Zajištění bezpečnosti datového centra

Bc. Libor Černý

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

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

Jméno a příjmení:	**Bc. Libor Černý**
Osobní číslo:	**A12766**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Zajištění bezpečnosti datového centra**
Téma anglicky:	**Ensuring the Security of a Data Centre**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Definujte požadavky na fyzickou bezpečnost datového centra.**
3. **Popište možnosti implementace systémů IPS.**
4. **Navrhněte fyzický a logický design počítačové sítě s ohledem na bezpečnostní požadavky.**
5. **Navrhněte systém kontroly bezpečnosti počítačové sítě pomoci systému IPS.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **COLE, Eric. Network security bible. 2nd ed. Indianapolis: Wiley Publishing, 2009, 891 p. ISBN 978-0-470-50249-5.**
2. **SOSINSKY, Barrie. Mistrovství-počítačové sítě. 1. vyd. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.**
3. **BERKA, Milan. Bezpečná počítačová síť. Praha: Dashofer, 2004, 1600 s. ISSN 1801-8033.**
4. **ENDORF, Carl. Detekce a prevence počítačového útoku. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.**
5. **FRYE, Douglas W. Network security policies and procedures. New York: Springer, 2007, 240 p. ISBN 03-874-7955-4.**
6. **SINGH, Abhishek. Vulnerability analysis and defense for the Internet. New York: Springer, 2008, 254 p. ISBN 03-877-4390-1.**
7. **WU, Chwan-Hwa. Introduction to computer networks and cybersecurity. Boca Raton: CRC Press, 2013, 1336 p. ISBN 978-1-4665-7213-3.**
8. **SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 304 s. ISBN 978-80-251-3752-9.**

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

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

ABSTRAKT

Práce popisuje problematiku a definuje požadavky na zabezpečení datového centra. Řeší fyzické zabezpečení a režimová opatření, bezpečnostní standardy v souladu s legislativními požadavky a doporučeními ČSN a ISO norem. Navrhuje fyzický design datového centra, logický design počítačové sítě a zamýšlí se nad ochranou počítačových sítí před hackerskými útoky pomocí systému detekce a prevence.

Klíčová slova: datové centrum, fyzický design, logický design, systém IPS, systém IDS.

ABSTRACT

The work describes the problem and defines the security requirements of a data centre. It addresses the physical security and regime measures, safety standards in accordance with legislative requirements and recommendations of ČSN and ISO standards. Suggests a physical data center design, logical design of computer networks and considers the protection of computer networks from hacker attacks using the detection and prevention systems.

Keywords: data centre, physical design, logical design, IPS, IDS.

Na tomto místě bych velmi rád poděkoval Ing. Miroslavu Matýskovi, Ph.D. za jeho odborné vedení, cenné připomínky a odborné rady, kterými přispěl k vypracování této diplomové práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Informace, podpůrné procesy, informační systémy a počítačové sítě jsou aktiva, která mají pro organizace hodnotu. Je tedy nutné je vhodným způsobem chránit. Bezpečnost informací a systémů zajišťuje potřebnou kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost podnikatelských investic.

Se vzrůstající propojeností prostředí informačních systémů jednotlivých organizací tato potřeba v současné době roste, jelikož jsou informace a systémy vystaveny zvyšujícímu se počtu známých i neznámých hrozeb a zranitelností. Mezi zranitelnosti a bezpečnostní hrozby řadíme např. počítačové podvody, špionáže, hackerské útoky, sabotáže, vandalizmus, požáry a povodně, počítačové viry, útoky typu odepření služby.

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních rizik. Výdaje na bezpečnostní opatření by měly odpovídat ztrátám způsobeným narušením bezpečnosti. Výsledky hodnocení rizik pomohou určit vedení organizace odpovídající kroky i priority pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu. Hodnocení rizik by mělo být prováděno periodicky, aby bylo možné včas reagovat na jakékoliv změny v bezpečnostních požadavcích.

Datové centrum jsou prostory či objekty určené k bezpečnému umístění technologií informačních systémů. Pojem datové centrum představuje komplex standardů, norem, požadavků a doporučení, které je nutné dodržovat. Nicméně praktické zkušenosti, všeobecný nadhled nad problematikou a porozumění široké škále oblastí a technologií je nezbytnou podmínkou pro úspěšné vytvoření designu datového centra. Zabezpečení datového centra úzce souvisí s fyzickou bezpečností. Fyzická bezpečnost je soubor konstrukčních, technických a organizačních opatření a norem. Normy jsou definovány jako směrnice nebo pravidlo, jehož zachování je závazné. Normy skupiny ISO 27000 popisují zavádění, provozování, monitorování, udržování a zlepšování systému managementu bezpečnosti informací.

Cílem IDS a IPS systémů je poskytnout profesionálům kompletní obrázek o detekci narušení a schopnostech prevence, které jsou v současnosti dostupné. "*Narušení je aktivní posloupnost odpovídajících událostí, které se záměrně snaží uškodit takovou měrou, že popisovaný systém je nepoužitelný, dochází ke zpřístupnění neautorizovaných informací nebo je s nimi manipulováno.*"[1]

V roce 2003 významná výzkumná a konzultační firma Gartner Group ohlásila, že systémy detekce narušení, které byly na trhu dostupné, selhávají a že nesplnily očekávání s ohledem na svou cenu a že v následujícím roce budou již zastaralé. Tím se výrazně zvýšila pozornost o budování systémů detekce narušení a její prevence.

Detekce narušení má své problémy, jako např. falešné pozitivní útoky, provozní otázky ve vysokorychlostním prostředí a potíže s detekcí neznámých hrozeb. Většina problémů je způsobena nesprávnou implementací a nesprávným chápáním toho, co tato technologie může a nemůže poskytnout.

Zranitelné místo neboli zranitelnost je slabé místo, které může být zneužito k neoprávněnému přístupu do informačního systému organizace. Pokud je zranitelnost již veřejně známá a začne se používat na mnoha místech k podobným útokům, stane se z ní tzv. zneužití (exploit). Každý software má své chyby a výrobci je odstraňují pravidelnými aktualizacemi. Po zveřejnění aktualizace ji začnou ověřovat lidé, kteří mají zájem na útoku prostřednictvím příslušné zranitelnosti. Automatizovaný útok, který vadu zneužívá dříve, než jsou záplaty implementovány, se nazývá útok prvního dne (zero day exploits).

I. TEORETICKÁ ČÁST

1 LEGISLATIVNÍ POŽADAVKY A STANDARDIZACE

Nezávislé akreditované organizace provádějí bezpečnostní ohodnocení jednotlivých produktů a systémů na základě bezpečnostních standardů. Průkopníkem formalizovaných bezpečnostních kriterií jsou Trusted Computer System Evaluation Criteria (TCSEC), známá také jako „Orange Book“, která byla přijata v USA v roce 1983. V dalších letech začala vznikat řada národních standardů. Prvním krokem ke sjednocení bylo vytvoření standardu Information Technology Security Evaluation Criteria (ITSEC) na základě standardů Velké Británie, Francie, Německa a Holandska. Oproti TCSEC nabízel ITSEC větší míru flexibility z hlediska hodnocených systémů a jejich parametrů a lépe tak reagoval na požadavky komerční i bezpečnostní sféry.

