podpůrných aktiv, včetně určení garanta. I na tato aktiva budou aplikována bezpečnostní opatření a budou vyhodnocovány závislosti k aktivům primárním. Pro aktiva KII i VIS je požadováno stanovení klasifikace a zavedení pravidel a pro jejich ochranu. Je nezbytné řádné nakládání s vadnými médii, na kterých jsou nebo v minulosti byla aktiva uložena. Jedná se například o pevné disky z diskových polí, datové pásky nebo i CD a DVD média.

- **Bezpečnost lidských zdrojů (§9).** Zaměstnanci se řadí mezi podpůrná aktiva (kap. 3.4.1.), z tohoto důvodu je nezbytné i tato aktiva chránit. Neznamená to však fyzickou ochranu zaměstnanců, ale ochranu znalostí a informací, ke kterým mají zaměstnanci přístup a mohla by být zneužita a to třeba i nevědomě. Dle společnosti Doverville s.r.o. je až 80% všech bezpečnostních incidentů v organizacích pácháno vlastními zaměstnanci[1]. Proto je nezbytné klást důraz na pravidelná školení zaměstnanců v oblasti bezpečnosti informací, kde jsou všichni dotčení zaměstnanci řádně poučeni, jak s informacemi nakládat. Nutné je provádění pravidelných kontrol, zda jsou všechna nařízení zaměstnanci dodržována. Po ukončení pracovního poměru zaměstnance musí být jasně definováno, jak bude naloženo se všemi svěřenými prostředky. Obvykle je i stanovena doba, po kterou je zaměstnanec vázán mlčenlivostí. Pro oblast KII musí být navíc stanoveny postupy a pravidla pro určení jednotlivých rolí administrátorů a zaměstnanců, bezpečnostní školení jsou ukončena formou závěrečných testů. V případě porušení bezpečnostních pravidel jsou definována disciplinární řízení se zaměstnancem, pokud dojde ke změně postavení zaměstnance, musí být změněna i všechna jeho oprávnění tak, aby odpovídala nové pozici.

- **Řízení provozu a komunikací (§10).** NBÚ vyžaduje pro KII i VIS sledování a vyhodnocování bezpečnostních událostí. Tyto události, jak zmínil v poznámkách k vyhlášce Ing. Přemysl Pazderka, spoluautor vyhlášku k ZoKB, není povinné hlásit CERTu. Všechny bezpečnostní události jsou definované zákonem a jedná se o takové události, které nemají na VIS ani na KII žádný dopad. Pro příklad je možné uvést zafungování antivirového software nebo firewallu. Naopak je pro KII i VIS požadováno stanovení pravidel a postupů, aby byl zajištěn bezpečný provoz. Pro KII jsou tato pravidla specifikována podrobněji.

- **Řízení přístupu a bezpečné chování uživatelů (§11).** Tento paragraf z části souvisí s §9 - Bezpečnost lidských zdrojů a dále jej rozšiřuje. Aby mohl být

[1] http://www.doverville.cz/cs/poradenstvi-a-audity/risk-security/bezpecnost-lidskych-zdroju

efektivně řízen přístup uživatelů ke zdrojům, je nezbytné, aby měl každý uživatel KII nebo VIS unikátní identifikátor (login), na jehož základě mu budou přidělována nebo odebírána práva k jednotlivým IS. Je vyžadována ochrana všech autorizačních údajů a to jak ze strany všech uživatelů, tak ze strany administrátorů, pro KII je navíc nezbytné rušení nepotřebných oprávnění. Jak zmiňuje společnost Cisco, dochází v poslední době k rozvíjení trendu tzv. BYOD[2] zařízení. Nesmí být proto opomenuta ochrana i těchto zařízení. Jedná se obvykle o mobilní přístroje nebo notebooky, které jsou díky bezdrátovému připojení jednodušeji zneužitelné, proto se ochraně těchto zařízení musí věnovat zvýšená pozornost.

- **Akvizice, vývoj a údržba (§12)**. Tento paragraf ZoKB nařizuje subjektům, které patří do KII nebo VIS stanovit bezpečnostní požadavky na informační systémy a zahrnout je do projektu akvizice, vývoje a údržby systému. Zákon dále požaduje identifikaci, hodnocení a řízení rizik, které s touto činností souvisejí. Mezi povinnosti patří zajištění bezpečnosti vývojového prostředí IS a testovacích dat a také testování provedených změn v IS před tím, než je nová verze nasazena do ostrého provozu.

- **Zvládání kybernetických bezpečnostních událostí a incidentů (§13).** Zákon nařizuje pro subjekty KII a VIS vést dokumentaci systému zvládání kybernetických bezpečnostních incidentů. Je rovněž vyžadováno, aby povinné osoby zajistily, že budou oznámeny kybernetických bezpečnostních události od administrátorů, uživatelů a garantů aktiv. O všech těchto oznámeních musí být proveden záznam. Subjekty mají rovněž povinnost všechna oznámení vyhodnocovat, identifikovat a klasifikovat bezpečnostní incidenty a na základě analýzy zjištěných skutečností stanovit nová bezpečnostní opatření k zamezení jejich opakování.

[2] z anglického slovního spojení Bring Your Own Device – přineste si své vlastní zařízení (http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf). Jedná se o soukromé zařízení zaměstnance, se kterým má zaměstnanec povoleno přistupovat k firemním zdrojům a používat jej ke své pracovní činnosti.

- **Řízení kontinuity činností (§14).** Řízení kontinuity činností je proces, který připraví organizaci na řešení nepředvídatelných situací a zmírní jejich případné následky. V případě KII a VIS je velice důležité obnovit provoz postižených struktur v co možná nejkratším čase, aby byla obnovena alespoň jejich předem stanovená minimální úroveň poskytovaných služeb. Výsledkem by mělo být vytvoření havarijních plánů a plánů obnovy, které umožní v případě bezpečnostního incidentu nebo havárie této minimální úrovně dosáhnout. Vyhláška požaduje, aby povinné osoby prováděly řízení kontinuity činností u subjektů KII a VIS. Požadavky vyhlášky vycházejí z požadavků uvedených v normě ISO/IEC 27001. Proces je znázorněn na obrázku 4.


**Obrázek 4 - Business continuity management (zdroj: zpracováno dle (Martin Tobolka, 2011))**

- **Kontrola a audit (§15).** Jak již název napovídá, tento paragraf vyhlášky vychází z metodiky COBIT5 a nařizuje povinným osobám vytvářet vnitřní předpisy a smluvní závazky, které se vztahují k KII a VIS tak, aby bylo možné tyto předpisy a závazky prosazovat. Mezi další povinnosti patří pravidelná

kontrola a dokumentace dodržování stanovených bezpečnostních politik. Audit musí být prováděn osobou s odbornou kvalifikací (dle §36 zákona), kontrola infrastruktury KII by měla být prováděna automatizovanými nástroji. Zjištěné výsledky by měly být odborně vyhodnoceny a na případné zranitelnosti musí povinná osoba reagovat.

Druhou skupinou jsou opatření technická, obsahem je 12 položek (paragrafů vyhlášky). Jedná se o technická zařízení a technologie, které napomáhají zajišťování požadovaných bezpečnostních funkcí.

- **Fyzická bezpečnost (§16).** Pokud vyjdeme z normy ISO/IEC 27001, patří do fyzické bezpečnosti hlavně zabezpečené oblasti, tedy v podstatě bezpečnost budovy a místnosti včetně dveří a oken a elektronické zabezpečovací systémy (EZS). Mezi další části fyzické bezpečnosti patří kontrola vstupu do těchto zabezpečených oblastí nebo jejich ochrana před přírodními katastrofami v podobě požárů nebo povodní. Fyzická bezpečnost není jen o ochraně prostor, ale musí být zajištěna i dodávka elektrického proudu v případě selhání dodávky napájení od hlavního dodavatele a také optimální provozní podmínky v určených oblastech (obvykle serverovny). Prostředků, kterými lze požadavky na fyzickou bezpečnost splnit je několik druhů. Pro zabezpečení přístupu do objektu je možné použít mechanické zábrany ve spojení s EZS, pro kontrolu vstupu lze využít elektronické zámky napojené na čtečky elektronických karet či čipů. Celý objekt a jeho okolí umožní monitorovat speciální televizní okruhy nebo modernější kamerové systémy na bázi síťových prvků. Jako ochranu před výpadkem dodávky napájení se používají výkonné centrální záložní bateriové jednotky (UPS), dieselové elektrocentrály nebo ideálně kombinace obou systémů. Krátkodobé výpadky napájení obvykle pokrývá centrální UPS, která při delším výpadku zároveň poskytuje dostatek času pro nastartování dieselové elektrocentrály.

- **Nástroj pro ochranu integrity komunikačních sítí (§17).** Aby mohly být komunikační sítě chráněny, je nezbytné využívat nástroje, které celý proces zjednoduší, případně jej zautomatizují. Mezi takové nástroje patří firewall,

který na základě předem definovaných řídí datový provoz mezi sítěmi s různou úrovní zabezpečení a důvěryhodnosti. Nejčastěji jsou umisťovány na rozhraní sítí LAN a WAN, ale obvyklé je jejich použití i mezi LAN sítěmi – například pro řízení provozu mezi sítí pro přenos hlasu a videa a sítí datových serverů. Dříve si firewally vystačily se zdrojovou a cílovou IP adresou, případně porty na kterých probíhá komunikace, v současnosti dochází k integraci nástroje zvaného IDS.

IDS (z anglického Intrusion Detection System) je síťový nástroj, který pracuje na úrovni paketů, ve kterých se snaží odhalit škodlivý kód. IDS se obvykle zapojuje mimo hlavní tok dat (pomocí techniky zrcadlení portů), monitoruje více hostitelů najednou a tak je možné odhalit lavinovité šíření viru nebo síťového červa. Autor práce může z vlastní zkušenosti potvrdit, že i jeden prvek IDS v rozsáhlé a členité síti může odhalit šiřitele nebezpečného červa a tím napomoci jeho likvidaci – v roce 2010 docházelo v uzavřené síti k neustálému zamykání účtů uživatelů a to i přes nasazení antivirového software. Podezření padlo na nového červa nazývaného Conficker. Jelikož se jedná o velmi rozsáhlou a členitou intranetovou síť s vlastním správcem v každé lokalitě, nebylo jednoduché odhalit původce ani další šiřitele červa. Díky systému IDS v jedné z lokalit docházelo k informování ostatních správců o stanicích, ze kterých útoky neustále probíhají. S výraznou pomocí systému IDS a aplikací bezpečnostních záplat výrobce operačního systému se podařilo červa zlikvidovat.

Dalším, nástrojem, který výrazně napomáhá omezit útoky na komunikační infrastrukturu je nástroj IPS (z anglického Intrusion Prevention System). IPS se v podstatě chová stejně jako systém IDS s rozdílem, že je zapojena přímo jako jeden z prvků, přes které probíhá veškerý provoz. Pokud IPS zjistí dle svého pravidla nestandardní komunikaci, rovnou tuto komunikaci zablokuje. Oproti systému IDS tedy poskytuje okamžité zastavení podezřelé činnosti, která probíhá v síti. IPS se ale špatnou konfigurací může změnit v dvousečnou zbraň. V případě špatné definice pravidla nežádoucího provozu může dojít i k zablokování provozu, který blokován být nesmí. Aby se předešlo dlouhodobějším výpadkům komunikace z důvodu nastalého problému s IPS, je

k IPS paralelně zapojen tzv. bypass switch. Při normální činnosti tento switch směřuje data do systému IPS, při výpadku elektrické energie nebo při problému s IPS dojde k přepnutí provozu přímou cestou mimo IPS a to nezávisle na napájení, jelikož se jedná o pasivní zařízení.

Neméně důležitým faktorem, který může ovlivnit schopnost systému ustát útok, jsou použité síťové prvky. Při potřebě vybudovat robustní komunikační infrastrukturu, je vhodné užívat prvky renomovaných výrobců, kteří jsou technologicky na dobré úrovni. Tyto prvky jsou konstruovány na vysokou zátěž, zároveň jim výrobce věnuje po předem stanovenou dobu, maximální péči v podobě bezpečnostních záplat, oprav a v neposlední řadě i přidáváním nových vlastností nebo funkcí. I sebelepší síťové prvky však nemusí stačit, pokud dojde k vybudování síťové infrastruktury, která bude nevhodně navržena. Je tedy nezbytné použít design od certifikovaných systémových inženýrů, kteří mají dlouholeté zkušenosti a jsou schopni při dobré zadávací dokumentaci analyzovat nejen současné problémy, ale i problémy, které mohou nastat v budoucnosti – například rozšiřováním stávající sítě.

- **Nástroj pro ověřování identity uživatelů (§18).** S ověřováním identity se dnes v soukromé sféře setkáváme doslova na každém kroku. Pokud chceme odeslat nebo přečíst elektronickou poštu, sdělit svým kamarádům, co právě děláme nebo si do cloudového úložiště uložit své fotografie. Při každé z těchto činností jsme vyzváni k zadání uživatelského jména (identity) a hesla. Jsou hesla, která používáme dostatečně bezpečná? Dle některých internetových deníků[3] je i v roce 2014 nejčastěji používané heslo „123456“, následováno heslem „password“. ZoKB na tento problém myslí a nařizuje pro KII i VIS, aby měli všichni uživatelé i administrátoři heslo o takové složitosti, že bude obsahovat alespoň jedno velké písmeno, jedno malé písmeno, jednu číslici a jeden speciální znak, jeho minimální délka bude 8 znaků a maximální doba platnosti 100 dní. Pro KII jsou navíc stanoveny zvýšené nároky v podobě

[3] Společnost SplashData analyzuje na konci každého roku hesla, která byla na internetu kompromitována a vytváří z nich seznam 25 nejpoužívanějších resp. nejvíce zneužitých. Souhrn analýzy roku 2014 nabízí např. stránka http://www.prweb.com/releases/2015/01/prweb12456779.htm.

kontroly dříve použitých hesel, zamezení vícenásobné změny hesla jednoho uživatele během definovaného období (nejméně 24 hodin) a vynucení minimální délky hesla u administrátorských účtů na 15 znaků. Všechny tyto nároky je možné splnit pomocí dnes již běžně užívaných nástrojů, mezi které patří například Cisco ISE, Cisco ACS, Microsoft Active Directory nebo LDAP (Lightweight Directory Access Protocol), který je využíván na UNIXových systémech.