Standard Common Criteria for Information Technology Security Evaluation (často označovaného za Common Criteria – CC) byl následně v roce 1999 přijat také jako mezinárodní norma ISO/IEC 15408:1999. Mezinárodní dohody související s CC navíc umožnily vzájemné uznávání certifikace mezi zeměmi a definovaly společnou metodiku provádění ohodnocení. Mezi země uznávající certifikace provedené na základě této normy se řadí i Česká republika. Byla také vyvinuta společná metodologie pro provádění hodnocení – Common Evaluation Metodology (CEM). CEM zahrnuje hodnocení na úrovních EAL1 až EAL4. Hodnocení podle CC se soustřeďuje na hodnocení produktů IT (např. operační systémy, databázové systémy, síťové produkty, specializované bezpečnostní produkty), hodnocení sady bezpečnostních požadavků a specifikací pro daný produkt bezpečnostní cíl (Security Target, ST) a hodnocení implementačně nezávislé sady bezpečnostních požadavků nazývané profil ochrany (Protection Profile, PP). ST a PP se hodnotí zejména z hlediska úplnosti, konzistence a technické správnosti a tedy vhodnosti pro proklamované použití. Tyto požadavky mohou být vybrány z CC nebo být vyjádřeny explicitně a mají zahrnovat i úroveň jistoty ohodnocení (Evaluation Assurance Level, EAL). PP se obvykle vytváří tak, aby byl opakovatelně použitelný, a musí obsahovat i zdůvodnění bezpečnostních cílů a požadavků TOE (Target of Evaluation).

Legislativní požadavky na fyzickou bezpečnost datového centra:

- Vyhláška č. 528/2005 Sb. „*o fyzické bezpečnosti a certifikaci technických prostředků*“, vyhláška č. 19/2008 Sb. a vyhláška č. 454/2011 Sb.

- Zákon č. 32/2008 Sb., kterým se mění zákon č. 412/2005 Sb., *„o ochraně utajovaných informací a o bezpečnostní způsobilosti“*.

Normativní požadavky a standardy na fyzickou bezpečnost datového centra:

- Norma ČSN ISO/IEC 15408:2005.
- Norma ČSN ISO/IEC 17799:2005.
- Soubor norem ISO/IEC 27000.

Metodiky a nástroje CRAMM, RiskPAC, CORAS, EBIOS, Attack Tree Modelling, Octave, Mehari, SOMAP nebo Metodika řízení zranitelností ICT se používají k bezpečnostní analýze rizik informačních systémů, provádí hodnocení aktiv, hodnocení rizik a protiopatření, a výsledkem je pak reportování nebo audit bezpečnostního stavu informačních systémů. Metodiky využívají uvedené normy z oblasti informační bezpečnosti [2], [7].

1.1 Vyhláška č. 528/2005 Sb.

Tato vyhláška stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku. V podstatě slouží k určení míry zabezpečení bezpečné oblasti.

I když se týká zákona č. 412/2005 Sb. *„o ochraně utajovaných informací a o bezpečnostní způsobilosti“*, je možné její myšlenky použít i u jiných nebo méně citlivých informací jako poměrně dobrý návod na vybudování ochrany datových center. Dobrým materiálem je především příloha č. 1 této vyhlášky. Následné novelizace proběhly vyhláškami č. 19/2008 Sb. a č. 454/2011 Sb., ty však přináší jen formální úpravy a z věcného hlediska nedochází ke změnám. Ani změnou zákona č. 32/2008 Sb., kterým se mění zákony č. 412/2005 Sb., č. 499/2004 Sb., *„o archivnictví a spisové službě a o změně některých zákonů“*, a zákon č. 106/1999 Sb., *„o svobodném přístupu k informacím“*, nedochází ke změnám v definici fyzické bezpečnosti.

Vyhláška definuje následující základní pojmy, použitelné i pro účely datových center:

- objektem je budova nebo jiný ohraničený prostor, ve kterém se zpravidla nacházejí zabezpečené nebo jednací oblasti,

- hranicí objektu plášť budovy, fyzická bariéra (oplocení) nebo jinak viditelně vymezená hranice,
- hranicí zabezpečené oblasti stavebně nebo jinak viditelně ohraničený prostor,
- vstupem do objektu, zabezpečené oblasti místo určené pro vstup a výstup osob a místo určené pro vjezd a výjezd dopravních prostředků,
- hrozbou možnost vyzrazení nebo zneužití utajované informace při narušení fyzické bezpečnosti,
- rizikem pravděpodobnost, že se určitá hrozba uskuteční,
- mimořádnou situací stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití utajované informace,
- technickým prostředkem bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje, oznamuje nebo zaznamenává narušení zabezpečení objektu, zabezpečené oblasti nebo jednací oblasti a dále ničí utajované informace,
- úschovným objektem trezor nebo jiná uzamykatelná schránka [2], [8].

1.1.1 Zabezpečení objektu a zabezpečené oblasti

Hranici objektu nebo zabezpečené oblasti, zařazení objektu nebo zabezpečené oblasti do příslušné kategorie a zařazení zabezpečené oblasti do příslušné třídy stanoví provozovatel objektu. V případě, že hranice objektu je totožná s hranicí zabezpečené oblasti, je rozsah použití opatření fyzické bezpečnosti určen požadavky na kategorii zabezpečené oblasti.

Zabezpečení objektu nebo zabezpečené oblasti je zajišťováno kombinací opatření fyzické bezpečnosti, v závislosti na kategorii objektu, s ohledem na charakter hranice objektu a v závislosti na vyhodnocení rizik těmito technickými prostředky:

- pro kategorii Vyhrazené – mechanické zábranné prostředky,
- pro kategorii Důvěrné a Tajné – mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace,
- pro kategorii Přísně tajné – mechanické zábranné prostředky, zařízení elektrické zabezpečovací signalizace a speciální televizní systémy. Speciální televizní

systémy nesmí narušit ochranu utajovaných informací. Speciální televizní systémy lze nahradit tísňovými systémy.

Bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti jsou stanoveny v příloze č. 1 vyhlášky. Objekty a zabezpečené oblasti kategorie Důvěrné a vyšší, v nichž je zajištěna trvalá přítomnost zde pracujících osob, se zabezpečují zejména mechanickými zábrannými prostředky a zařízením elektrické zabezpečovací signalizace a nebo tísňovým systémem. Plní-li tyto zabezpečené oblasti současně úlohu stanovišť určených pro stálý výkon ostrahy, nemusí být vybaveny zařízeními elektrické zabezpečovací signalizace. K zabezpečení zabezpečených oblastí se používají certifikované nebo necertifikované technické prostředky. Necertifikované technické prostředky lze použít pouze za předpokladu, že nesníží úroveň ochrany požadované pro daný stupeň utajení. Mechanickými zábrannými prostředky se rozumí zejména zámky, dveře, mříže, folie, skla a další bezpečnostní konstrukční a stavební prvky. Mechanickými zábrannými prostředky se zabezpečují průlezné otvory, které dovolí průchod šablony o níže uvedených rozměrech.

Tab. 1. Rozměry průleznýchotvorů [2].

Průlezný otvor	Rozměr
obdélník	400mm x 250mm
elipsa	400mm x 300mm
kruh	průměr 350 mm

Pokud je průlezný otvor zabezpečen mechanickým zábranným prostředkem s jedním nebo více otvory (např. mříž), nesmí tyto otvory dovolit průchod šablony ve tvaru elipsy o rozměrech 250 mm x 150 mm a tloušťky 20 mm [2], [8].

1.1.2 Režimová opatření

Bodové hodnoty režimových opatření jsou stanoveny v příloze č. 1 vyhlášky. Režimová opatření jsou:

- stanovení oprávnění osob a dopravních prostředků pro vstup do objektu,

- stanovení oprávnění osob pro vstup do zabezpečené oblasti a jednací oblasti a způsob kontroly těchto oprávnění,
- kontrolní opatření při vstupu do objektu, zabezpečených oblastí a způsob kontroly těchto opatření,
- podmínky a způsob kontroly pohybu osob v objektu, zabezpečené oblasti a způsob kontroly a vynášení utajovaných informací z objektu, zabezpečené oblasti,
- režim manipulace s klíči a identifikačními prostředky, zejména způsob jejich označování, přidělování, úschovy a evidence,
- režim manipulace s technickými prostředky a jejich používání,
- režim pohybu utajovaných informací v objektu, zabezpečené oblasti.

Oprávnění ke vstupu do objektu nebo zabezpečené oblasti vydává odpovědná osoba. Oprávnění ke vstupu lze vydat osobě, která je poučena a je držitelem oznámení o splnění podmínek pro přístup k utajované informaci anebo obecně osobě oprávněné pro vstup do datového centra. Seznam osob se ukládá u odpovědné osoby.

Osoby bez oprávnění ke vstupu mohou do objektu vstupovat pouze za doprovodu osoby oprávněné ke vstupu do příslušného objektu, zabezpečené oblasti.

Na vstupu do objektu se provádí kontrola vstupu a u osob bez oprávnění ke vstupu do objektu je vedena evidence údajů a povinně se stanoví režim návštěv s doprovodem.

Při vstupu osob bez oprávnění ke vstupu do objektu kategorie Přísně tajné se u nich provádí kontrola zařízením sloužícím k vyhledávání nebezpečných látek nebo předmětů [2], [8].

1.2 ČSN ISO/IEC 15408:2005

Norma využívá kritéria CC, podle kterých musí informační systém obsahovat vhodné bezpečnostní funkce, jakými jsou např. řízení přístupu, autentizace, audit apod. Norma definuje sedm úrovní EAL, v komerční praxi se však používají pouze první čtyři. Jednotlivé úrovně lze popsat následujícím způsobem:

- EAL1 je vhodná, pokud je vyžadována určitá základní důvěra ve správnost fungování hodnoceného PP, ST nebo TOE, avšak hrozby nejsou považovány za

vážné. Důvěry se dosahuje nezávislým testováním shody hodnoceného PP, ST nebo TOE s neformální funkční specifikací a zkoumáním předložených příruček pro uživatele.

- EAL2 již vyžaduje spolupráci vývojáře, který musí v podstatě dodat funkční specifikace, určité informace o návrhu bezpečnostních funkcí (na úrovni globálního návrhu, high-level design) a výsledky testování, avšak vývoj si nevyžaduje více úsilí nežli je potřebné pro dodržování dobré komerční praxe, a v podstatě nepřináší zvýšení nákladů. Poskytuje nízkou až střední nezávisle ověřenou bezpečnost v případě, že není dostupná kompletní informace z fáze vývoje. Důvěry se dosahuje analýzou vyžadované dokumentace, ověřením výsledků některých testů, analýzou síly funkcí a analýzou zřejmých zranitelností. Pro TOE musí být sestaven seznam konfigurace a vypracovány procedura pro bezpečnou instalaci, generování a spouštění.
- EAL3 je možno ještě dosáhnout bez podstatných změn základních existujících vývojářských praktik. Je aplikovatelná v případě, že se vyžaduje střední úroveň nezávisle ověřené bezpečnosti a je opřena o důkladné zkoumání TOE (ST, PP). Navíc oproti EAL2 se vyžaduje rozsáhlejší testování, kontroly vývojového prostředí a zajištění správy konfigurace.
- EAL4 stále umožňuje pohybovat se v rámci dobré komerční vývojářské praxe. Jakkoliv přísné jsou tyto praktiky, nevyžadují podstatné specializované znalosti, dovednosti a jiné zdroje. EAL4 je nejvyšší úrovní záruk, kterou lze dosáhnout (za rozumné náklady) zpětně pro již existující produkt. Poskytuje střední až vysokou úroveň záruky nezávisle ověřené bezpečnosti pro běžnou komoditu produktů a vyžaduje ze strany vývojáře nebo uživatelů připravenost k pokrytí dodatečných specifických nákladů spjatých s bezpečnostním inženýrstvím. Navíc oproti EAL3 se již vyžaduje také detailní návrh (low-level design) TOE, neformální model bezpečnostní politiky TOE a dodání určité podmnožiny implementace (např. část zdrojového kódu bezpečnostních funkcí). Nezávislá analýza zranitelností musí demonstrovat odolnost vůči průniku útočníků s nízkým potenciálem pro útok. Kontroly vývojového prostředí jsou doplněny modelem životního cyklu, stanovením nástrojů a automatizovanou správou konfigurace [2], [8].

1.3 ČSN ISO/IEC 17799:2005

Norma byla schválena v originálním znění Českým normalizačním institutem v roce 2001. Tato mezinárodní norma obsahuje postupy a opatření, které by měl management daného subjektu implementovat pro zajištění informační bezpečnosti – pro zajištění integrity, důvěrnosti a dostupnosti informací. Norma popisuje samotný pojem informační bezpečnost, důležitost informační bezpečnosti a stanovení požadavků na bezpečnost.

Norma obsahuje celkem 11 základních oddílů bezpečnosti, které jsou dále rozděleny do 39 kategorií bezpečnosti (počet je uvedený v závorce za názvem oddílu):

- Bezpečnostní politika (1).
- Organizace bezpečnosti (2).
- Klasifikace a řízení aktiv (2).
- Bezpečnost lidských zdrojů (3).
- Fyzická bezpečnost a bezpečnost prostředí (2).
- Řízení komunikací a řízení provozu (10).
- Řízení přístupu (7).
- Vývoj, údržba a rozšíření informačního systému (6).
- Zvládání bezpečnostních incidentů (2).
- Řízení kontinuity činností organizace (1).
- Soulad s požadavky (3).

Každá z 39 kategorií bezpečnosti obsahuje cíl kontrolního opatření, který určuje čeho má být dosaženo a jedno nebo více opatření, která lze použít k dosažení stanoveného cíle opatření. Cíle opatření poskytují kvalitní základ pro definici sady axiomů pro bezpečnostní politiku. Norma nepřikazuje, která opatření musí být bezpodmínečně aplikována, ale ponechává rozhodnutí na organizaci. Vhodná opatření jsou vybírána na základě hodnocení rizik a jejich implementace je závislá na konkrétní situaci. Cílem není implementovat vše, co norma popisuje, ale spíše naplnit všechny aplikovatelné cíle opatření. Tento přístup zajišťuje, že norma je široce aplikovatelná a dává uživatelům velkou flexibilitu při implementaci. Oddíl zaměřený na fyzickou bezpečnost a bezpečnost prostředí popisuje

problematiku fyzického přístupu nepovolaných osob do zabezpečených objektů, do bezpečných místností a k citlivým zařízením. Zpracování citlivých a kritických obchodních informací má být umístěno v bezpečných oblastech a k jejich ochraně mají být zavedeny vhodné postupy. Má být prováděna kontrola jejich dodržování [2], [7].

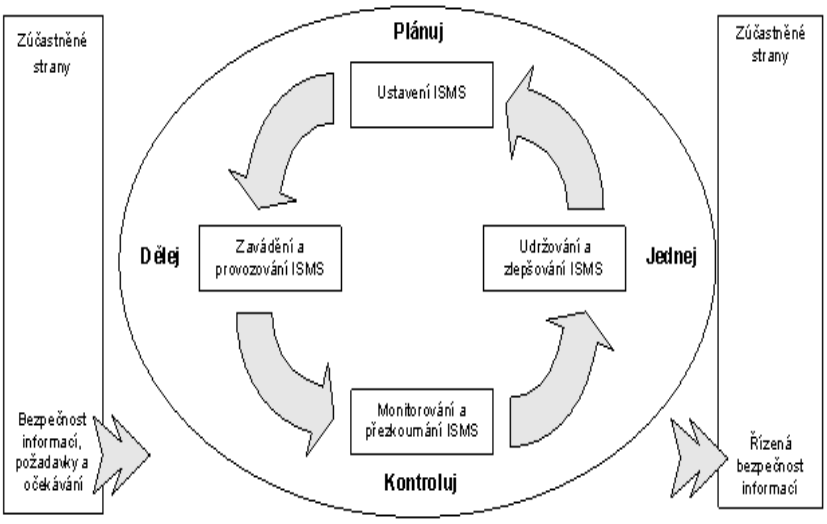
1.4 Norma ISO/IEC 27001:2005

Tato mezinárodní norma poskytuje podporu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování systému managementu bezpečnosti informací (ISMS – Information Security Management System). Přijetí ISMS by mělo být strategickým rozhodnutím organizace. Návrh a zavedení ISMS v organizaci je podmíněno potřebami a cíli činností, požadavky na bezpečnost, dále pak používanými procesy a velikostí a strukturou organizace. Tato norma je určena k posuzování souladu ze strany zainteresovaných interních i externích stran.