- **Nástroj pro řízení přístupových oprávnění (§19).** Analýza předcházejícího paragrafu osvětlila nutné podmínky zabezpečení uživatelského účtu pro přístup do informačních systémů nebo administrace. Nezbytnou součástí ochrany VIS i KII je řízení přístupových oprávnění k samotným aplikacím a datovým souborům, dále pak správa a řízení oprávnění pro čtení, zápis dat a změnu oprávnění. Pro KII je povinnost rozšířena o povinnost zaznamenávat použití všech přístupových oprávnění. Jako nástroj pro řízení přístupových oprávnění je možné použít IPS, firewally nebo v případě BYOD (soukromá zařízení uživatelů) protokol 802.1x. V součinnosti s těmito nástroji je nezbytné definovat jednotlivá práva na úrovni aplikací a operačních systémů.

- **Nástroj pro ochranu před škodlivým kódem (§20).** Mezi neméně důležité nástroje pro ochranu aktiv subjektů KII i VIS patří antivirové a antimalwarové softwary. ZoKB pro oba subjekty vyžaduje použití nástrojů pro antivirovou ochranu a to v rozsahu kontroly od koncových pracovních stanic po servery a sdílená datová úložiště. Důraz by měl být kladen na častou, pravidelnou automatickou aktualizaci definic a signatur, aby mohlo antivirové řešení co nejrychleji reagovat na nově vzniklé hrozby. V případě „útoku nultého dne“, který na svých stránkách blíže popisuje například internetový deník WIRED[4] je vhodná kontrola spouštěných aplikací pomocí whitelistu, což je seznam povolených aplikací. Antivirový software by měl být centrálně spravovaný, aby byl administrátor okamžitě vyrozuměn o záchytu infekce. Jako vhodný doplněk antivirového řešení mohou být užita specializovaná síťová

[4] http://www.wired.com/2014/11/what-is-a-zero-day

antimalwarová zařízení. Antivirových a antimalwarových řešení existuje v současnosti nepřeberné množství. Některá řešení však nedisponují centralizovanou správou klientských stanic nebo jejich výsledky nejsou uspokojivé. Každoročně provádí několik specializovaných internetových magazínů[5] porovnání nejznámějších antivirových řešení, která mohou usnadnit výběr korporátního řešení.

- **Nástroj pro zaznamenávání činností KII a VIS, jejich uživatelů a správců (§21).** Aby mohl být jednodušeji odhalen původce hrozby nebo důvod jejího vzniku, nařizuje zákon pro subjekty VIS i KII použití nástroje nebo nástrojů pro zaznamenávání činností, které zajistí sběr informací o provozních a bezpečnostních událostech. Zaznamenávány by měly být události, mezi které se řadí:
    - typ činnosti
    - přesný čas události
    - identifikace technického aktiva, které činnost zaznamenalo
    - identifikaci původce a místa činnosti
    - úspěšnost či neúspěšnost pokusu

  Dále je nezbytné ochránit důležité informace před neoprávněným čtením a změnou. U subjektů KII i VIS je povinné zaznamenávat:

    - přihlášení a odhlášení uživatelů a administrátorů
    - činnosti provedené administrátory
    - činnosti vedoucí k navýšení oprávnění
    - neúspěšné činnosti
    - spuštění a ukončení práce systému
    - varovná nebo chybová hlášení
    - přístupy logům
    - pokus o manipulaci s logy
    - použití mechanismů autentizace, včetně změn údajů k přihlášení
    - neprovedené činnosti v důsledku nedostatku oprávnění

[5] http://www.av-comparatives.org nebo http://www.av-test.org

- **Nástroj pro detekci kybernetických bezpečnostních událostí (§22).** Aktivním technickým nástrojem, jehož použití vyžaduje ZoKB je nástroj pro detekci kybernetických bezpečnostních událostí. Subjekty KII i VIS mají za povinnost takový nástroj používat k zajištění ověření, kontroly a případné blokování komunikace mezi vnitřní a vnější sítí, pro KII platí přísnější pravidla v podobě ověření, kontroly a případného blokování komunikace v rámci vnitřní komunikační sítě a v rámci určených serverů. Pro detekci bezpečnostních událostí je možné využít například produkty společnosti Cisco, SourceFire nebo řešení INVEA FlowMon a Arbor Networks DDoS.

- **Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (§23).** Aby bylo smysluplné použití nástrojů dle §22, je povinnost pro subjekty KII použít technické prostředky, které dokáží získaná data ukládat, vyhodnocovat a poskytovat informace o kybernetických bezpečnostních událostech (KBU) bezpečnostním rolím. Vyhodnocování by mělo probíhat nepřetržitě, tak aby bylo zajištěno využívání získaných informací o KBU k optimalizaci bezpečnostních vlastností informačních a komunikačních technologií. Další z podmínek, které jsou na KII kladeny je stanovení bezpečnostní politiky pro použití a údržbu nástroje a pravidelná aktualizace nastavených pravidel pro zpřesnění chodu nástroje pro vyhodnocování KBU. Jako nástroje pro sběr a vyhodnocení mohou být zmíněny produkty RSA Envision, AccelOps nebo Splunk.

- **Aplikační bezpečnost (§24).** Tento paragraf ZoKB nařizuje subjektům VIS i KII, jak se starat o aplikační bezpečnost. Oba typy subjektů jsou povinny provádět bezpečnostní testy aplikací, které jsou přístupné z vnější sítě před uvedením do provozu a po každé zásadní změně bezpečnostních mechanizmů, subjekty KII jsou navíc vázány povinností zajistit ochranu aplikací a informací dostupných z vnějších sítí před:
    - neoprávněnou činností
    - popřením provedených činností
    - kompromitací nebo neautorizovanou změnou

- transakcí před nedokončením, nesprávným směrováním, neautorizovanou změnou, kompromitací, neautorizovaným duplikováním, opakováním

Bezpečnostní testy aplikací se mohou provádět způsobem, který se nazývá „etický hacking“. Podrobný popis této problematiky přesahuje rámec této práce, podrobnosti a úskalí etického hackingu je možné nalézt například v knize Hacking – manuál hackera *(HARRIS, 2008, s. 25-40)*, ve které je možné nalézt i výčet penetračních nástrojů, které jsou k této činnosti používány - například Core IMPACT, Immunity CANVAS nebo Metasploit *(HARRIS, 2008, s. 164-179)*.

- **Kryptografické prostředky (§25).** Technické opatření, které má za úkol ochránit integritu a důvěryhodnost citlivých dat, se nazývá kryptografické prostředky. Jelikož mohou být data uložena na vyměnitelných médiích, přenášena po komunikačních sítích nebo ukládána na mobilní zařízení, mají VIS i KII za povinnost stanovit politiky pro používání kryptografické ochrany, aby byla zajištěna ochrana důvěryhodnosti a integrity těchto dat a mohla být prokázána odpovědnost za provedenou činnost. Aby byla ochrana účinná, je nezbytné zvolit správně typ i sílu kryptovacího prostředku. Pro subjekty KII jsou z tohoto důvodu stanoveny minimální požadavky na sílu šifrovacích klíčů. Použité mohou být symetrické algoritmy (např. AES, RC4, SNOW 2.0), asymetrické algoritmy (např. DSA, ECDH), pro hash je možné využít funkce SHA2, RIPEMD-160 nebo Whirpool. Použití aktivních prvků s podporou požadovaných kryptografických standardů je samozřejmostí, stejně jako nasazení nástroje pro správu mobilních zařízení (MDM).

- **Nástroje pro zajištění vysoké úrovně dostupnosti (§26).** Pojem „vysoká úroveň dostupnosti“ je dnes převážně spojován se zkratkou SLA, která označuje úroveň poskytovaných služeb. Jak řešit tento problém, pokud nejsou prvky KII spravovány pomocí servisní smlouvy bylo částečně zmíněno v §17 v souvislosti s kvalitním návrhem síťové infrastruktury. Konkrétně se jedná o kvalitní návrh infrastruktury, ve kterém je počítáno s nasazením prvku

v módu redundance, aby při výpadku hlavního prvku převzal jeho činnost prvek záložní nebo aby došlo pouze k snížení propustnosti, nikoliv k celému výpadku. Současně je vhodné vytvořit sklad náhradních technických aktiv, který umožní rychlou výměnu vadného prvku a tím návrat sítě do standardního stavu, zároveň by všechny použité prvky měly být odolné proti útokům, které jsou schopné snížit dostupnost služeb. V případě servisní smlouvy s externím dodavatelem služeb a infrastruktury nesmí být ve smlouvě opomenuty důležité části jako je požadavek na redundanci kritických komponent, sklad náhradních komponent a servis prvků v režimu 24/7/365.

- **Bezpečnost průmyslových a řídicích systémů (§27)**. I poslední paragraf výčtu technických opatření se týká pouze subjektů KII a jak napovídá jeho název, týká se převážně infrastruktury zařízení, které jsou řízeny specializovanými průmyslovými systémy. Zákon nařizuje, aby k těmto průmyslovým a řídicím systémům byl omezen jak fyzický, tak vzdálený přístup. Jednotlivé systémy musí být chráněny před známými zranitelnostmi a musí být zaručeno bezprostřední obnovení chodu po selhání v důsledku kybernetického bezpečnostního incidentu. Mezi zařízení, které splňují definici, je možné zahrnout například elektrárny nebo teplárny.

# 4 Shrnutí teoretické části

Úkolem teoretické části diplomové práce bylo čtenářovi osvětlit problematiku termínu ISMS, který je velice důležitý ve vztahu k bezpečnosti informací organizace. Z pojmu ISMS přešel autor plynule k normám řady ISO/IEC27000, aby bylo možné v navazujících kapitolách analyzovat Zákon o kybernetické bezpečnosti. V kapitole 1 a jejích podkapitolách se autor práce dopodrobna věnoval třem nejdůležitějším normám, které zákon č.181/2014 Sb. využívá. Důležité pojmy zákona jsou definovány obdobně jako v normě ISO/IEC27000, některé definice byly zjednodušeny bez dopadu na význam, některé byly naopak přidány z důvodu specifika jejich výkladu do vyhlášky, která zákon provází.

V další části teoretické části se autor věnoval frameworku COBIT. Byla představena historie frameworku, vysvětleny byly jeho hlavní principy. COBIT nabízí, na rozdíl od norem ISO/IEC27000, ucelený pohled na řízení informační bezpečnost organizace. Od verze 4.1 v sobě zahrnuje metodiku RiskIT, tedy metodiku pro řízení IT rizik. V části, která byla nazvána „COBIT5 for Risk“ je možné nalézt desítky scénářů, které se této problematice věnují. Ty však nezacházejí do přílišných detailů, což je jeden z hlavních rozdílů mezi COBIT a ISO/IEC27000 v souvislosti s bezpečnosti informací. Další rozdíly je možné nalézt v kapitole 2.3, kde se jim autor práce věnuje včetně jejich detailního rozboru.

V poslední kapitole teoretické části autor detailně analyzuje Zákon o kybernetické bezpečnosti, vysvětluje důležité pojmy, které jsou zákonem používány. Následně jsou představeny tři základní pilíře zákona a jsou vymezeny povinnosti správců subjektů, kterých se zákon týká. Pro úplnost a jednodušší orientaci v problému jsou uvedeny příklady těchto subjektů včetně jejich zařazení do příslušných skupin. V poslední části kapitoly o Zákonu o kybernetické bezpečnosti jsou detailně analyzovány obě skupiny bezpečnostních opatření – tedy opatření organizačních a opatření technických. Organizační opatření se týkají procesů, které jsou spojeny s otázkou bezpečnostních rolí, administrativních záležitostí při přidělování oprávnění, zároveň do této skupiny patří procesy personálního charakteru. Opatření technická se věnují problematice technických zařízení a technologií, které napomáhají zajišťování požadovaných bezpečnostních funkcí.

# 5 Bezpečnostní rizika komunikační infrastruktury

Jelikož autor pracuje ve státním subjektu, jehož zaměstnanci mají přístup k mnoha citlivým údajům ve smyslu zákona č. 101/2000 Sb.[6], rozhodl se prověřit, zda současná opatření, ať už technická či organizační, tyto údaje dostatečně chrání. Subjekt, ve kterém autor pracuje, zaměstnává více než 1400 zaměstnanců, někteří z nich jsou oprávněni nahlížet do informačních systémů, které mohou obsahovat osobní nebo dokonce citlivé osobní údaje nebo tyto údaje mají k dispozici přímo na svých osobních počítačích. Více než 400 z těchto zaměstnanců pracuje v objektu, který je předmětem této analýzy. Z tohoto důvodu je nezbytné dodržovat určitá organizační opatření a v oblasti komunikační infrastruktury nasazovat taková technická opatření, která znemožní zneužití těchto dat.

## 5.1 Fyzická bezpečnost

V kapitole 3.4.5 (§16) autor stručně nastínil problematiku fyzické bezpečnosti z pohledu Zákona o kybernetické bezpečnosti. Fyzickou bezpečnost tvoří systém opatření, která mají zabránit nebo ztížit přístup k informacím těm osobám, které s nimi nejsou oprávněny nakládat, popřípadě přístup nebo pokus o něj zaznamenat. *(Perdikaris, 2014)*

### 5.1.1 Základní oblasti fyzické bezpečnosti

Fyzická bezpečnost se rozděluje do několika samostatných celků, které vymezují použití jednotlivých bezpečnostních mechanismů.

a) Bezpečnost perimetru (Perimeter security) - ochrana perimetru má za úkol detekovat nepovolené překročení hranice určité oblasti. Tato oblast bezprostředně obklopuje prostor, který obsahuje chráněný informační systém. Tento prostor si můžeme představit například jako pozemek okolo objektu. Dle důležitosti jsou aplikována technologická bezpečnostní opatření, mezi která mohou patřit vysoké ploty nebo zdi, ale i aktivní systémy využívající paprsek nebo kamery, které celý prostor monitorují a v případě jeho narušení mohou informovat ostrahu. V případě užití kamerových systémů je nezbytné postupovat dle zákona č. 101/2000Sb, orientační návod, jak vhodné použít metodiku s názvem „Provozování kamerových systémů“, kterou je možné nalézt na stránkách Úřadu

[6] zákon o ochraně osobních údajů

pro ochranu osobních údajů, ve složitějších nebo nejasných případech je doporučováno kontaktovat s dotazem přímo samotný úřad *(Úřad pro ochranu osobních údajů, 2012)*. Oblast je vyobrazena na obrázku č. 5 žlutou barvou.

b) Kontrola přístupu (access control) – tato část fyzické bezpečnosti zajišťuje kontrolu při vstupu za perimetr, tedy obvykle do objektu, ve kterém se vyskytuje chráněné aktivum (např. uložené informace v elektronické podobě). Oblast je vyobrazena na obrázku č. 5 barvou červenou. Kontrolovat by se měly veškeré vstupy do objektu (vchody, brány pro vjezd vozidel), v případě, že byl jako perimetr zvolen plášť budovy, je nezbytné použít mechanismy kontroly přístupu i na zajištění jednotlivých oken a dalších technologických otvorů v tomto plášti, které by mohly být zneužity. Jako vhodnou kombinaci si lze představit mříže na oknech, které zastanou funkci pasivní bezpečnosti a elektronická čidla umístěná uvnitř místnosti na jednotlivých oknech, která v případě narušení prostoru upozorní ostrahu objektu. Pro kontrolu přístupu je možné využít pracovní síly – vrátného, který dle nastavených pravidel kontroluje osoby, které do chráněného objektu vstupují nebo jej opouštějí, vhodné je použití systémů EKV (elektronická kontrola vstupu), které vpustí pouze osoby, které vlastní přístupovou čipovou kartu nebo znají nastavené heslo.

c) Vnitřní bezpečnost (interior security) – Ochrana vnitřní bezpečnosti, jak je již patrné z názvu, má za cíl ochránit prostory a systémy, které obsahují citlivá data nebo s nimi pracují. Taková oblast nebo oblasti by se v obrázku 5 vyskytovaly uvnitř červené oblasti. Ochrana bude tedy zaměřena na jednotlivé kancelářské místnosti, ale je nezbytné myslet i na centrální klimatizaci nebo garáže, ve kterých jsou parkována vozidla obsahující nepřenosné technologické prvky, které taktéž citlivé informace mohou obsahovat. Vhodný pasivní technologický prvek pro ochranu vnitřní bezpečnosti jsou kvalitní dveře ve spojení s vhodnou vložkou zámku, které poskytnou zabezpečení hlídané místnosti po dobu dlouhodobé nepřítomnosti osob, které do těchto prostor pravidelně přistupují. Nezbytné je však tyto prvky kombinovat s prvky aktivní ochrany, tedy ideálně se systémem EKV, kamerovým systémem, který se umístí do přístupové cesty a aktivními

senzory (mikrovlnné, infračervené, magnetické kontakty) uvnitř místnosti, které v případě průniku spustí poplach.

**Obrázek 5 - Fyzická bezpečnost - Perimetr (zdroj: autor a http://mapy.google.cz)**

Jako doplněk vnitřní bezpečnosti může být využito technologických prvků, které znemožní nebo alespoň ztíží fyzickou manipulaci s chráněnými zařízeními, tedy jejich rozebrání zničení nebo odnesení. Mezi tyto prvky mohou patřit například zámky rackových skříní, zámky na počítačích nebo i plomby, které sice nezabrání rozebrání přístroje, ale dokáží upozornit, že s ním docházelo k nějaké manipulaci. Všechna tato opatření jsou doplňkovým stupněm fyzické ochrany.

Mezi zvláštní opatření fyzické bezpečnosti bezesporu patří také ochrana před výpadkem dodávky elektrické energie, bez které by žádné technické opatření nemohlo plnit svou úlohu. Všechny elektronické systémy by měly být vybaveny záložním systémem napájení, důraz musí být kladen i na typ použitých elektronických zámků s ohledem na bezpečnost osob. Všechny zámky, které se nacházejí v koridoru značené únikové cesty, by se po vyčerpání záložní elektrické energie měly odemknout, aby – například v případě

požáru – mohly osoby, které se v objektu nacházejí, bezpečně opustit ohrožený prostor. *(Kingsley-Hefty, 2013)*

### 5.1.2 Organizační opatření

Fyzická bezpečnost není pouze o technologických opatřeních, ale nezbytná jsou i opatření organizační. Mezi tato opatření patří určení osob nebo subjektů, které jsou zodpovědné za provádění kontroly fyzické bezpečnosti, pravidelné testování funkčnosti ochranných systémů, ale mají také za povinnost spravovat databázi osob, které mají do objektu nebo jeho určitých částí přístup. Organizační opatření se ale týkají i ostatních osob, které jsou autorizovány pro vstup do objektu. *(Ricks, 2014)* Tyto osoby musí být každoročně školeny v oblasti bezpečnosti informací, v případě, že je jejich činnost spojena s utajovanými informacemi, jsou povinny – při vyšším stupni utajení – podstoupit pravidelnou prověrku NBÚ[7]. Jako samozřejmost by měla být strukturovaná dokumentace, ve které budou přesně veškeré prostředky popsány, včetně způsobu jejich využití ve fyzické ochraně hlídaných aktiv. Mapa všech zařízení s přesným umístěním je vhodným doplňkem této dokumentace.

## 5.2 Analýza fyzické bezpečnosti objektu

Autor práce by rád úvodem sdělil, že není zaměstnán jako pracovník, který nemá na starost fyzickou bezpečnost organizace a tak jsou následující řádky pouze jeho subjektivním pohledem na problematiku fyzické bezpečnosti v organizaci, ve které pracuje. Autor rovněž mohl přehlédnout skrytý prostředek, který zabezpečuje místo, které je v analýze zmíněno jako možné riziko. Z důvodu povahy organizace není vhodné zveřejňovat její název, účel či umístění, aby tato práce nemohla sloužit jako návod a být zneužita pro napadení objektu.

Objekt, který se autor pokouší analyzovat, se nachází na otevřeném prostranství v městě, ve které m žije více než 25000 obyvatel. V blízkosti objektu se nachází sídliště, ale i zdravotnické centrum, takže jde o oblast s velkým výskytem obyvatel. Objekt se skládá z šesti podlaží, z toho jedno je pod úrovní terénu. Do objektu je možné vstoupit jedním ze čtyř vstupů, dle úrovně oprávnění.

[7]bezpečnostní prověrky NBÚ se řídí zákonem 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

### 5.2.1 Perimetr

Perimetr objektu tvoří z jedné strany zatravněná plocha, která je volně přístupná, další tři strany perimetru jsou vymezeny nízkým plotem, který je v několika místech přerušený vjezdovými branami, které jsou neustále otevřené. Nejedná se tedy o opatření, které by pasivně zamezovalo vstupu do perimetru, ale pouze jej vymezuje. Perimetr je hlídán cca desítkou kamer, které jsou pod nepřetržitým dohledem několika operátorů. Jelikož je perimetr otevřený, není možné, aby kamerový dohled rozpoznal, zda ten, kdo se v perimetru vyskytuje, je zaměstnanec nebo potenciální útočník, který aplikuje metodiku zvanou „Red teaming“[8].

### 5.2.2 Opatření pro perimetr

Vzhledem k povaze perimetru analyzovaného objektu lze vytknout fakt, že ač je perimetr ze tří stran obklopen plotem, přístup do něj je v podstatě volný i pro osoby, které nejsou zaměstnanci organizace. Tím je umožněno bližší zkoumání možných přístupových cest do objektu, aniž by pohyb takových osob alespoň zvýšil pozornost ostrahy. Ostraha, která je na tento fenomén zvyklá, ztrácí pozornost nebo pohyb všech osob v perimetru ignoruje do té doby, než dojde k nějakému incidentu.

Prvním doporučením autora je uzavírat příjezdové brány perimetru tak, aby byl minimalizován pohyb osob, které nemají pracovní nebo smluvní vztah směrem k organizaci. Samotný fakt, že při zavřené bráně musí případný narušitel překonat plot, je na kamerovém systému dobře rozpoznatelný a mohou tak být okamžitě uvedena v činnost předem definovaná protiopatření. Z hlediska kontroly části perimetru, která není ohraničena mechanickou zábranou, doporučuje autor zvýšit počet kamer tak, aby byl pokryt celý prostor okolo obvodového pláště budovy v těchto místech. Narušení tohoto prostoru i přes jeho otevřenost běžně nenastává a tak každý pohyb osoby nebo osob může opět znamenat pokus o nalezení slabého místa.

### 5.2.3 Kontrola přístupu za perimetr

Jak bylo v minulé kapitole zmíněno, překonání perimetru zkoumaného objektu není nesnadný úkol. O to důležitější je nutnost kvalitní ochrany přístupu za perimetr. V kapitole 5.2 autor zmiňuje možnost přístupu do objektu čtyřmi místy – jedná se o 2 vstupy pro

[8] Red teaming je jednou z technik penetračního testování a využívá širšího pohledu na hledání cest dovnitř organizace. Název je odvozený od žargonu armády, kdy červený (red) team označuje nepřítele.

osoby a 2 vjezdy pro vozidla. Oba vjezdy jsou neustále monitorovány několika kamerami, takže probíhá kontinuální monitoring všech vozidel, která do objektu přijíždějí nebo jej opouštějí. Jeden z vjezdů je plně automatický, ovládaný osobní zaměstnaneckou přístupovou kartou. Z důvodu plné automatizace jsou nastolena přísná pravidla, která byla schválena vedením organizace a uvedena v příslušném nařízení. Každý zaměstnanec je povinen seznámit se, jak se po průjezdu branou chovat, aby nemohlo během samočinného zavírání brány dojít k průniku neautorizovaných osob do objektu nebo naopak z objektu ven. Tento vjezd je určen pouze pro vozidla organizace, ve výjimečných případech je možné jej po dohodě využít i pro vozidla smluvních stran – například při odvozu kontejneru se sutí apod.

Druhý vjezd do objektu je určen jak pro vozidla organizace, tak pro zásobování. Tento vjezd je užíván převážně během pracovní doby, je střežen pracovníkem ostrahy, který může manuálně ovládat mechanickou závoru. Aby bylo možné využít tento vjezd do objektu smluvním partnerem, je potřeba vlastnit dlouhodobé povolení od vedení organizace nebo potřebu vjezdu nahlásit předem kompetentnímu pracovníkovi, který o povolení bezodkladně rozhodne. I tento vjezd je monitorován několika kamerami, jejichž zorná pole se důmyslně překrývají[9]. Součástí tohoto vjezdu je i samostatný vchod pro zaměstnance.

Vchod pro zaměstnance je z vnější části budovy monitorován stejnými kamerami jako vjezd popisovaný na konci minulé kapitoly. Aby bylo možné použít zaměstnanecký vchod, musí zaměstnanec použít zaměstnaneckou kartu (proběhne autentizace systémem EKV). Po překonání vstupních dveří může být zaměstnanec navíc vyzván pracovníkem ostrahy, aby zaměstnaneckou kartu předložil k nahlédnutí. Tato procedura je čistě na zvážení pracovníka ostrahy (nenajdeme zde žádné cedulky z dob minulých, které požadují předložení karty bez vyzvání), v případě, že pracovník ostrahy nepojme podezření, jsou poslední překážkou před vstupem do budovy druhé dveře se systémem EKV.

Hlavní vchod do budovy je jediný vchod, který může využívat pro přístup do budovy organizace také široká veřejnost. Pro zaměstnance platí stejná pravidla, jako v případě

[9] I přes zmínku na začátku hlavní kapitoly, že autor nepracuje jako pracovník zajišťující fyzickou bezpečnost, má k výstupu z kamerového systému přístup z důvodu monitorování funkčnosti a nastavování jednotlivých kamer, které jsou součástí síťové infrastruktury.

vchodu pro zaměstnance s tím rozdílem, že z hlavního vchodu mohou využít čtyř možných přístupových cest a to pouze přiložením zaměstnanecké karty. Pokud si je zaměstnanec ostrahy jistý přicházející osobou, může sám dálkově odjistit dveře a zaměstnance tak pustit dál. V případě návštěvy nebo jednání cizí osoby je nezbytné, aby byla osoba vyzvednuta pracovníkem organizace. V případě že osoba není dopředu nahlášena, dojde k její identifikaci a zápisu do knihy návštěv. Vzhledem k povaze organizace je nepřípustné, aby se taková osoba pohybovala po objektu samostatně, bez doprovodu. Při opouštění budovy následuje opačná procedura, tedy je proveden zápis do knihy návštěv o čase odchodu.

### 5.2.4 Opatření pro zlepšení kontroly přístupu za perimetr

Autor práce se domnívá, že jedno z rizik spočívá ve vjezdu vozidel, která pravidelně dováží různé zboží na základě dlouhodobé dohody. I v tomto případě hraje hlavní roli lidský faktor – tedy pracovníci ostrahy, kteří tato vozidla vpouštějí za hranice budovy bez řádné kontroly zavazadlového prostoru. K dobru budiž řečeno, že pro možnost vstupu do objektu ze dvora budovy je nezbytné použít zaměstnaneckou kartu, avšak zde si autor dokáže představit využití nějakého způsobu sociálního hackingu[10].

Obdobný problém může nastat u hlavního vchodu. Zde se také projevuje lidský faktor strážných, kteří občas nechávají jedny přístupové dveře do nitra budovy otevřené. Občas nastane situace, ve které je strážný natolik zaměstnán jinou neodkladnou činností (vyřizování telefonátu) a nemusí tak zaznamenat osobu, která by mohla téměř nepozorovaně proniknout těmito dveřmi do budovy. Dálkové ovládání dveří není navíc podmíněné přiložením zaměstnanecké karty, takže otevřít dveře lze i bez autorizace ke vstupu. Autor by doporučil minimalizovat selhání lidského faktoru častým školením zaměstnanců ostrahy, které by doplnil vydáním nařízení, kterým by byl striktně definován režim všech přístupových cest. V případě, že by byl zjištěn prohřešek proti nařízení vedení společnosti, tento prohřešek kázeňsky trestat.

Jako jeden z problémů byla zmíněna možnost dálkového otevření vstupních dveří do objektu pracovníkem ostrahy bez toho, aby měl pracovník povinnost autentizace. Tato možnost, dle autora práce, zcela ruší jakoukoliv snahu o zpřístupnění budovy pouze

[10] Sociální hacking je technika, při které se využívá hlouposti nebo nepodezíravosti některých jedinců. Jako příklad je možné uvést situaci, kdy osoba, která se bude snažit o přístup do objektu, požádá kolemjdoucího, zda by mu neotevřel dveře a nepodržel je, protože má v rukou těžké břemeno.

osobám, které obdrží autorizaci. Celé ovládání je navíc umístěno v místě, které je viditelné z velké části vstupní haly a to, že je celý prostor monitorován několika kamerami, nezabrání potenciálnímu útočníkovi proniknout do budovy.

### 5.2.5 Vnitřní bezpečnost objektu

Další částí fyzické bezpečnosti objektu je zajištění jeho vnitřní bezpečnosti. Toto zabezpečení se v podstatě prolíná s kontrolou přístupu za perimetr – tedy v místech přístupu do chráněné části budovy. Analyzovaná budova je z větší části průchozí bez nutnosti používat přístupové karty, pouze pro několik vyhrazených sektorů tato povinnost zůstala. Vzhledem k počtu zaměstnanců, kterých je v této budově více než 500, je při troše „drzosti“[11] téměř nemožné odhalit osobu, která se po budově pohybuje bez patřičné autorizace. Může za to i fakt, že kamerový systém zachycuje pouze místa, kterými je možné do budovy vstoupit z perimetru standardní cestou. Každý další pohyb osob v rámci budovy není monitorován, jediný prvek, který může odhalit nebo minimálně znepříjemnit pohyb takové osoby po objektu je všímavý zaměstnanec.