Aby organizace fungovala efektivně, musí identifikovat a řídit mnoho vzájemně propojených činností. Norma prosazuje přijetí procesního přístupu, který znamená:

- pochopení požadavků na bezpečnost informací organizace a potřebu stanovení politiky a cílů bezpečnosti informací,
- zavedení a provozování opatření pro management bezpečnosti informací v kontextu s řízením celkových rizik činností organizace,
- monitorování a přezkoumání výkonnosti a účinnosti ISMS,
- neustálé zlepšování založené na objektivním měření.

Model známý jako Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act, PDCA) může být aplikován na všechny procesy ISMS tak, jak jsou zavedeny touto normou. ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup a pomocí nezbytných činností a procesů vytváří výstupy bezpečnosti informací, které splňují tyto požadavky a očekávání.



Obr. 1. PDCA model aplikovaný na procesy ISMS [2].

Tab. 2. Aplikace ISMS procesů podle PDCA [2].

Plánuj (ustavení ISMS).	Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
Dělej (zavádění a provozování ISMS).	Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
Kontroluj (monitorování a přezkoumání ISMS).	Posouzení, kde je to možné i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
Jednej (udržování a zlepšování ISMS).	Přijetí opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.

Systém řízení by měl vyváženě přistupovat k řešení fyzické, technické, procedurální a personální bezpečnosti. Bez formálního přístupu u komplexního systému hrozí nebezpečí opomenutí vedoucí k narušení bezpečnosti. Bezpečnost informací je zejména o systému řízení, nikoli o technologiích. Bezpečnostní politiky lze vydat jako samostatné dokumenty, které jsou jako podřízená součást dokumentu „Celková bezpečnostní informační politika“. Výhodou takového přístupu je snadnější aktualizace podřízených dokumentů. Na jednotlivé bezpečnostní politiky by pak měla navazovat jednotlivá opatření z odpovídající normy.

Vzorové bezpečnostní politiky ISMS podle ISO 27001 jsou:

- Systémová bezpečnostní politika – systém ochrany proti škodlivým kódům.
- Systémová bezpečnostní politika – systém práce s internetem.
- Systémová bezpečnostní politika – interní sítě.
- Systémová bezpečnostní politika – systémy pro vzdálený přístup.
- Systémová bezpečnostní politika pro síťové prvky.
- Systémová bezpečnostní politika správy hesel.
- Systémová bezpečnostní politika pro virtuální privátní sítě (VPN) [2], [8], [9].

1.5 Další normy skupiny ISO 27000

Mezinárodní organizace pro standardizaci ISO (International Organization for Standardization) rezervovala sérii 27000 pro normy z oblasti bezpečnosti informací. Na základě standardu ISO Guide 83 publikovaného v roce 2012, mají všechny standardy rodiny 27000 definovanou jednotnou strukturu a pravidla pro začlenění specifických požadavků.

Doposud byly publikovány následující normy (pozn. zúžený výběr pouze pro účely práce):

- ISO 27000 – poskytuje celkový přehled, definice pojmů a terminologický slovník pro všechny ostatní normy ze série 27000.
- ISO 27001 – hlavní norma pro ISMS, dříve známá jako BS7799, podle které jsou systémy certifikovány. Poslední revize normy byla publikována v roce 2013.

Specifikuje požadavky na implementaci bezpečnostních opatření a závazné požadavky nezbytné pro certifikaci.

- ISO 27002:2005 – norma byla publikována v roce 2005 jako ISO/IEC 17799:2005. V roce 2007 došlo k jejímu přejmenování na ISO/IEC 27002:2005, kdy obsah předchozí normy byl zachován. Poslední revize normy proběhla v roce 2013. Poskytuje návod na implementaci opatření pro dosažení informační bezpečnosti. Soubor postupů pro řízení informační bezpečnosti. Obsahuje katalog v praxi osvědčených bezpečnostních opatření.
- ISO 27003:2010 – návod pro návrh a zavedení ISMS v souladu s ISO 27001. Obsahuje procesně orientovaný přístup, založený na modelu PDCA, k úspěšné implementaci ISMS dle ISO 27001.
- ISO 27004:2009 – Měření řízení informační bezpečnosti - návod pro vývoj a proces měření s cílem hodnotit efektivnost ISMS.
- ISO 27005:2011 – Řízení rizika informační bezpečnosti – poskytuje metodiku pro hodnocení rizik.
- ISO 27006:2007 – požadavky na akreditaci orgánů vykonávající audity a certifikace ISMS.
- ISO 27007:2011 – požadavky na provádění auditů ISMS.
- ISO 27008:2011 – obsahuje doporučení auditorům ISMS a doplňuje ISO 27007.
- ISO 27010:2012 – poskytuje doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci.
- ISO 27031:2011 – obsahuje doporučení pro zajištění kontinuity činností organizace (business continuity).
- ISO 27033:2009 – soustava norem poskytující doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí. Prozatím byly vydány první tři části normy:
    - ISO/IEC 27033-1:2009 Network Security Part 1: Overview and concepts,
    - ISO/IEC 27033-2:2009 Network Security Part 2: Guidelines for the design and implementation of network security,

- ISO/IEC 27033-3:2010 Network Security Part 3: Reference networking scenarios – Threats, design techniques and control issues.

Připravované normy:

- ISO 27017 – norma by měla poskytovat doporučení pro zabezpečení cloud computingu.
- ISO 27018 – norma by měla poskytovat doporučení ohledně ochrany osobních údajů v cloud computingu.
- ISO 27039 **– norma** by měla obsahovat doporučení pro výběr, nasazení a provoz systémů pro detekci a prevenci bezpečnostních průniků (Intrusion Detection and Prevention Systems – IDPS) [2], [7], [10], [12].

1.6 Metodika řízení zranitelností ICT

Typy zranitelností v oblasti informačních a komunikačních technologií (Information and Communication Technologies – ICT) vycházejí z jejich technologické podstaty:

- chyby v programovém kódu, vzniklé během vývoje produktu nebo při aktualizacích a opravách SW,
- chyby v nastavení bezpečnostních parametrů, vzniklé během instalace, konfigurace a provozních modifikacích,
- chyby v návrhu bezpečnostní koncepce nebo architektury IS.

První skupina představuje nejčastější typ, protože chyby se vyskytují prakticky u všech technických prostředků informačních systémů – např. Firmware serverů, síťových prvků, telekomunikačních zařízení, operačních systémech i aplikacích.