Jedny z nejdůležitějších místností v objektu jsou místnosti technologické. Je jich celkem sedm, z toho šest slouží primárně jako patchovací zóny mezi přístupovými prvky sítě a datovými zásuvkami uživatelů. Největší technologická místnost navíc plní funkcionalitu centrálního datového centra. Všechny místnosti jsou vybaveny pasivní protipožární ochranou a jsou plně klimatizované. Zabezpečeny jsou pouze mechanickými zámky s kvalitními vložkami, tři z nich jsou v zónách, kam je nezbytné získat autorizovaný přístup vyšší úrovně. Napájení technologických místností při výpadku elektrické energie zajišťuje centrální UPS, která poskytuje dostatečnou dobu pro nastartování dieselového generátoru, jehož doba chodu je omezena pouze množstvím připraveného paliva nebo jeho neočekávanou poruchou, která může za určitých okolností nastat. Jeho stav se v nepravidelných intervalech kontroluje a to včetně přepojení dodávky energie. Všechny prvky, které se starají o bezproblémový chod důležitých technologických prvků, jsou pomocí mobilních technologií schopné informovat předem určené osoby v případě, že došlo k neočekávané události (výpadek napájení budovy, výpadek klimatizace), obdobnou informaci odešlou i při navrácení stavu do stavu obvyklého.

[11] Autor práce úmyslně nezmiňuje způsob, jakým je možné získat přístup, aby nebyla ohrožena bezpečnost budovy. Možnost tohoto přístupu zná pouze díky pracovní náplni svého zaměstnání.

Nejen v technologických místnostech, ale prakticky ve všech kancelářích je možné spatřit výpočetní techniku, která je propojena pomocí datové sítě, datové zásuvky se nacházejí v chodbách, ale i v perimetru objektu (například vstupní vestibul) a jsou volně přístupné. Jejich ochrana tedy patří také do vnitřní bezpečnosti objektu. Tato ochrana je úzce spojena s ochranou síťové infrastruktury, bude jí tedy věnována samostatná kapitola.

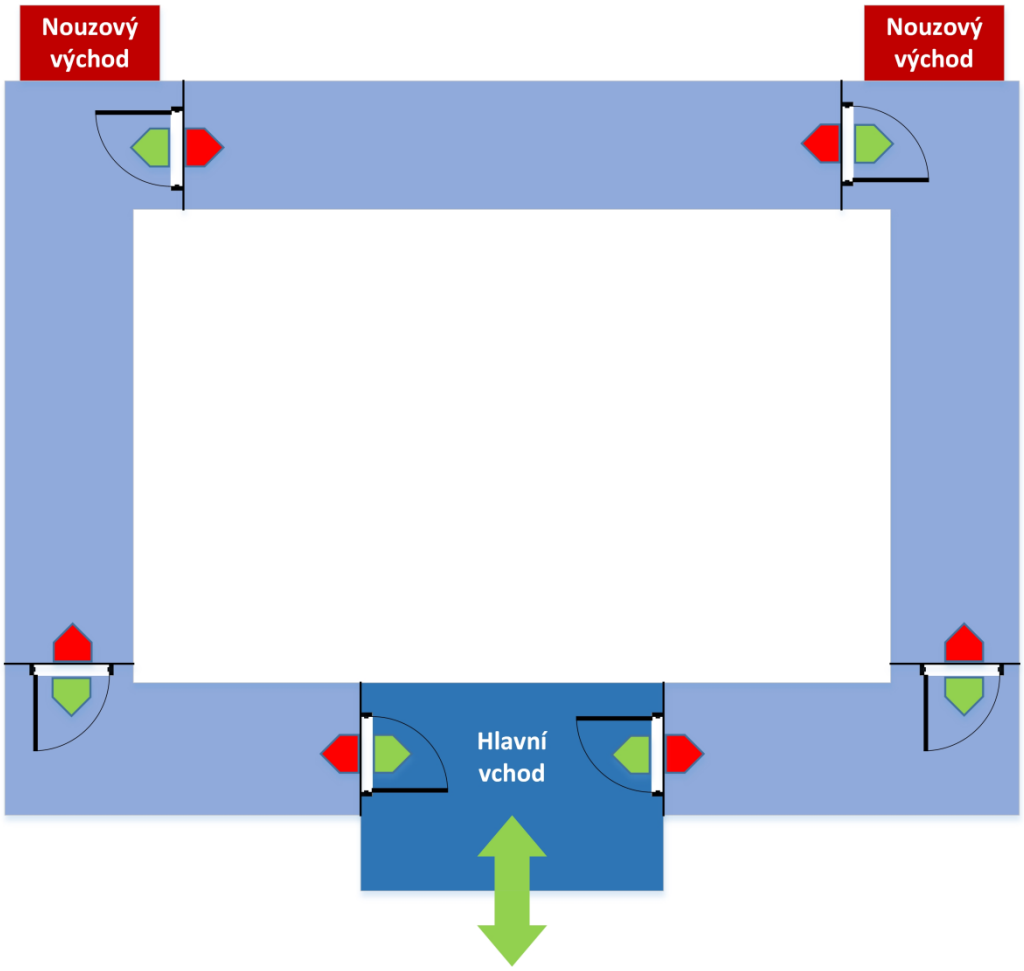
### 5.2.6 Opatření pro zlepšení vnitřní bezpečnosti objektu

Autor práce by se více zaměřil na rozčlenění budovy tak, aby nebylo možné postupovat směrem do nitra budovy bez patřičné autorizace. Z praktického hlediska by se jednalo o přepažení chodeb v místech, kde dochází k jejich větvení. Jednoduchou zábranu by tvořily sádrokartonové příčky s dveřmi, ovládanými systémem EKV. V návaznosti na bezpečnost osob při požáru nebo jiném stavu, který vyžaduje rychlou evakuaci, by bylo nezbytné dodržet pravidlo, že směrem k nouzovým východům je možné dveře otevírat klikou, aby se evakuované osoby neocitly v slepé pasti. Jelikož je budova vícepodlažní, bylo by nutné aplikovat podobné pravidlo ve všech podlažích, aby nebylo možné najít žádnou cestu, která by umožňovala projití téměř celého objektu bez nutnosti autentizace, tak jako je tomu doposud. Pro řešení tohoto problému by bylo možné použít techniku procházení grafu – vrcholy by představovaly jednotlivé, oddělené části chodeb, hrany by byly jednosměrné, ve směru zelených šipek, tedy volné cesty dveřmi, tak jak je znázorněno v příkladu na obrázku č. 6, který zjednodušeně vyobrazuje první nadzemní podlaží.

V technologických místnostech by autor doporučil osadit kamery, které by prováděly monitorování a v lepším případě i záznam vstupních prostor, aby bylo možné po určitou dobu zpětně dohledat potřebné obrazové informace. Společně s použitím systému EKV by tak celek poskytoval přesný přehled o tom, kdo a kdy do technologické místnosti vstoupil, jak dlouho se v ní zdržoval a v případě dostatku kamer i základní informaci o jeho činnosti uvnitř.

Aby byla celá technologie lépe chráněna proti náhlému výpadku elektrické energie, doporučuje autor zpracovat podrobnou dokumentaci, která by obsahovala údaje o umístění všech technologických místností. Z dokumentace by také mělo být jasné, kde se nacházejí hlavní vypínače napájení technologických místností, aby v případě požáru mohlo být napájení bezodkladně odpojeno a nebyly tak ohroženy životy zasahujících pracovníků. Vhodné by bylo provádět několikrát ročně testy všech agregátů, které se starají o dodávku

náhradní energie a to přesným časovým harmonogramem a nikoliv pouze náhodně. Poslední doporučené opatření v souvislosti s dodávkou náhradní elektrické energie je vybudování přípojného místa pro mobilní elektrocentrálu na vnějším plášti budovy, aby bylo možné v případě havárie hlavního generátoru, použít generátor záložní. Toto opatření se začalo během psaní této práce realizovat na doporučení autora. Přesto je dobré jej zmínit, protože jeho přípravou je možné riziko spojené s výpadkem elektrické energie minimalizovat.




**Obrázek 6 - možnost změny prostupů budovou. Zeleně je vyznačena volná cesta, červený směr vyžaduje autentizaci. (zdroj: autor)**

V souvislosti s technologickými místnostmi vidí autor, díky své pracovní náplni, ještě jeden závažný problém. Týká se volně přístupných datových zásuvek na chodbách. Tyto mohou být zneužity k připojení cizího zařízení do vnitřní sítě organizace. Jejich zneužití je možné minimalizovat více způsoby. První způsob by znamenal změnu v organizačních opatřeních způsobem, že by nemohl nastat případ volného pohybu

jakékoliv neautorizované osoby po objektu. Tento stav by znamenal, že každá osoba, která není autorizována pro vstup pomocí systému EKV, musí být nutně za každé situace doprovázena zaměstnancem organizace. Toto opatření by bylo vynuceno výše uvedeným doporučením o přepažení všech chodeb. Druhý způsob ochrany je nasazení technických opatření, které zasahují do první vrstvy ISO/OSI modelu sítě a bude mu věnována samostatná kapitola.

## 5.3 Analýza bezpečnosti fyzické vrstvy síťové infrastruktury

Pojem síťová bezpečnost není stav, ale neustálý proces, kterým se snažíme dosáhnout a posléze i udržet uspokojivé zabezpečení sítě. *(Cole, 2009)* Tento proces by se dal přirovnat k Demingově cyklu, který byl vysvětlen v kapitole o frameworku COBIT. Jelikož se síťové technologie rychle vyvíjí, dochází k zlepšování znalostí potenciálních útočníků, kteří používají více sofistikované nástroje i techniky. Nejen z tohoto důvodu je nezbytné neustále vylepšovat zabezpečení síťové infrastruktury. Hrozbou pro síťovou infrastrukturu může být i neznalý uživatel, který „jenom zapojí kabel do síťové zdířky“. Při nedokonalém nastavení všech prvků sítě tím může způsobit její kolaps. Jelikož informace o ochraně sítě na vyšších vrstvách jsou publikovány ve většině odborných časopisů a v dostatečném množství, bude se autor v následujících kapitolách věnovat především problematice ochrany sítě na fyzické vrstvě ISO/OSI modelu. Ochrana fyzické vrstvy sítě úzce souvisí s fyzickou bezpečností, která je v Zákoně o kybernetické bezpečnosti vyžadována. Kapitola samotná bude rozdělena do několika částí. V první části dojde k představení fyzické vrstvy ISO/OSI modelu, v následující části bude analyzováno síťové prostředí zkoumaného objektu ve vztahu k bezpečnosti a fyzické vrstvě, v dalších kapitole autor představí řešení a reálnou implementaci s ukázkami. Nakonec autor zhodnotí celé řešení, budou prezentovány jeho silné stránky, ale i problémy, které při implementaci vznikly.

### 5.3.1 Fyzická vrstva v ISO/OSI modelu

Fyzická vrstva ISO/OSI modelu je jeho první - nejnižší vrstvou. Tato vrstva představuje přenosové prostředí pro signály, u kterého definuje všechny jeho elektrické a fyzikální vlastnosti. Definice fyzické vrstvy obsahuje informace o vlastnostech použitých kabelů, použitých napěťových úrovních, ale stanovuje i způsob přenosu informací v podobě bitových hodnot. *(Ciampa, 2012)* Všechny tyto informace lze shrnout názvem

protokolu, který se na fyzické vrstvě užívá, v analyzovaném případě půjde o 1000BASE-T, tedy gigabitový ethernet, vedený po metalických kabelech.

### 5.3.2 Analýza síťové bezpečnosti

V kapitolách 5.1 a 5.2 byl představen analyzovaný objekt z hlediska fyzické bezpečnosti. Autor zde opatrně naznačil strukturu objektu, zamyslel se nad slabými stránkami, které ze svého pohledu shledal jako možné bezpečnostní riziko. Tato kapitola se bude věnovat technickým zařízením a prvkům sítě, které jsou sice umístěné uvnitř budovy, ale jejich zneužití představuje určité riziko. Výhodou analyzované infrastruktury je její izolace od okolního světa. Z veřejných sítí není možné jakékoliv připojení dovnitř, stejně tak je tomu opačným směrem. Tím je minimalizováno riziko napadení celého systému z veřejně dostupných sítí, mezi které se řadí například celosvětová síť internet. Důležité segmenty sítě jsou odděleny na druhé vrstvě OSI/ISO modelu pomocí virtuálních podsítí (tzv. VLAN) a provoz, který mezi nimi probíhá je umožněn pouze v omezené míře, pomocí firewallu. O správu třetí vrstvy sítě se stará zasmluvněný externí subjekt, který administruje síť ve všech pobočkách naší organizace. Smluvně je vše zastřešeno nadřazenou organizací, jejíž systémy spadají do skupiny subjektů VIS a část její infrastruktury splňuje podmínky pro zařazení do KII. Jedinou možností, jak lépe zabezpečit infrastrukturu našeho objektu je tedy důraz na bezpečnost sítě už v první její vrstvě – tedy minimalizovat riziko připojení cizích zařízení, která by mohla být zneužita, do vnitřní sítě. Pro pořádek je nezbytné blíže prezentovat síťové prostředí, které má být ochráněno.

V kapitole o fyzické bezpečnosti bylo poznamenáno, že v objektu se nachází celkem sedm technologických místností, které jsou umístěné v různých částech objektu. Technologické místnosti jsou pospojovány systémem „do hvězdy“ pomocí optických vláken tak, aby při výpadku jednoho spoje nebyl narušen provoz v jiných částech objektu. V každé technologické místnosti je osazen určitý počet přístupových switchů v dostatečném počtu, aby mohl být do vnitřní sítě připojen každý z více než 400 zaměstnanců, kteří v tomto objektu pracují. Switchů je celkem 30, z toho je 25 switchů přístupových, tedy těch, které jsou určené pro přímé připojení koncových stanic uživatelů. Jedná se o modely Cisco Catalyst WS-C2960S-48FPS-L, se softwarem C2960S-UNIVERSALK9-M ve verzi 150-2.SE6. Všechny přístupové switche jsou vybaveny

48 ethernet porty, což při plném osazení umožňuje obsloužit až 1200 samostatně připojených koncových zařízení. K jejich připojení do infrastruktury je využito metalické kabeláže kategorie 6, která zaručuje kompatibilitu se standardem 1000BASE-T při maximální délce 100 metrů, kdy je 90 metrů uvažováno jako délka vodorovné kabeláže, která spojuje účastnickou zásuvku s aktivním prvkem, zbylých 10 metrů je uvažováno jako délka připojovacího kabelu od datové zásuvky k samotnému zařízení. Datových zásuvek se v celém objektu vyskytuje bezmála 3000, počet zásuvek v jedné místnosti se pohybuje mezi 4 a 16 kusy, dle velikosti místnosti. Udržet pořádek v takovém počtu přípojných míst je velice obtížný, v objektu navíc dochází k poměrně častému stěhování osob. Nezřídka se tak stává, že datová zásuvka, která není využívána, je stále zapojena do datové sítě a tím může poskytovat přístup do určité virtuální sítě osobám, které nejsou pro takový přístup autorizovány. Řešením by mohla být restrikce přístupu na porty aktivních prvků dle MAC adresy, avšak toto řešení je nevhodné vzhledem k možnosti MAC adresu na zařízení změnit a celou kontrolu tak obejít. *(Bloch, 2011)* Nasazení protokolu 802.1X[12], který umožňuje zabezpečení přístupu do počítačové sítě, problém neřeší, jelikož existují zařízení, která tento protokol nepodporují. U těchto zařízení se autentizace protokolem 802.1X vypíná a spoléhá se pouze na kontrolu MAC adres. *(Kizza, 2014)* Jelikož je správa síťové vrstvy infrastruktury svěřena externí organizaci, která se snaží o jednotný přístup a nastavení sítě i u ostatních poboček stejného typu, je nesnadné domoci se jakýchkoliv změn v nastavení sítě. Zbývá tedy poslední možnost – správa sítě na její fyzické vrstvě, která umí plnit úlohu aktivní ochrany bez většího zásahu do konfigurace logického rozdělení sítě.

Zbývá tedy najít vhodné řešení, které by splňovalo naše požadavky:

- nezávislost managementu na vyšších vrstvách sítě
- grafické rozhraní, s jednoduchým ovládáním
- rozhraní v českém jazyce
- víceuživatelské prostředí s možností nastavení rolí jednotlivým uživatelům
- průchodnost PoE v případě prvků vložených mezi aktivní prvky a koncová zařízení
- zobrazení stavu sítě v reálném čase

[12] Podrobněji je princip ověřování vysvětlen například na internetové stránce http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html

- možnost hlášení předem zvolených událostí emailem

Existuje několik řešení, která jsou vhodná pro správu fyzické vrstvy sítě. Mezi nalezené systémy je možné zařadit například Quareo od Tyco Connectivity Ltd., MapiT od Siemon Interconnect Solutions, MIIM™ od Molex Incorporated; PanView IQ by Panduit Corp. nebo CommScope SYSTIMAX iPatch Systém. Jako řešení byl vybrán produkt MIIM™ od společnosti Molex. Jedná se o certifikované řešení, které splňuje bezpečnostní nároky kladené naší organizací, mezi výhody lze zařadit téměř kompletní počeštění celého systému. Praktická ukázka byla před samotným rozhodnutím o nákupu předvedena pomocí „demokufříku“, na kterém bylo možné odzkoušet všechny situace, které mohou během provozu nastat. Další faktor, který ovlivnil výběr, bylo zastoupení společnosti Molex v České Republice, dostatečný počet certifikovaných instalačních partnerů a stávající infrastruktura, která je kompatibilní s řešením Molex MIIM™ ve vztahu k HW úpravám koncových zásuvek. Molex MIIM™ je certifikovaný nástroj normy ISO 27001 *(NetWork Group, 2014)*.

## 5.4 Molex MIIM™

Systém MIIM™ je ucelené řešení pro správu a monitoring fyzické vrstvy sítě od společnosti Molex Premise Networks. Jedná se o součást APLMM[13] systému, který umožňuje kompletní, vylepšenou správu fyzické vrstvy. Řešení MIIM umožňuje správu přesunů, rozšíření a změn sítě včetně správy pracovních příkazů. Systém navíc nepřetržitě monitoruje a mapuje fyzickou vrstvu, včetně neporušenosti horizontální strukturované kabeláže od telekomunikační místnosti až po připojené koncové zařízení. Systém je schopen detekovat připojení/odpojení síťových zařízení, porovnává reálně nasazené prvky sítě s jejich návrhem, takže jej lze považovat za jedno z možných technických opatření Zákona o kybernetické bezpečnosti (§16, §17). Systém navíc umožňuje technikům realizaci pracovních příkazů pomocí řízeného propojování.

Shrnutí nejdůležitějších charakteristik:

- Nepřetržitě monitoruje fyzickou vrstvu včetně kabelů, přepínačů a síťových zařízení

[13] Advanced Physical Layer Lifecycle Management – rozšířený management životního cyklu fyzické vrstvy

- Dokáže detekovat přerušení horizontálního kabelu a přerušená spojení mezi propojovacím kabelem a uživatelskými počítači
- Porovnává reálně nasazené prvky sítě s jejich návrhem a upozorňuje na veškeré odchylky
- Nepřetržitě monitoruje přítomnost zařízení připojených do datové a to i v případě, kdy je zařízení vypnuté. Lze nakonfigurovat výstrahy upozorňující personál na neoprávněné odpojení zařízení nebo na neoprávněné pokusy o připojení k síti.
- Usnadňuje správu plánování a zaznamenávání přesunů, rozšíření a změn sítě a včetně ověřování správného provádění pracovních příkazů.
- Umožňuje řízené propojování, kdy jsou na propojovacích panelech umístěny diody LED, které indikují porty s nevyřízenými pracovními příkazy

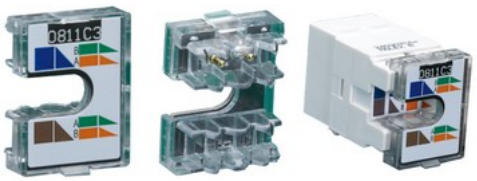
### 5.4.1 Princip managementu na fyzické vrstvě Molex MIIM™

Systém Molex MIIM™ je unikátní tím, že pro svou funkčnost nevyžaduje speciální kabeláž. Využívá standardní horizontální kabeláže, tedy kabely twisted-pair, které se používají pro metalické síťové propoje. V případě kvalitní stávající kabeláže není, při nasazování systému Molex MIIM™, nutná její kompletní výměna. Strukturovaná kabeláž v naší organizaci prošla kompletní obměnou v roce 2012, veškerá horizontální kabeláž byla nahrazena kabely kategorie 6. Spolu s horizontální kabeláží došlo k výměně téměř všech účastnických zásuvek. Původní zásuvky byly nahrazeny zásuvkami Molex, ponecháno bylo pouze několik zásuvek ABB Tango. Všechny tyto zásuvky jsou kompatibilní se systémem Molex MIIM™, nezbytné je tedy pouze osadit terminační člen, který napomáhá celému systému kontrolovat celistvost horizontální kabeláže. Celý systém je mnohem složitější, vedle pasivních prvků využívá i prvky aktivní, včetně řídícího serveru, který veškeré informace zaznamenává do SQL databáze. Pro pochopení celé hierarchie je vhodné jednotlivé prvky představit a vysvětlit jejich úlohu v celém systému.

#### Terminátor koncové zásuvky

O terminačním členu koncové zásuvky byla zmínka již v předchozím odstavci kapitoly 5.4.1. Jeho úlohou je uzavírat impedanční smyčku na horizontální kabeláži. Terminátor se instaluje do účastnické zásuvky, možnost jeho instalace je podmíněna osazením tzv. keystone (modulová zdířka pro konektor RJ45) značky Molex. Instalace

spočívá v pouhém nasazení na keystone bez nutnosti opětovného ranžírování[14] jednotlivých vodičů horizontální kabeláže. Samotná instalace zabere pouze několik sekund, stejně rychle je možné provést demontáž. Dle technické specifikace zaručuje společnost Molex funkčnost po dobu minimálně 20 instalačních cyklů.



**Obrázek 7 - Vzhled a instalace terminátoru koncové zásuvky (zdroj: autor)**

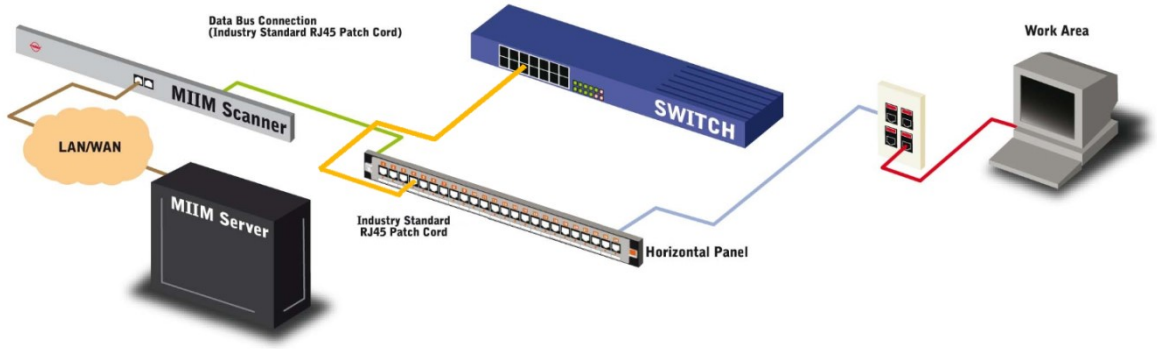
## Patch-panel

Dalším prvkem managementu fyzické vrstvy Molex MIIM™ je speciální patch-panel, do kterého je naranžírován druhý konec horizontálního kabelu. V tuto chvíli autor považuje za nezbytné vysvětlit rozdíl v režimech, ve kterých je možné celý systém provozovat, jelikož volba režimu ovlivňuje i výběr panelu, jehož funkci chce autor vysvětlit.

Celý systém může pracovat ve dvou režimech, volba režimu je závislá na velikosti investice, kterou je zákazník ochoten vynaložit a probíhá již ve fázi plánování. Levnější varianta je varianta s jednoduchou reprezentací – označována jako „InterConnect“. Tato varianta je vhodná pro cenově kritické instalace. Její výhodou je nižší pořizovací cena, instalace klade menší nároky na prostor v jednotlivých rozvaděčích. Mezi nevýhody patří omezené možnosti plánování patchovacích prací nebo omezená identifikace koncových zařízení. Zapojení systému InterConnect je znázorněno na obrázku č. 8.

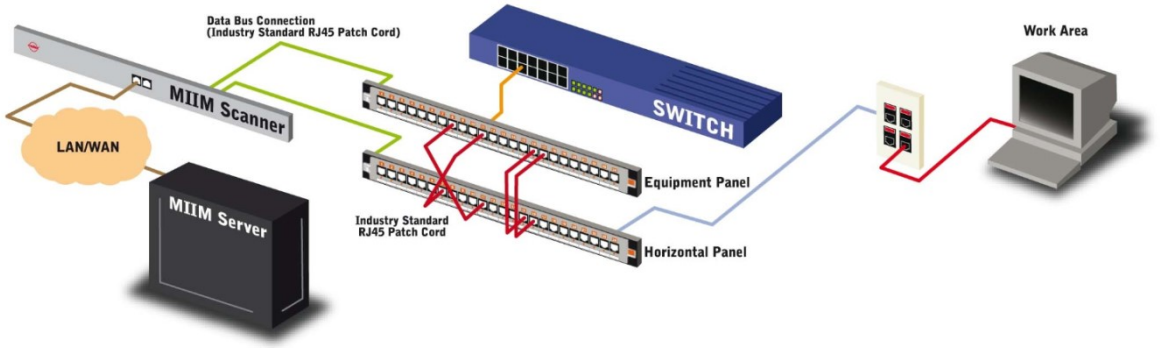
Tato levnější varianta umožňuje monitorovat celistvost kabeláže mezi koncovým zařízením a patch-panelem v rozvaděči. Není možné monitorovat celistvost propojení mezi aktivním prvkem (switchem) a patch-panelem. Indikace vybrané zásuvky na patch panelu je možná, nikoliv však indikace portu aktivního prvku.

[14] Ranžírování nebo také tzv. narážení kabelů je technika spojování kabelů strukturované kabeláže s rozvodnými panely nebo koncovými zásuvkami.




**Obrázek 8 - režim InterConnect (zdroj: Radek Helán, 2010)**

Řešení, které poskytuje monitoring celé cesty je označováno jako „CrossConnect“. Jeho zapojení je znázorněno na obrázku č. 9. Od zapojení InterConnect se liší jedním přidaným patch-panelem, navíc jsou tyto panely odlišné od panelu, který je použitý v InterConnect řešení. Mezi výhody patří výše zmíněný monitoring celé cesty od aktivního prvku, až po koncové zařízení, v případě plánování prací v patch zóně dokáže systém indikovat na obou panelech konkrétní zásuvky, které se mají propojit nebo naopak bylo naplánováno jejich rozpojení. V naší organizaci byla, po zvážení všech výhod a nevýhod jednotlivých řešení, zvolena varianta CrossConnect. Z tohoto důvodu bude v další části práce princip vysvětlován na této variantě.




**Obrázek 9 - režim CrossConnect (zdroj: Radek Helán, 2010)**

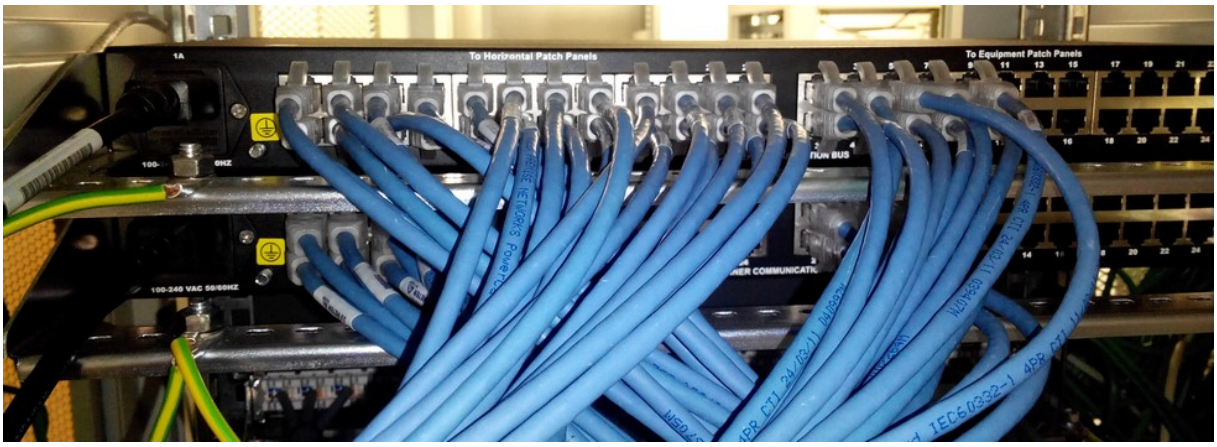
Panely varianty Cross Connect se dělí na dva typy. Panel, do kterého je zakončena horizontální kabeláž od účastnické zásuvky se označuje „PP“. Jedná se o zkratku slovního

spojení „Passive Panel“, na obrázku 9 je vyobrazen jako spodní panel s popiskem „Horizontal Panel“. Panel, do kterého jsou vyvedeny krátké propojovací kabely z aktivního prvku, se označuje „CC“, podle slovního spojení „Cross Connect“ – na obrázku se jedná o horní panel s popiskem „Equipment Panel“. Fyzicky jsou oba panely totožné. Aby je systém dokázal odlišit, je nezbytné jejich správné nastavení v dalším prvku, který se nazývá MIIM Scanner. Každý panel poskytuje 24 ethernetových zásuvek standardu RJ45, které jsou chráněny prachovou clonkou. V případě, že jsou použity 48-portové aktivní prvky, připadají na každý aktivní prvek 2 CC panely, do jednoho PP panelu je možné připojit 24 koncových zásuvek. Dohromady bylo v naší organizaci instalováno 52 CC a 120 PP panelů, které monitorují více než 2850 koncových zásuvek a 1248 zásuvek aktivních síťových prvků.