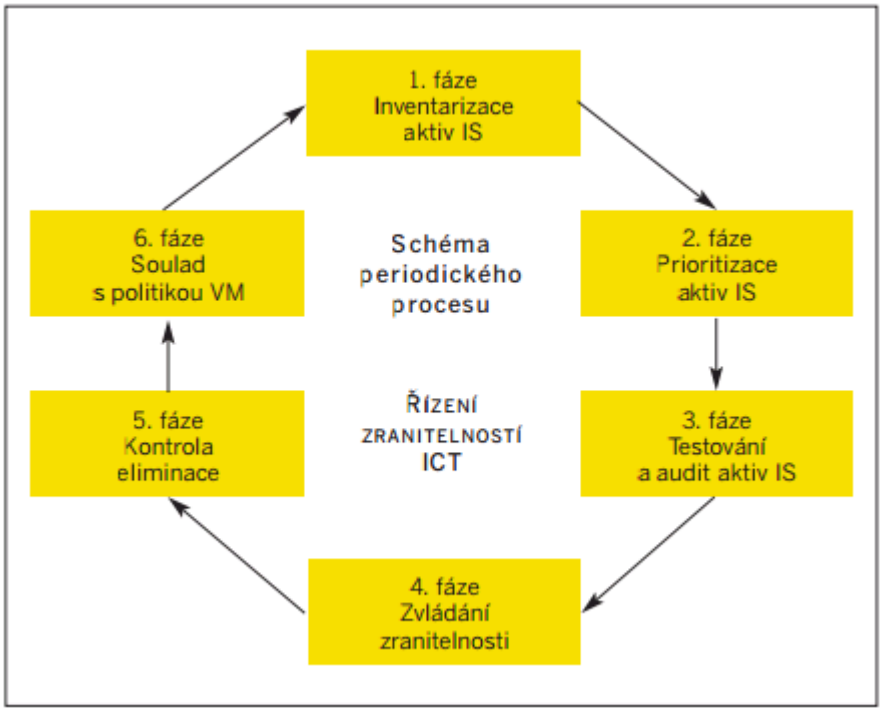
Druhá skupina je silně závislá na znalostech a dovednostech administrátorů nebo dodavatelů systémů, provádějící implementaci systémů.

Třetí skupina je nejobtížněji identifikovatelná a hodnotitelná, jelikož návrh závisí na mnoha dalších okolnostech, jako jsou potřeby a preference organizace, finanční požadavky nebo požadavky odpovědných osob v organizaci. Tento typ zranitelností nelze zjistit pomocí automatizovaných nástrojů jako jsou vulnerability scannery. Jediným způsobem je

expertní posouzení návrhu, porovnání koncepce a architektury s „best practices“ v dané oblasti.

Experti ve svém oboru se dokáží s nadhledem podívat na zvolenou koncepci a upozornit na slabá místa.

Systém řízení zranitelností byl poprvé zaveden do normy ISO 17999:2005 s cílem snížit rizika vyplývající ze zneužití veřejně publikovaných technických zranitelností. V roce 2005 byl standard začleněn do norem skupiny ISO 27001:2005 a tím byla otevřena cesta k certifikacím Systémů řízení bezpečnosti informací. Zranitelnost tvoří jednu ze tří složek rizika (aktivum, zranitelnost, hrozba) a proto proces řízení zranitelností náleží do procesu řízení rizik IS. Hlavním principem tohoto procesu je posunout se z výchozího stavu ad-hoc řešení problémů a intuitivních instalací bezpečnostních záplat do stavu řízení zranitelností, kdy se zranitelnosti řeší podle priorit.



Obr. 2. Schéma periodického procesu řízení zranitelností ICT [2].

Zranitelnosti produktů a systémů lze dělit podle způsobu jejich dostupnosti na vnější nebo vnitřní hrozby. Dále dle způsobu zneužití na network-based (NB) a host-based (HB). NB útoky jsou branou útočníků pro další eskalaci útoků uvnitř infrastruktury, jsou dostupné po

síti pomocí otevřených TCP portů libovolnému útočníkovi. Statistickým sledováním zranitelností a typů útoků se zabývá i firma Qualys Inc., která vydává seznam nejkritičtějších a nejrozšířenějších zranitelností dle SANS TOP 20 [2], [12], [20].

1.7 Analýza rizik

Na základě analýzy rizik lze stanovit bezpečnostní opatření pro vnitřní a vnější hrozby, nepokryté již identifikovanými požadavky, a případně sílu mechanismů, kterými mají být vzhledem ke zvýšenému riziku bezpečnostní funkce realizovány. Jednou z hrozeb specifických pro datová centra je, že neoprávněná osoba získá fyzický přístup i přes použitá opatření fyzické bezpečnosti, následně odcizí, poškodí, zničí HW vybavení nebo kabeláž, popřípadě získá médium s utajovanými informacemi, logický přístup do systému umožňující narušení systémového a aplikačního programového vybavení a manipulaci s utajovanými informacemi. Pro analýzu rizik lze použít několik specifických metodik (viz. 1), nicméně všechny se shodují v základních principech, které jsou uplatněny v následujícím postupu CRAMM Express:

- Identifikace a vytvoření modelu aktiv a stanovení jejich hodnoty.
- Identifikace hrozeb a zranitelností a určení jejich úrovně, výpočet míry rizika.
- Návrh protiopatření na pokrytí zjištěných rizik.

Metodika CRAMM je plně kompatibilní s normami řady 27000.

Prvním ze dvou základních přístupů analýz rizik je analýza rizik využívající matice aktiv a zranitelností. Do matice aktiv se doplní identifikovaná aktiva spolu s jejich hodnotou. Do matice zranitelností identifikované hrozby a jejich pravděpodobnosti. Pro identifikaci hrozeb lze využít katalog hrozeb uvedený v ČSN ISO/IEC TR 13335, nebo norem ČSN 17799 a ISO 27005. V dalším kroku se posuzuje zranitelnost jednotlivých aktiv jednotlivými hrozbami a doplní se matice zranitelností. V případě, že mezi aktivem a hrozbou není vazba (hrozba nemá vliv na aktivum), zůstává daná buňka prázdná. Posledním krokem analýzy je výpočet míry rizika. Poslouží k tomu vzorec R=T*A*V, kde R je míra rizika, T je pravděpodobnost vzniku hrozby, A je hodnota aktiva, a V je zranitelnost daného aktiva. Vypočtená míra rizika se doplní do matice rizik. Poslední krok analýzy je stanovení hranice pro nízká (přijatelná), střední a vysoká rizika.

Druhým přístupem analýzy rizik je analýza rizik vyhodnocující pravděpodobnost incidentu a jeho dopad. Tato metoda prezentuje poněkud odlišný přístup k určení míry rizika. Oproti předchozí metodě využívá pouze parametry dva (pravděpodobnost a dopad incidentu). Tato analýza rizik je více popisná. Nejprve se doplní identifikovaná aktiva a jejich hodnota. Dále je nutné k jednotlivým aktivům identifikovat hrozby, zranitelnosti a existující opatření. Odhadne se pravděpodobnost incidentu, že daná hrozba využije zranitelnosti a ohrozí tím dané aktivum. Pravděpodobnost incidentu je snižována existujícími opatřeními. Dopad, jako další parametr, lze zvolit shodně s hodnotou aktiva nebo nižší v případě, že incidentem dojde pouze k částečnému poškození aktiva. Míra rizika je následně vypočtena podle vztahu R = PI x D, kde PI je pravděpodobnost incidentu, D je dopad incidentu [2], [7], [8].

1.8 Bezpečnostní politiky informačního systému

Bezpečnostní politiku (BP) lze definovat jako soubor norem, požadavků a pravidel, které vymezují přístup organizace k zajištění bezpečnosti. Z hlediska časové posloupnosti Berka[2] navrhuje nejprve provést analýzu rizik a následně pak definovat BP, která bude eliminovat rizika. V opačném případě je nutné po dokončení analýzy provést zpětnou revizi politiky. Informační systém neexistuje izolovaně, ale je součástí organizace. Proto i politika IS vychází z celkové BP organizace:

Obchodní strategie organizace => Bezpečnostní politika organizace => Bezpečnostní politika IS.

Celková BP je základní dokument celkového zabezpečení organizace, který umožňuje koncepční a konzistentní budování bezpečnosti jak v oblasti IT, tak v ostatních oblastech. Tento dokument v obecné rovině popisuje základní požadavky organizace na zabezpečení a jeho cílem je ochrana veškerého hmotného i nehmotného majetku firmy, ochrana jejího dobrého jména a předmětu činnosti organizace. Obsah BP musí pokrývat veškeré aspekty zabezpečení ochrany organizace, počínaje ochranou budov přes definování jednotlivých skupin zaměstnanců, zálohování dat až po plány obnovy činnosti. Obsah BP schvaluje vedení organizace a její schválená podoba je závazná pro všechny zaměstnance organizace. Prostřednictvím smluv s třetími stranami se pak jednotlivé relevantní požadavky BP přenášejí i na smluvní partnery organizace a jejich zaměstnance. Z pohledu standardizace bezpečnostní politiky se je v současné době možné opřít o

standardy ISO, zejména ISO/IEC 17799:2005 IT: Code of Practice for Information Security Management a ISO/IEC 17799:200O IT: Code of Practice for Information Security Management. Tyto standardy pomáhají zejména při definici cílů a strategií BP, nejsou však plnohodnotným návodem na její vypracování.

Standardní postup při tvorbě a implementaci BP:

- předběžná studie,
- zadání,
- analýza rizik,
- bezpečnostní politika organizace,
- realizace BP,
- realizace a tvorba bezpečnostní dokumentace nižší úrovně,
- průběžná realizace osvěty – udržování bezpečnostního povědomí zaměstnanců.

Předběžná studie se nepovažuje za nezbytnou součást řešení, jde však o poměrně levnou záležitost, jež může celý projekt zkrátit a ve finále ušetřit finance. Účelem studie je získat základní orientaci o činnostech organizace a základní údaje o bezpečnostní situaci. Na podkladě těchto informací je možné stanovit přesněji rozsah budoucích nutných prací, rozvržení a náplň jednotlivých etap. V zadání stanoví organizace své požadavky na bezpečnost. Řešitel toto zadání koriguje ve smyslu zákonných předpisů a případně navrhuje doplnění opomenutých skutečností. Kvalitní bezpečnostní politiku lze sestavit pouze na základě provedené analýzy rizik (AR). AR by měla rovněž předcházet jakýmkoliv finančním investicím do bezpečnosti. Výstupem AR je ocenění hmotných a nehmotných aktiv organizace, včetně finančního ohodnocení v případě poškození, ztráty či nedostupnosti daného aktiva, seznam veškerých hrozeb, které byly ve vztahu k aktivům organizace identifikovaný, i s jejich ohodnocením a návrhem postupů na minimalizaci. Provedení AR předpokládá výběr vhodné metody a nástroje (základní, neformální, podrobná analýza, kombinovaný přístup) a případně příslušného nástroje (CRAMM, RiskPAC).

Struktura BP:

- Stanovení účelu BP, prohlášení o závaznosti BP pro pracovníky a deklarace plné podpory ze strany vedení organizace.
- Definice požadované úrovně bezpečnosti.
- Definice úrovní zabezpečení a míry odolnosti proti jednotlivým typům útoků.
- Definice bezpečnostního managementu organizace.
- Základní (obecné) bezpečnostní opatření v oblasti administrativní, personální, fyzické a systémové (oblast IT/ICT).
- Normy chování zaměstnanců organizace.
- Havarijní plány a postupy v obecné rovině.
- Deklarace souladu řešení bezpečnosti s relevantní legislativou a normami [2], [7], [8].

2 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost a ochrana informačních technologií je nezbytná vzhledem k existenci řady rizikových jevů, jako jsou kriminální chování jednotlivců či organizovaných skupin, nekalé obchodní praktiky, terorismus, porušení pracovně-právních předpisů, rizikové chování osob neznalých, požáry a živelné pohromy. Každý z uvedených jevů lze kvantifikovat procentem pravděpodobnosti, která úzce souvisí na lokalitě firmy, předmětu podnikání, medializaci a personální struktuře.

Pro účinnou a efektivní implementaci prvků fyzické bezpečnosti ochrany IT využíváme tří základních postupů a opatření:

- organizační (režimová) opatření,
- fyzická ochrana (ostraha),
- technické a mechanické prostředky.

Režimová opatření stanovují:

- oprávnění osob a dopravních prostředků pro vstup a vjezd (výstup/ výjezd) do/z objektu,
- oprávnění osob pro vstup do zabezpečené oblasti a jednací oblasti,
- způsob kontroly těchto oprávnění,
- způsob manipulace s klíči a identifikačními prostředky,
- způsob manipulace s technickými prostředky a jejich používání,
- podmínky a způsob kontroly pohybu osob v objektu, zabezpečené oblasti a jednací oblasti,
- způsob kontroly a vynášení utajovaných informací z objektu, zabezpečené oblasti a jednací oblasti.

Ostraha se nepřetržitě zajišťuje u objektu, ve kterém se nachází zabezpečená oblast kategorie:

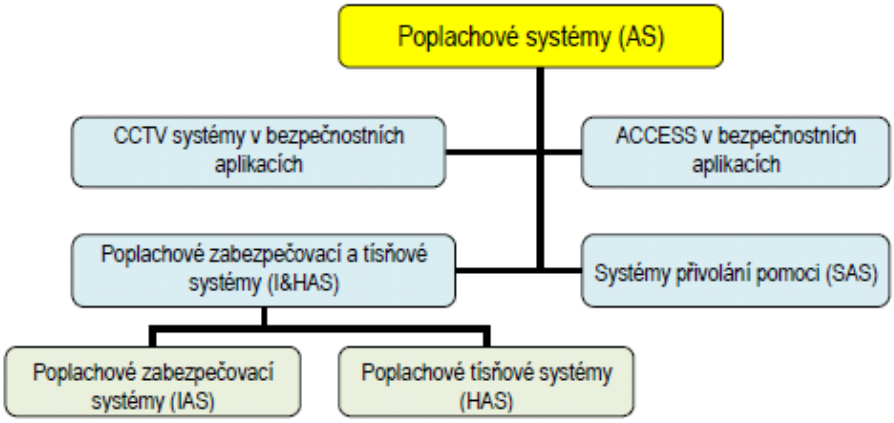
- přísně tajné, nejméně 2 osobami u objektu,

- tajné, nejméně 1 osobou u objektu a 1 další osobou, které poplachové hlášení technických prostředků umožní rychlý zásah,
- důvěrné, nejméně 1 osobou, které poplachové hlášení technických prostředků umožní rychlý zásah.

Uvedené základní informace o zajištění ostrahy a režimových opatření představují důležité východisko pro zpracování návrhu poplachového zabezpečovacího a tísňového systému - pro výběr vhodných komponent systému, jejich umístění, konfiguraci systému a způsob jeho ovládání.

Technické prostředky:

- poplachový zabezpečovací systém (PZS),
- systémy přivolání pomoci (SAS),
- kamerové systémy (CCTV),
- systém kontroly vstupu (ACS),
- elektrická požární signalizace (EPS),
- samočinné hasící zařízení (SHZ),
- komunikační systémy,
- mechanické zábranné systémy (MZS),
- speciální systémy – rentgeny, detektory kovů, výbušnin a drog.



Obr. 3. Klasifikace poplachových systémů [4].

Projektová dokumentace je nezbytnou součástí implementace fyzické bezpečnosti. Popisuje technický objekt v jeho rozsahu, způsobu provedení, návaznosti na okolí a vnější vlivy, požadavky na realizaci a požadavky zadavatele. Cílem projektové dokumentace je prezentace jednoznačného a přesného vyjádření všech navržených komponent a prvků systému, jejich lokaci, vzájemné vazby a vlivů na okolí, jako podklad pro realizaci díla.

Tab. 3. Klasifikace projektové dokumentace [4].

Zkratka	Název	Legislativa
NSS	Návrh skladby systému	ČSN CLC/TS 50131-7
DUR	Dokumentace pro územní rozhodnutí	Vyhláška č. 503/2006 Sb., TNI 33 4591-1
DOS	Dokumentace pro ohlášení stavby	Vyhláška č. 499/2006 Sb., TNI 33 4591-1
DSP	Dokumentace pro stavební povolení	Vyhláška č. 499/2006 Sb., TNI 33 4591-1
DPS	Dokumentace pro provádění stavby	Vyhláška č. 499/2006 Sb., TNI 33 4591-1, Vyhláška 230/2012 Sb.
ZD	Zadávací dokumentace	Zákon č. 137/2006 Sb.
DVD	Dokumentace pro výběr dodavatele	TNI 33 4591-1
RDS	Realizační dokumentace stavby	ČSN CLC/TS 50131-7
DKV	Dílenská a konstrukční dokumentace	Pozn. rozšiřuje realizační dokumentaci
DSPS	Dokumentace skutečného provedení stavby	Vyhláška č. 499/2006 Sb.