### MIIM scanner

Jedním z nejdůležitějších prvků celého systému Molex MIIM™ je MIIM scanner. Scanner se stará o obsluhu všech panelů, které jsou do něj připojeny pomocí proprietární vnitřní sběrnice. Do jednoho scanneru je možné zapojit 24 CC a 24 PP panelů, což při plném obsažení znamená 576 datových koncových zásuvek a 576 portů aktivních prvků. V naší instalaci jsme ve dvou technologických místnostech narazili na technologický strop těchto prvků, protože bylo nezbytné obsloužit cca 1000 koncových zásuvek. Řešením bylo osazení dvou MIIM scannerů do jednoho rozvaděče, jak je znázorněno na obrázku 10 a 11.


**Obrázek 10 - dva MIIM scannery obsluhující jednu technologickou místnost – status LED (zdroj: autor)**




**Obrázek 11 - dva MIIM scannery obsluhující jednu technologickou místnost - připojení panelů (zdroj: autor)**

Tato situace bohužel pro obsluhu znamená nepříjemnou komplikaci, jelikož – jak bude zmíněno v další kapitole – je možná plánovat propojení CC a PP panelů pouze v rámci zapojení jednoho scanneru. Zajímavostí, která je na obrázku 10 patrná, je, že CC panelů (Equipment patch Panels) je zapojeno výrazně méně, než panelů PP. Tato situace je dána poměrem počtu všech datových zásuvek k počtu portů aktivních prvků. Konkrétní čísla, která odpovídají vyobrazenému zapojení, jsou: 903 zapojených koncových zásuvek, z toho 576 v horním scanneru. Ve stejném scanneru je zapojeno pět přístupových switchů řady Cisco Catalyst 2960S s 48 porty, tedy celkem 240 portů. Druhý scanner obsluhuje tři aktivní síťové prvky a cca 320 koncových zásuvek. Nastala tedy situace, při které bylo nezbytné správně rozhodnout o přidělení jednotlivých síťových segmentů k jednotlivým scannerům. Tuto situaci považuje autor za jednu z hlavních slabin celého systému, jelikož je systémově nemožné propojit oba scannery tak, aby se chovaly jako jeden celistvý celek. Dle zástupců společnosti Molex je v přípravě novější verze MIIM scanneru výšky 2U, který by dokázal obsloužit a monitorovat více než 1100 koncových zásuvek.

MIIM scanner není jen hloupé zařízení, které měří impedanci horizontálních i cross-connect vodičů, ale musí zároveň uchovávat celou tabulku informací o tom, jaký je aktuální stav propojů v patch zóně. Tuto tabulku následně synchronizuje s centrálním serverem. Scanner je možné nastavovat z uživatelského rozhraní systému, mezi hlavní parametry patří dva časové údaje – doba částečného a plného skenování cross-connect propojů patch zóny.

Quick-scan je, jak napovídá název, rychlejší varianta skenování, která pouze provádí kontrolu, zda nedošlo k odpojení naplánovaných propojů v patchovací zóně. Aby bylo skenování jednodušší, využívá každý scanner své vnitřní tabulky propojů, takže není nezbytné kontrolovat všechny možné kombinace, které mohou nastat. Jako příklad je možné uvést situaci, kdy máme v celé patchovací zóně naplánováno pouze pět propojů, tedy pět účastnických zásuvek propojených na pět portů aktivního prvku. Scanner provede měření impedance pouze v rámci těchto pěti propojů mezi CC a PP panely. Pokud zjistí nesrovnalost, v tomto případě by se jednalo například o odpojení cross-connect propoje, předá informaci řídícímu serveru, který dle svého nastavení provede předem nastavenou činnost (odeslání emailu, apod.). Vždy je zároveň nesrovnalost indikována v přehledovém zobrazení rackových skříní, konkrétně červenou (propoj naplánován v systému, ale neodpovídá jeho fyzické propojení) nebo žlutou (propoj fyzicky existuje, ale nebyl naplánován v systému) barvou. Standardní barva pro stav, kdy naplánovaný propoj odpovídá fyzickému stavu, je zelená. Rychlost skenování je dána počtem zapojených cross-connect kabelů. Čím více je jich v databázi scanneru uloženo, tím je skenování pomalejší, neboť je nebytné prověřit každý jednotlivý naplánovaný propoj.

Jiná je situace u tzv. full-scanu. Tento proces trvá podstatně déle než quick-scan, protože má za úkol zjistit, zda nedošlo k zapojení nového cross-connect propoje. Jelikož scanner jednoduše nepozná, zda došlo k propojení nějakých dvou zásuvek, musí zkontrolovat všechny kombinace zásuvek každého CC panelu se všemi zásuvkami každého PP panelu. Tento proces je poměrně časově náročný, zkontrolovat 576 účastnických zásuvek proti 240 portům aktivních prvků zabere scanneru cca 30 minut. Z tohoto důvodu je full-scan prováděn v delších časových intervalech a i celému systému trvá déle odhalit rozdíl oproti naplánovanému stavu. Dle zastoupení společnosti Molex probíhají v současné době dokončovací práce na nové revizi panelů, které jsou odlišné od stávající verze. Tyto nové panely by měly eliminovat potřebu provádění full-scanu, protože každá jednotlivá zásuvka panelu bude vybavena mikrospínačem. Při každém zasunutí cross-connect kabelu dojde k sepnutí tohoto mikrospínače, který předá systému informaci o zásuvce, se kterou bylo manipulováno. Tím byl představen princip, kterým dokáže systém Molex MIIM™ detekovat takové změny ve fyzickém zapojení sítě, které nebyly naplánovány obsluhou. V další kapitole bude vysvětlen správný postup plánování prací včetně ukázek stavů, které se zobrazují obsluze.

#### MIIM server

MIIM server je centrální součást celého systému, která sbírá veškeré informace ze všech aktivních prvků (MIIM scannerů), vyhodnocuje stavy a upozorňuje přes webové rozhraní na případné nesrovnalosti na jednotlivých zásuvkách, panelech, připojených koncových zařízeních nebo cross-connect propojích. V pravidelných intervalech komunikuje s jednotlivými MIIM scannery, zadává příkazy k provedení full-scanu nebo k zapnutí indikace na určeném portu nebo portech. Zároveň porovnává svou databázi, která využívá řešení SQL server společnosti Microsoft, s databází jednotlivých scannerů, aby bylo možné obsluhu upozornit na nesrovnalosti, které mohly vzniknout omylem, vadnou kabeláží nebo třeba úmyslným odpojením zařízení. Pro zobrazení informací o stavu fyzické vrstvy sítě je využíváno webové rozhraní, které využívá framework Microsoft Silverlight. Autor práce by si dovedl představit použití jiného – modernějšího a rychlejšího standardu (například HTML5), který by poskytoval rychlejší odezvy a menší hardwarové nároky při zachování vizuální stránky aplikace. Zároveň by odpadl problém s neoficiálními implementacemi Silverlightu pod operačními systémy rodiny Unix, kde je nutné používat náhradu v podobě Mono nebo Pipelight.

### 5.4.2 Obsluha

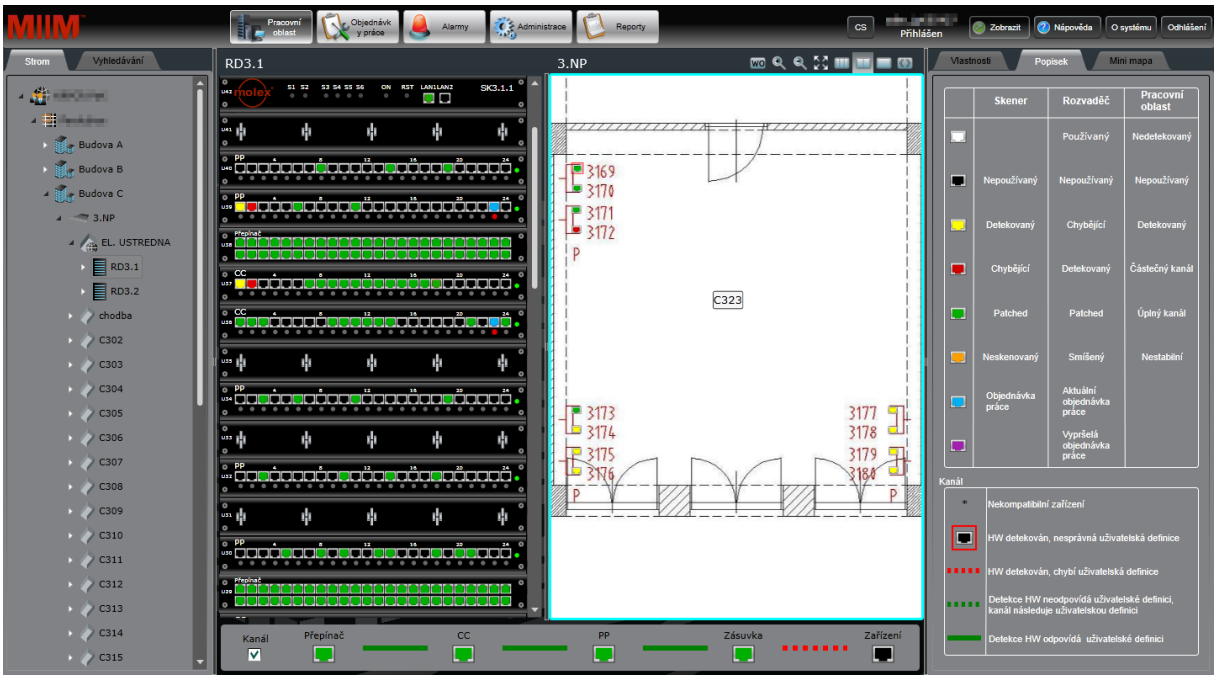
V předchozí kapitole autor vysvětlil základní princip funkčnosti systému Molex MIIM™. Systém by však bez řádně proškolené obsluhy nebyl schopen podávat relevantní informace o aktuálním stavu fyzické vrstvy sítě nebo plánovaných změnách.

#### Oprávnění uživatelů

Jelikož je systém určen spíše pro organizace s větší síťovou infrastrukturou, je nezbytné, aby poskytoval a zaznamenával veškeré informace o zadavateli změn v síti, dále také informaci, komu byla práce přidělena a kdy byla nebo nebyla vykonána. První obrazovka po načtení webové stránky s managementem, kterou uživatel spatří na obrazovce, je přihlašovací okno. Po úspěšné autentizaci uživatele jsou mu přidělena práva dle nastavení skupiny, do které je uživatel přidělen a dle těchto práv je autorizován k určitému druhu činnosti. Využít lze lokální databázi uživatelů nebo doménové účty. Ke každému uživateli je možné přidělit události, o kterých obdrží informace prostřednictvím emailu. Technikům, kteří mají za úkol aplikovat požadované změny, jsou doručovány objednávky práce, pracovníkovi hlídajícímu bezpečnost je možné přidělit zasílání informací o jakýchkoliv změnách.

## Přehled sítě

Částí systému, kde se administrátoři a zadavatelé změn sítě nejvíce pohybují, je přehled fyzického zapojení sítě. Celý objekt je rozdělen do bloků, dále do jednotlivých podlaží a místností v nich. Každá část objektu má přidělenu technologickou místnost, kde se sbíhají všechny horizontální kabely z této části. Číslování datových zásuvek je koncipováno tak, aby bylo na první pohled patrné, ve které technologické místnosti bude zásuvka zapojena do aktivního prvku, čímž je usnadněna i orientace v administraci systému. Všechny prostory, ve kterých se vyskytují koncové prvky, které jsou nezbytné pro správnou orientaci (koncové zásuvky, PP a CC panely), jsou zmapovány a tyto mapové podklady se přímo zobrazují v podobě podrobné mapy. Do této mapy byly vloženy všechny koncové zásuvky, takže ze statické mapy mapa aktivní, na které je zobrazen aktuální stav každé zásuvky. Pro lepší představu, jak může operátor vidět stav sítě, je na straně 76 umístěn obrázek č. 12. I zde platí pravidlo – čím větší monitor je připojený k operátorskému PC, tím více informací je možné na jedné obrazovce zobrazit. Na obrázku jsou záměrně zobrazené tři hlavní stavy, se kterými je možné se běžně setkat.




**Obrázek 12 - přehled fyzické vrstvy sítě (zdroj: autor)**

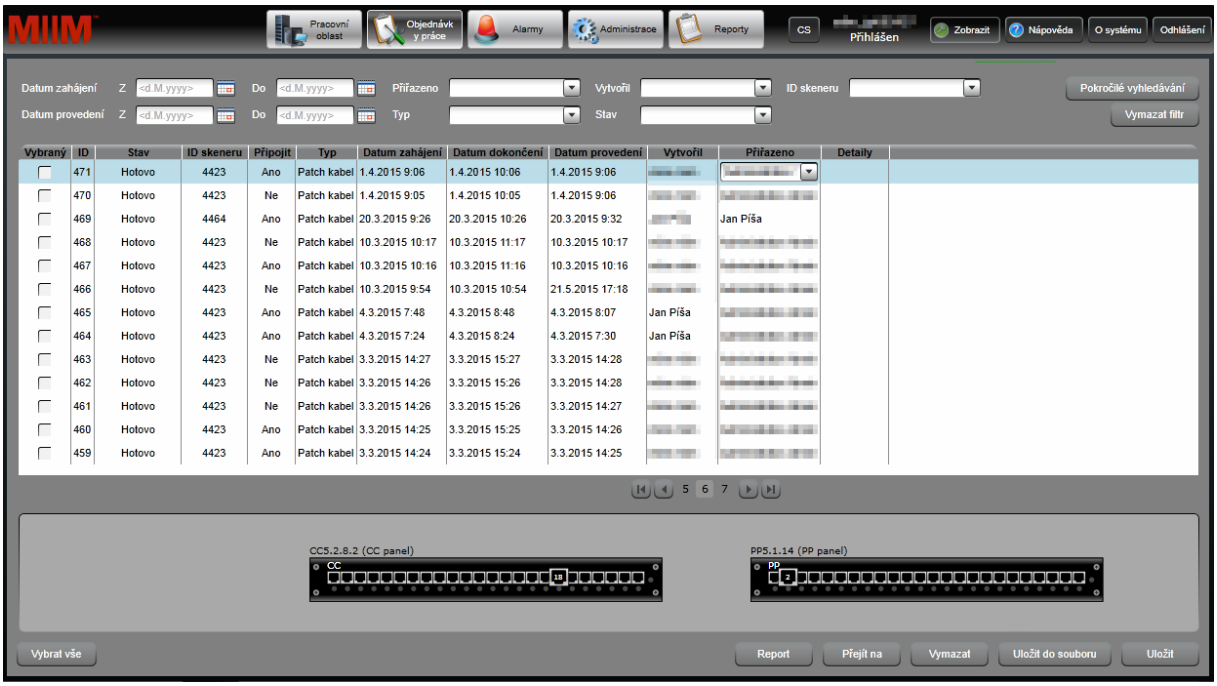
V zobrazení rackové skříně jsou barevně označeny stavy:

- žlutá dvojice zásuvek – mezi těmito zásuvkami není naplánován propoj, ale fyzicky je přítomný cross-connect patch

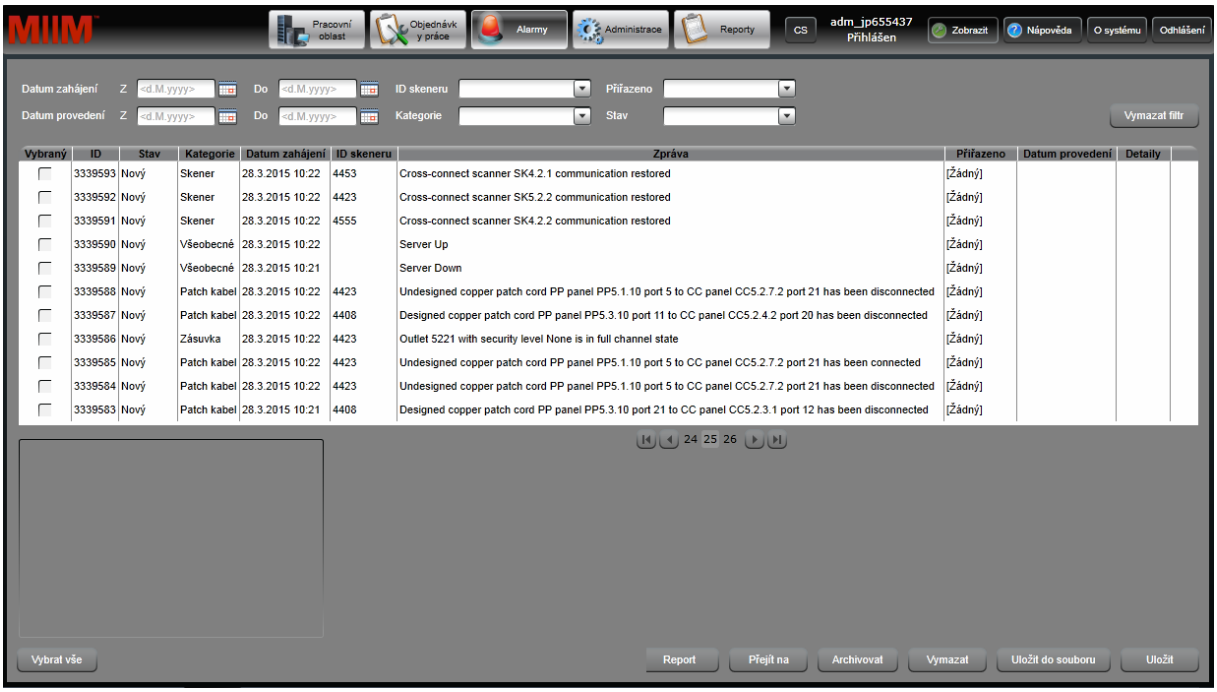
- červená dvojice zásuvek – mezi těmito zásuvkami je naplánován propoj, ale fyzické propojení cross-connect patchem není přítomné
- modrá dvojice zásuvek, doplněná červenou indikací – naplánovaná práce, tyto dvě zásuvky dostal technik za úkol propojit nebo rozpojit. Přímo v rozvaděči jsou označeny oba panely, na kterých se zásuvky nacházejí, rozsvícenou postranní červenou LED. Stejně jsou označeny i obě konkrétní zásuvky. Jejich nalezení je tak otázkou jednotek sekund. Po splnění úkolu diody zhasnou a v aplikaci dojde k přebarvení pozic na barvu zelenou nebo černou dle toho, jaký je aktuální stav těchto zásuvek. Pokud dojde ke srovnání stavu červeně nebo žlutě označených zásuvek s jejich stavem v databázi systému, dojde také ke změně barvy. Tento nestandardní stav je také možné potvrdit dvěma kliky myši přímo z tohoto přehledu. Tím je systému řečeno, že aktuální fyzický stav je správný, i když nesouhlasí s definicí. Ve spodní části obrazovky je možné zaškrtnout položku „Kanál“. Po aktivaci je zobrazena stav celého fyzického propojení od aktivního prvku, až po koncové zařízení. Zobrazuje se vždy cesta té zásuvky, která je vybrána v přehledu, nezáleží, zda byla vybrána zásuvka v přehledové mapě nebo v zobrazení rackové skříně. Na obrázku 12 je zobrazen stav, kdy je celá cesta propojena, koncové zařízení je v zásuvce zapojeno, ale chybí jeho uživatelská definice. Bez uživatelské definice nelze pohyb tohoto zařízení sledovat. V pravé části je možné zobrazit legendu, mini mapu nebo vlastnosti vybrané zásuvky (popis, pozice, ID v systému apod.).

### Alarmy

Alarmy jsou pro bezpečnostní pracovníky nejdůležitější sekcí v systému Molex MIIM™. Samotný seznam může býti poměrně rozsáhlý, logují se všechny nestandardní stavy, od nestabilní zásuvky, po výpadek samotného serveru. Na obrázku č. 14 je znázorněn detail části záznamu alarmů z reálného nasazení systému. V seznamu lze nalézt, že došlo k řízenému zastavení a opětovnému puštění serveru, po jeho spuštění se začaly postupně připojovat scannery, které obnovily se serverem komunikaci. Nejzajímavější záznamy vzhledem k bezpečnosti jsou patrné ve spodní polovině okna se záznamy. Z nich je patrné, že někdo manipuloval s cross-connect propoji, je zaznamenán čas, identifikace PP a CC panelu, včetně čísla konkrétního portu a situace, která nastala oproti normálu.




**Obrázek 13 - záznam úkolů a provedených prací (zdroj: autor)**




**Obrázek 14 - záznam alarmů (zdroj: autor)**

Vidíme, že nejprve (spodní záznam) došlo k rozpojení cross-connect propoje, který byl v systému nadefinován, poté byl fyzicky rozpojen a hned zase zapojen propoj, který v systému nadefinován není. Následuje informace, že byla obnovena plná komunikace se zásuvkou 5221. Z tohoto výpisu alarmů je možné generovat report.

### 5.4.3 Silné a slabé stránky systému Molex MIIM™

Nástroj Molex MIIM™ je poměrně mocný nástroj. Výčet všech detailů, které je možné nastavit nebo sledovat by mnohonásobně překračoval rámec této práce. Proto se autor zaměří na silné, ale i slabé stránky, které během implementace systému a krátkého používání zjistil a nakonec rozhodne, zda má cenu o případném nasazení nástroje Molex MIIM™ v současné době uvažovat, či nikoliv.

#### Silné stránky dle výrobce

Jelikož byl nástroj společnosti Molex v organizaci, ve které autor pracuje, nasazován během psaní této diplomové práce, bude autor vycházet z informací, kterými se chlubí PR oddělení výrobce systému – bude použit český překlad, který je dostupný na stránkách společnosti NetworkGroup s r.o.[15], která je oficiálním distributorem společnosti Molex Premise Networks pro Českou republiku. Tyto informace budou krátce okomentovány zkušenostmi, které autor získal v průběhu implementace a testování.

- ***Nepřetržitě monitoruje fyzickou vrstvu včetně kabelů, přepínačů a síťových zařízení.*** S tímto tvrzením se dá v podstatě souhlasit, otázkou zůstává „nepřetržitost“ ve smyslu nových propojení v patch zóně. V kapitole 5.4.1 autor vysvětluje princip skenování pomocí tzv. full-scanu, který probíhá v pravidelných intervalech. Doba tohoto skenování se pohybuje v řádech desítek minut – dle počtu sledovaných CC a PP zásuvek. Nové – nenaplánované propoje – se tedy v dohledu systému mohou objevit třeba až za 30 minut. Tato doba je dostatečná k připojení cizího zařízení a jeho opětovného odpojení. Navíc full-scan je indikován diodou jak na konkrétním scanneru, tak na jednotlivých panelech, na kterých právě skenování probíhá. Potenciální útočník, který má přístup přímo k MIIM scannerům, tak může získat během relativně krátkého sledování získat informace o tom, kdy bude probíhat další skenování sítě a cca jak dlouho bude trvat.

- ***Ověřuje neporušenost horizontálních kabelů až po datové zásuvky na pracovištích, detekuje přerušená spojení a poruchy izolace. Dokáže detekovat přerušení horizontálního kabelu a přerušená spojení mezi***

[15] http://www.networkgroup.cz/index.php?module=shop_catalog&action=list_products&id=132

***propojovacím kabelem a uživatelskými počítači.*** Na tomto tvrzení může osoby znalé fyzikálních zákonů zarazit tvrzení o ověření poruchy izolace. Po krátké analýze originálního znění[16] došel autor k závěru, že se jedná o špatný překlad. Vhodnější překlad by mohl znít například „Pomáhá určovat chyby způsobené přepojováním kabelů v technologické místnosti“. O tomto tvrzení nemohou být žádné spory – systém je opravdu schopný detekovat chybějící propoje a to jak v rámci patch zóny, tak mezi koncovou zásuvkou a zařízením. Bohužel se nám nepodařilo pomocí systému MIIM diagnostikovat takové horizontální kabely, které mají například přerušenou pouze jednu žílu a síťová komunikace tak nemůže být navázána. Tyto kabely musíme tedy stále diagnostikovat pomocí digitálních měřících přístrojů, které byly k tomuto účelu navrženy.

- ***Porovnává reálně nasazené prvky sítě s jejich návrhem a zvýrazňuje veškeré odchylky.*** V tomto ohledu nelze systému nic vytknout. Zařízení, které je v systému řádně nadefinováno, je hlídáno, aby nebylo zapojeno do jiné datové zásuvky. V případě změny nebo odpojení je v grafickém přehledu názorně zařízení zobrazeno tak, jak je uvedeno v grafické legendě přehledu. Zároveň dojde k aktivaci alarmu a celá nesrovnalost zapsána do logu.

- ***Nepřetržitě monitoruje přítomnost zařízení připojených do datové zásuvky na pracovišti, a to i v případě, kdy je zařízení vypnuté. Lze nakonfigurovat výstrahy upozorňující personál na neoprávněné odpojení zařízení nebo na neoprávněné pokusy o připojení k síti.*** Tento bod, který Molex uvádí, úzce souvisí s předchozím. Autor jej proto ponechá bez komentáře.

- ***Událostmi řízené dotazování připojených zařízení zajišťuje poskytování aktuálních informací ze všech zařízení připojených ke všem datovým zásuvkám.*** Celý systém dokáže komunikovat s připojenými zařízeními na vyšších vrstvách OSI-ISO modelu. Zatím se nám nepodařilo získat informace

[16] http://www.networkgroup.cz/my_files/katalog/metalicke_prvky_molex/MIIM-Flyer.pdf

o zařízeních, která jsou připojena za IP telefony, které jsou v naší organizaci využívány.

- ***Usnadňuje správu zakázek, včetně plánování a zaznamenávání přesunů, rozšíření a změn sítě a včetně ověřování správného provádění pracovních příkazů.*** Tato vlastnost, společně s monitorováním připojených zařízení rozhodla v našem případě o pořízení kompletního systému ve variantě „CrossConnect“. Prakticky denně tuto vlastnost využíváme. Bohužel až po implementaci jsme narazili na několik zásadních problémů, které se při předvádění celého systému nemohly projevit vzhledem k diametrálnímu rozdílu v počtu spravovaných datových zásuvek mezi reálnou instalací a předváděcím vzorkem. Podrobněji se autor vrátí k problémům v další části této kapitoly.

- ***Umožňuje řízené propojování, kdy jsou na propojovacích panelech umístěny diody LED, které indikují porty s nevyřízenými pracovními příkazy.*** Výborná funkcionalita, která usnadní vyhledání příslušných zásuvek, pro které byl vypracován plán zapojení nebo odpojení. Zároveň je možné ručně rozsvěcet každou zásuvku manuálně přímo z přehledu stavu sítě. Avšak ani zde není vše bezproblémové.

### Slabé stránky a problémy, které nastaly - z pohledu uživatele

- Microsoft Silverlight. Pomalý, náročný framework, který by mohl být nahrazen například pomocí HTML5 standardu. Občas se stává, že plugin v prohlížeči havaruje, někdy systém přestane reagovat a je nezbytné obnovit zobrazenou stránku. Bohužel po obnovení stránky systém zobrazí prvotní okno, takže je nezbytné opět se proklikat na obsah, který byl zobrazen před obnovením.

- Detekce poškozených horizontálních kabelů. Bohužel, zatím se nepodařilo zjistit, jak a zda vůbec je MIIM schopen detekovat částečně poškozený horizontální kabel. Autor provedl analýzu terminačního členu v datové zásuvce, aby zjistil, zda tento člen pomáhá systému při diagnostice.