Studie je dokumentace zpracovávaná v rámci předprojektové přípravy, řešící prověření konkrétního místa realizace, vnějších vlivů, limitů území, legislativních omezení,

dostupných zdrojů a dalších faktorů ovlivňují navrhované dílo. Cílem studie je navrhnout možná řešení, technickou proveditelnost, základní problémy, vytyčit rozsah prací a typy a rozsah profesí včetně vzájemné koordinace a rovněž stanovit předběžné náklady. Z hlediska informačních systému se jedná zejména o mechanické a technické vybavení – zařízení objektu, nároky na připojení k silovým a elektronickým komunikacím veřejných sítí, dopravní dostupnost apod. Kromě uvedených norem řady ISO 27000 je nutné při realizaci postupovat v souladu s legislativou, kterou řeší např. stavební zákon č. 50/1978Sb. Dále dodržovat aktuálně platné technické normy, zejména ČSN EN 50131-1:2007 a ČSN CLC/TS 50131-7:2011 [2], [4].

2.1 Poplachový zabezpečovací systém

Požadavky na systémy PZS definuje norma ČSN EN 50131–1, metodické pokyny České asociace pojišťoven a požadavky Národního bezpečnostního úřadu. Norma ČSN EN 50131–1 rozděluje systémy PZS do 4 stupňů dle rizika:

- stupeň zabezpečení 1 pro nízké riziko (byty, chaty),
- stupeň zabezpečení 2 pro nízké až střední riziko (obchody, sklady, kanceláře),
- stupeň zabezpečení 3 pro střední až vysoké riziko (peněžní ústavy, galerie, státní úřady),
- stupeň zabezpečení 4 pro vysoké riziko (trezory a peněžní provozy bank).

Systém PZS určitého stupně musí být složen z prvků certifikovaných pro tento stupeň anebo vyšší a konfigurace prvků musí splňovat požadavky pro tento stupeň. Potvrzení je dáno ve formě atestu na formuláři České asociace pojišťoven. S ohledem na klasifikaci prostředí instalace se stanovují třídy prostředí:

I. vnitřní, ale omezené na prostředí kanceláří a bytů,

II. vnitřní všeobecné (např. obchody, restaurace, sklady, schodiště, výrobní a montážní prostory),

III. venkovní (vnější), které jsou však chráněny proti přímému dešti a slunci, nebo vnitřní prostory s extrémními podmínkami prostředí (stodoly, půdy, garáže),

IV. venkovní (vnější) všeobecné.

Tab. 4. Přehled ČSN v oblasti poplachových zabezpečovacích a tísňových systém [4].

Číslo normy	Název normy
ČSN EN 50 131-1 ed.2	Poplachové systémy - PZTS - Část 1: Systémové požadavky
ČSN EN 50 131-2-2	Poplachové systémy - PZTS - Část 2-2: Detektory narušení - Pasivní infračervené detektory
ČSN EN 50 131-2-3	Poplachové systémy - PZTS - Část 2-3: Požadavky na mikrovlnné detektory
ČSN EN 50 131-2-4	Poplachové systémy - PZTS - Část 2-4: Požadavky na kombinované pasivní infračervené a mikrovlnné detektory
ČSN EN 50 131-2-5	Poplachové systémy - PZTS - Část 2-5: Požadavky na kombinované pasivní infračervené a ultrazvukové detektory
ČSN EN 50 131-2-6	Poplachové systémy - PZTS - Část 2-6: Detektory otevření (magnetické kontakty)
ČSN EN 50 131-2-7-1	Poplachové systémy - PZTS - Část 2-7-1: Detektory narušení - Detektory rozbíjení skla (akustické)
ČSN EN 50 131-2-7-2	Poplachové systémy - PZTS - Část 2-7-2: Detektory narušení - Detektory rozbíjení skla (pasivní)
ČSN EN 50 131-2-7-3	Poplachové systémy - PZTS - Část 2-7-3: Detektory narušení - Detektory rozbíjení skla (aktivní)
ČSN EN 50 131-3	Poplachové systémy - PZTS - Část 3: Ústředny
ČSN EN 50 131-4	Poplachové systémy - PZTS - Část 4: Výstražná zařízení
ČSN EN 50 131-5	Poplachové systémy - PZTS - Část 5-3: Požadavky na zařízení využívající bezdrátové propojení
ČSN EN 50 131-6 ed. 2	Poplachové systémy - PZTS - Část 6: Napájecí zdroje
ČSN EN 50 131-7	Poplachové systémy - PZTS - Část 7: Pokyny pro aplikace
ČSN EN 50 131-8	Poplachové systémy - PZTS - Část 8: Zamlžovací bezpečnostní zařízení/systémy

Souvislost mezi stupněm zabezpečení a odolnosti vůči znalostem a vybavení narušitelů:

- Stupeň 1: Předpokládá se, že narušitelé mají malou znalost PZTS a mají k dispozici omezený sortiment snadno dostupných nástrojů.
- Stupeň 2: Předpokládá se, že narušitelé mají omezené znalosti PZTS a používají základní sortiment běžného nářadí a přenosných přístrojů.
- Stupeň 3: Předpokládá se, narušitelé jsou obeznámeni s PZTS a mají rozsáhlý sortiment nástrojů a přenosných elektronických zařízení.
- Stupeň 4: Používá se tehdy, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že narušitelé nebo lupiči jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů PZTS.

Umísťování komponent souvisí s technickým posouzením jednotlivých komponent v daném prostoru. Je nutné respektovat doporučení k montáži dané výrobcem, vlivy prostředí (elektromagnetické rušení, tepelné zdroje, průvan, zvuky a ruchy), požadavky na zabezpečení pro umístění ústředny PZTS.

Návrh PZTS předpokládá zajištění ochrany v následujících oblastech:

- Obvodová/perimetrická ochrana – je nutné provést ochranu hranic pozemku objektu.
- Plášťová ochrana – ochrana pláště objektu, dveří, oken, stěn, průchodů inženýrských sítí do objektu.
- Prostorová/volumetrická ochrana – ochrana prostoru uvnitř objektu – serveroven, chodeb, skladů, kanceláří.
- Předmětová ochrana – zaměřená na určitý předmět (trezor, rozvaděč apod.).
- Osobní ochrana – umožňuje pracovníkovi v případě tísně přivolat pomoc [2], [4].

2.2 Elektrická požární signalizace

EPS slouží k monitorování prostředí s ohledem na rychlou a včasnou detekci požáru, k zajištění možnosti vyvolání požárního poplachu a zajištění technologických procesů k minimalizaci dopadů vzniklého požáru. Požadavky na systémy EPS jsou definovány ve vyhlášce MV č. 241/2001 Sb. *„o stanovení podmínek požární bezpečnosti a výkonu*

státního požárního dozoru“, v ČSN 342710 *„Předpisy pro zařízení EPS“*, ČSN 730875 *„Navrhování EPS“*, ČSN EN 54, ve vyhlášce č. 23/2008 *„o technických podmínkách požární ochrany staveb“*.

Při návrhu systému EPS je nutné respektovat Projekt požární ochrany objektu. Projektování provádí osoba způsobilá, která získala oprávnění k projektové činnosti podle zákona č. 360/1992 Sb. „o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě“, ve znění zákona č. 164/1993 Sb., zákona č. 275/1994 Sb. a zákona č. 276/1994 Sb.