V terminačním členu se nachází pouze jeden odpor mezi dvěma datovými žílami. Buď tedy Molex spoléhá na to, že dojde vždy k přerušení celého kabelu nebo autor práce nesprávně pochopil princip detekce poškozeného horizontálního vedení. Jelikož jsou však autorovi v současnosti známé zásuvky, jejichž přívodní horizontální kabel vykazuje přerušený vodič, aniž by systém něco zaznamenal, domnívá se autor práce, že musí dojít k přerušení celého kabelu.

- Pomalá reakce v průběhu full-scanu. Pokud probíhá na scanneru full-scan a v tuto dobu je na stejný scanner naplánován úkon zapojení nebo odpojení propoje, trvá celý proces neúměrně dlouho, pravděpodobně z důvodu velkého vytížení tohoto aktivního prvku.

- Signalizace zásuvek v patch zóně pomocí LED. I když je signalizace velice šikovně vymyšlena, nelze opomenout jednu situaci, která nastává, pokud je naplánováno rozpojení cross-connect propoje mezi CC a PP panely. Úkol je naplánován, obě LED svítí jasně červenou barvou. Jakmile je však vytažen propojovací kabel z jedné ze zásuvek, okamžitě zhasíná i LED u druhé zásuvky, která ještě nebyla fyzicky odpojena. Systém totiž vyhodnotí, že došlo k přerušení propoje mezi CC a PP zásuvkou a tak předpokládá, že celý úkon již byl dokonán. Nezbývá tedy nic jiného než vytahovat oba konektory současně, což v případě větší vzdálenosti mezi CC a PP panelem není možné. V takovém případě doporučuje autor vytahovat jako první konec kabelu, který je na straně CC panelu (aktivní prvky), na straně PP jsou totiž zásuvky popsány jedinečným, lehko zapamatovatelným číselným kódem.

- Vícenásobné plánování v rámci jednoho scanneru nebo dokonce zásuvky. Největší problém pro techniky a osoby, které plánují změny v patch zóně je nemožnost jednoduše naplánovat více změn v rámci jednoho scanneru tak, aby nemuselo být dodrženo pořadí těchto prací. Na panelech se totiž rozsvítí indikační LED pro první naplánovaný úkol a nezhasnou, dokud není tento úkol dokončen. Teprve poté systém načte další úkol a rozsvítí příslušné LED.

V případě, kdy se o patch zónu stará více techniků, může docházet k jejich zmatení, protože mohou být rozsvíceny indikační LED jiného úkolu, než který má daný technik přidělený. Ještě horší situace nastává, když je potřeba přepojit jednu konkrétní datovou zásuvku do jiného portu CC panelu (panel na straně aktivního prvku) například z důvodu změny VLAN, které jsou na jednotlivých portech switche nastaveny. Tento úkol se musí provést ve třech krocích – naplánovat odpojení původního propoje, počkat na odebrání cross-connect kabelu technikem a poté opět naplánovat cross-connect propojení do jiné zásuvky. Pokud je propojení fyzicky změněno bez tohoto postupu, dojde k tzv. „smíšenému stavu“, ze kterého se systém občas nevzpamatuje, pokud není tento stav rychle vyřešen vrácením do původního fyzického stavu kabeláže. V této situaci je jednodušší provést rekonfiguraci aktivního prvku, která s sebou nese ale určité riziko chyby a například odpojení celého aktivního prvku.

- Scanner neumí získat z připojených aktivních prvků ID vlan sítě, která je na konkrétním portu nastavena a zobrazit jej v přehledu. Tato funkcionalita vyloženě chybí. V naší organizaci používáme cca desítku vlan sítí na aktivních prvcích. Každá vlan má jiné možnosti, takže je nezbytné před plánováním zapojení datové zásuvky nahlédnout do jiné aplikace na přehled portů aktivního prvku, aby nedošlo k propojení koncového zařízení do nesprávné vlan.

- Cena řešení navyšuje cenu strukturované kabeláže o 20 až 50% v závislosti na velikosti instalace. Nejedná se tedy o levné řešení.

Aby byl autor práce objektivní, je nezbytné na tomto místě zmínit fakt, že společnost Molex se k zjištěným problémům nestaví zády a přislíbila řešení, které by některé problémy mělo vyřešit. Konkrétně problémy s trváním full-scanu, předčasným zhasínáním LED při rozpojování a eliminací „smíšeného stavu“ zásuvek. Bude ovšem nezbytné vyměnit všechny CC a PP panely, takže v určitých termínech se budeme muset v celém objektu potýkat s výpadky sítě v důsledku fyzického přepojování. Co se týče technického řešení – ve všech zásuvkách CC a PP panelů by měl přibýt mikrospínač, který bude při

zasunutí či vysunutí konektoru okamžitě oznamovat změnu stavu konkrétní zásuvky. Předběžně byl slíben termín vydání nových prvků na duben 2015.

Pokud výrobce vyřeší hlavní problémy, které byly popsány v této kapitole, lze řešení doporučit tam, kde se používá velké množství datových zásuvek a je kladen důraz na vyšší bezpečnost fyzické vrstvy sítě. Navíc po zhodnocení rizik, která mohou nastat v souvislosti se špatným fyzickým zabezpečením sítě, může být cena tohoto řešení zanedbatelnou položkou proti škodě, která může být způsobena.

# 6 Závěr

Cílem této diplomové práce bylo provést analýzu povinnosti subjektů státní správy v souvislosti s nově přijatým Zákonem o kybernetické bezpečnosti. Autor vycházel z tohoto zákona a z příslušných prováděcí právních předpisů (vyhlášek), které k tomu zákonu byly vydány.

V první kapitole a jejích podkapitolách se autor zaměřil na rodinu norem ISO/IEC 27000 a její jednotlivé části. Tyto normy jsou současným etalonem pro posuzování implementace ISMS a Zákon o kybernetické bezpečnosti z nich vychází. Podrobně byly prozkoumány požadavky norem ISO/IEC 27000, 27001 a 27002.

V navazující – druhé – kapitole se autor zaměřil na framework COBIT, ze kterého tvůrci Zákona o kybernetické bezpečnosti také vycházeli. Jelikož COBIT se na celou problematiku zaměřuje z hlediska organizace jako celku, byly na konci kapitoly shrnuty nejvíce patrné rozdíly mezi tímto frameworkem a ISO/IEC 27000.

Ve třetí kapitole autor analyzoval předpis č. 181/2014 Sb. – tedy Zákon o kybernetické bezpečnosti. Nejprve byl představen důvod vzniku tohoto zákona, jeho historie a základní principy. Podrobněji se autor zaměřil na důležité pojmy, které mají přesnou definici, a je tedy nezbytné jim porozumět. V navazující podkapitole byly vymezeny stěžejní body zákona, které je nezbytné dodržovat. Hlavní pilíře této kapitoly byly podrobněji autorem analyzovány v následujících podkapitolách, které se věnují povinnostem jednotlivých správců systémů a způsobu hlášení kybernetických incidentů. V poslední podkapitole byla představena bezpečnostní opatření včetně krátkých analýz jednotlivých bodů.

Ve čtvrté kapitole autor shrnuje celou teoretickou část do krátkého, přehledného celku. Jelikož je teoretická část obsáhlá, byly zde vyzdviženy nejdůležitější části z každé kapitoly. Z první kapitoly se jednalo o pojem ISMS a ISO/IEC27000. Z druhé kapitoly autor shrnul nejdůležitější body framewroku COBIT a porovnal jej s rodinou norem ISO/IEC27000. Ze třetí kapitoly byly vybrány odstavce, ve kterých autor upozorňuje na veškeré důležité informace týkající se Zákona o kybernetické bezpečnosti.

Pátá kapitola se zaměřuje na využití předchozích shrnutých znalostí v konkrétním prostředí a představuje jedno z možných řešení pro fyzickou bezpečnost objektu, ale i pro fyzickou a linkovou vrstvu modelu ISO/OSI. V prvé části se autor zaměřil na vysvětlení problematiky fyzické bezpečnosti, včetně základních pojmů a oblastí, které do ní spadají. V druhé části se autor pokusil vycházet z vlastních zkušeností a odhalit tak slabá místa zabezpečení objektu organizace, ve které pracuje. Byla navržena některá opatření, která by měla přispět k zlepšení tohoto zabezpečení. Jako stěžejní část práce si autor vybral analýzu bezpečnosti fyzické vrstvy, včetně návrhu zlepšení současné situace. V poslední podkapitole bylo toto řešení představeno a podrobně vysvětleny principy ochrany, kterou poskytuje na fyzické vrstvě sítě. Na závěr byly analyzovány silné a slabé stránky tohoto řešení, které se podařilo zjistit během implementace a krátkodobého užívání, které probíhalo současně při psaní této práce.

# 7 Seznam použité literatury


- GiTy a.s., 2008, ISMS - Seriál o řízení bezpečnosti [online]. [cit. 2015-02-01]. Dostupné z http://www.chrantesidata.cz/cs/art/472/

- ČSN ISO/IEC27000 třetí vydání, Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

- ISO27000 directory, 2010, An Introduction To ISO 27001 [online]. [cit. 2015-02-02], Dostupné z: http://www.27000.org/iso-27001.htm

- ANSI, 2015a, International Electrotechnical Commission [online]. [cit. 2015-02-02]. Dostupné z: http://webstore.ansi.org/SdoInfo.aspx?sdoid=40

- ANSI, 2015b, International Organization for Standardization [online]. [cit. 2015-02-02]. Dostupné z: http://webstore.ansi.org/SdoInfo.aspx?sdoid=39

- RAC s r.o., 2014, Řada norem ISO/IEC 27000. [online]. Sep 03, 2014 [cit. 2015-02-03]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ISO27000

- BERNARD, Pierre. *Cobit 5: a management guide*. 1st ed. Editor Ronald D Krutz. S.l.: Van Haren Pub, 2012. ISBN 978-908-7537-012.

- ISACA, 2012, Introduction to COBIT 5 [online]. [cit. 2015-02-03]. Dostupné z: http://www.isaca.org/Education/Upcoming-Events/Documents/Intro-COBIT5.pdf

- HARMER Geoff. Governance of Enterprise It Based on Cobit 5 A Management Guide. It Governance Pub, 2014. ISBN 978-184-9285-186.

- ISACA, 2015, Risk Scenarios Using COBIT 5 for Risk [online]. [cit. 2015-02-03]. Dostupné z: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Risk-Scenarios-Using-COBIT-5-for-Risk.aspx

- Varun Arora, 2010, Comparing different information security standards: COBIT v s. ISO 27001 [online]. [cit. 2015-02-04]. Dostupné z: https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf

- ITbiz.cz, 2014. Co bude znamenat zákon o kybernetické bezpečnosti pro firmy? [online]. Aug 29, 2014 [cit. 2015-02-04]. Dostupné z: http://www.itbiz.cz/zakon-o-kyberneticke-bezpecnosti-co-znamena-pro-firmy

- MENIER s.r.o., 2013, Návrh zákona o kybernetické bezpečnosti [online]. [cit. 2015-02-07]. Dostupné z: http://www.kyberbezpecnost.cz/?p=30

- CIMIB, 2013, Návrh zákona o kybernetické bezpečnosti [online]. [cit. 2015-02-08]. Dostupné z: http://www.cimib.cz/novinka/12-navrh-zakona-o-kyberneticke-bezpecnosti

- PETERKA, Jiří, 2014, Kdo (a co) bude spadat pod nový zákon o kybernetické bezpečnosti? [online]. [cit. 2015-02-09]. Dostupné z: http://www.lupa.cz/clanky/kdo-a-co-bude-spadat-pod-novy-zakon-o-kyberneticke-bezpecnosti/

- NBÚ, 2014, Prohlášení Národního bezpečnostního úřadu k vývoji legislativy v oblasti kybernetické bezpečnosti [online]. [cit. 2015-02-09]. Dostupné z: http://www.nbu.cz/cs/aktuality/611-prohlaseni-narodniho-bezpecnostniho-uradu-k-vyvoji-legislativy-v-oblasti-kyberneticke-bezpecnosti/

- Bureau Veritas Czech Republic, 2014, Zákon o kybernetické bezpečnosti podepsán prezidentem, účinnost od 1. ledna 2015 [online]. [cit. 2015-02-10]. Dostupné z: http://www.bureauveritas.cz/wps/wcm/connect/bv_cz/local/home/news/press-releases/zakon-o-kyberneticke-bezpecnosti

- TOBOLKA, Martin, 2011, Jak na havarijní plány a plány obnovy ICT infrastruktury? [online]. [cit. 2015-02-09]. Dostupné z: http://www.systemonline.cz/sprava-it/ jak-na-havarijni-plany-a-plany-obnovy-ict-infrastruktury.htm

- HARRIS, Shon. *Hacking: manuál hackera*. 1. vyd. Praha: Grada, 2008, ISBN 978-80-247-1346-5.

- PERDIKARIS, John. *Physical security and environmental protection*. 2014. ISBN 978-148-2211-948.

- *Provozování kamerových systémů: metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů*. Editor David Burian. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2012, 27 s. ISBN 978-80-210-6017-3.KIZZA, Joseph Migga. *Computer network security and cyber ethics*. Fourth edition, 2014. ISBN 978-078-6493-920.

- KINGSLEY-HEFTY, John. *Physical security strategy and process playbook*. Oxford: Elsevier, 2013. ISBN 978-012-4172-272.

- RICKS, Truett A.; RICKS Bobby E.; DINGLE Jeffrey. *Physical security and safety: a field guide for the practitioner*. 2014. ISBN 978-148-2227-024.

- COLE, Eric a CONLEY James W. *Network security bible*. 2nd ed. Indianapolis: Wiley Publishing, 2009. ISBN 978-0-470-50249-5.

- CIAMPA, Mark D. *Security guide to network security fundamentals*. 4th ed. Boston, MA: Course Technology, Cengage Learning, 2012. ISBN 11-116-4012-2.

- BLOCH, Matthieu a BARROS, Joao. *Physical-layer security: from information theory to security engineering*. New York: Cambridge University Press, 2011. ISBN 978-052-1516-501.

- KIZZA, Joseph Migga. *Computer network security and cyber ethics*. Fourth edition, 2014. ISBN 978-078-6493-920.

- NETWORK GROUP, s.r.o., 2014, Management fyzické vrstvy [online]. [cit. 2015-03-31]. Dostupné z: http://proficomms.cz/Files/download/bezpecnost_2014/proficomms_MIIM.pdf

- HELÁN, Radek, Inteligentní sítě – management na fyzické vrstvě [online]. [cit. 2015-03-31]. Dostupné z: http://www.netguru.cz/odborne-clanky/inteligentni-sit-management-na-fyzicke-vrstv.html

# 8 Seznam ilustrací

# 9 Seznam tabulek