Systém EPS je tvořen následujícími komponentami, které definuje vyhláška č. 50/78 Sb. z pohledu elektrotechnické způsobilosti:

- EN 54-2 Ústředna,
- EN 54-3 Sirény,
- EN 54-4 Napájecí zdroj,
- EN 54-5 Hlásiče teplot,
- EN 54-7 Hlásiče kouře,
- EN 54-10 Hlásiče plamene,
- EN 54-11 Hlásiče tlačítkové,
- EN 54-12 Hlásiče lineární,
- EN 54-13 Systémové požadavky,
- TS 54-14 Aplikační návody,
- EN 54-15 Hlásiče multisenzorové,
- EN 54-16 Ústředny pro hlasové zdroje zvuku,
- EN 54-17 Izolátory,
- EN 54-18 Vstupně výstupní zařízení,
- EN 54-20 Nasávací hlásiče,
- EN 54-21 Přenosová zařízení,
- EN 54-22 Lineární tepelné hlásiče,

- EN 54-23 Optická poplachová zařízení,
- EN 54-24 Reproduktory pro hlasové zdroje zvuku,
- EN 54-25 Komponenty využívající radiové linky,
- EN 14604 Autonomní hlásiče [2], [4].

2.3 Samočinné hasící zařízení

SHZ se využívá v prostorách, kde je potřeba zajistit rychlou reakci na vzniklý požár. Jsou to pevně zabudovaná hasicí zařízení ve stavbě nebo v technologickém zařízení. Podle ISO ČSN 8421–4 sestávají z vypočítané zásoby hasiva, přiváděného na stabilní hubici, kterou je hasivo dodáváno k hašení požáru s možností ručního nebo samočinného spouštění. Zásoba hasiva je u vodních a pěnových SHZ v zásobní nádrži nebo v tlakové nádobě, u plynových a práškových SHZ v tlakových láhvích nebo tlakových zásobnících. Součástí SHZ jsou řídící a kontrolní armatury, poplachová zařízení a potrubní rozvody s otevřenými nebo uzavřenými výstřikovými koncovkami.

Podle charakteru ohrožení a velikosti prostorů se volí i typ samočinného zařízení:

- Vodní SHZ (sprinklery) – spouští se teplotní pojistkou v trysce. Jsou vhodné pro velké prostory s velkou koncentrací osob. Z principu hašení nejsou vhodné pro místnosti s vyšší koncentrací hodnot (serverovny, archívy, knihovny).
- Plynové SHZ (FM200, Inergen) – neničí hodnoty, vhodné pro uzavřené a utěsněné prostory s možností odvětrání. Je nutné uvažovat i prostory nad podhledy a pod zvýšenou podlahou.

SHZ se dělí podle způsobu ovládání na ruční, samočinné – vždy s možností ručního spuštění, kombinované. Aby se snížilo riziko planého poplachu, používá se detekce požáru na dvou stupních, přičemž každý stupeň představuje využití automatických hlásičů na jiných fyzikálních principech. Lze kombinovat i systém automatický s ručním. Pokud je detekován požár pomocí prvního principu, je vyhlášen poplach prvního stupně a systém informuje pomocí sirén a stroboskopu o vyhlášeném poplachu. Při detekci podle druhého principu je systém aktivován. Je nutné zajistit plynovou těsnost prostoru, vypnutí vzduchotechniky a uzavření dveří [2], [20].

2.4 Kamerové systémy

Uzavřený kamerový systém (CCTV – Circuit Closed Television) slouží k monitorování bezpečnostní situace vně i uvnitř objektu a sledování provozu objektu. Obrazové informace se zaznamenávají a po určitou dobu archivují. Požadavky na kamerové systémy jsou stanoveny v normě ČSN EN 50132. Prostory podléhající zákonu č. 148/1998 Sb. *„o ochraně utajovaných skutečností“* musí splňovat požadavky metodiky NBÚ. Spolehlivost a jakost zařízení popisuje norma ČSN IEC 50 (191).

Tab. 5. Přehled ČSN v oblasti CCTV [4].

Číslo normy	Název normy
ČSN EN 50132-1	CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky
ČSN EN 50132-5-1	CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 5-1: Video přenosy - obecné provozní požadavky
ČSN EN 50132-5-2	CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 5-2: IP video přenosové protokoly
ČSN EN 50132-5-5	CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 5: Přenos videosignálu
ČSN EN 50132-5-7	CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikaci

Norma ČSN EN 50132 se vztahuje na následující zařízení:

- černobílé kamery,
- barevné kamery,
- objektivy,
- příslušenství,
- místní a hlavní řídící jednotky,
- černobílé monitory,
- barevné monitory,

- záznamová zařízení,
- zařízení pro okamžitý výtisk obrazu,
- videodetektory pohybu.

Prostory, které jsou střeženy CCTV, musí být označeny informačními tabulemi. S ohledem na bezpečnostní požadavky se instalace kamer v objektech předpokládá:

- na plášti objektu s důrazem na vstupy do objektu, kolektorové trasy a kabelové kanály,
- na perimetru pozemku,
- na klíčových místech uvnitř objektu – hlavní chodby, průchody, nouzové východy,
- přehledové kamery na bezpečnostně a technologicky významných místech v objektu – serverovny,
- detailní kamery na bezpečnostně a technologicky významných místech nebo přímo zařízeních.

Detekce pohybu je vlastnost kamerového systému, která vyvolá poplachový stav při detekci pohybu ve videosignálu. Kvalitní systémy provádí vektorové vyhodnocení detekce pohybu a umožňují masking (vyjmutí definovaných ploch) [2], [4].

2.5 Bezpečnostní systémy kontroly vstupu

Systémy kontroly vstupů zahrnují konstrukční a organizační náležitosti společně se zařízením k ovládání vstupů. Principem činnosti elektronické kontroly vstupu (ACS – Access Control System) je identifikace žadatele o vstup pomocí identifikačního média. Identifikace může probíhat na různých fyzikálních přenosech. Většinou se jedná o přenosech identifikačního čísla z média do systému. Protože nelze zcela vyloučit technickou možnost klonování některých médií, je vhodné doplnit identifikaci o prvek, který není svázán s médiem – např. zadání osobního identifikačního čísla (PIN) nebo biometrická kontrola držitele.

Systém ACS se skládá z následujících komponent:

- snímače identifikačního média,
- vyhodnocovací (řídící) jednotky,

- programovací zařízení nebo počítačová nadstavba u rozsáhlejších systémů.

Hlavním významem systémů kontroly vstupů je:

- rozhodovat o povolení vstupu (kdo má poskytnutý vstup),
- rozhodovat o místě vstupu,
- rozhodovat o časovém omezení vstupu,
- redukovat riziko nepovoleného vstupu.

Požadavky na další systémové funkce systému ACS:

- řízení interlocku – další dveře lze otevřít, poté co předchozí byly uzavřeny,
- antipassback – do prostoru je možné znovu vstoupit až po jeho opuštění,
- klíčová karta – prostor lze klíčovou kartou uzamknout, poté do tohoto prostoru nemají další oprávnění přístup do opětovného odemknutí,
- čtyři oči – pro vstup se musí v oprávněném čase identifikovat dvě oprávněné osoby,
- guardtour – sledování obchůzkové činnosti bezpečnostní služby,
- evidence návštěv,
- řízení evakuace – systém informuje, kdo zůstal v objektu,
- kontrola obsazení oblasti,
- návaznost na ostatní bezpečnostní a personální technologie,
- příkazová karta – použití karty zajistí ovládání dalších zařízení (osvětlení, PZS),
- vazba na další technologie – ovládání kamerového systému, klimatizace, větrání, PZS,
- uživatelský komfort a podpora grafiky a map.

Systém kontroly vstupu by měl vždy zajišťovat únik z objektu v případě nouze. Pro tyto případy je nutné zajistit instalaci panikových tlačítek nebo panikových kování pro nouzové otevření dveří. Nouzové otevření dveří může být i přímá funkce EPS.

Požadavky na ACS systémy jsou stanoveny v normě ČSN EN 50133. Prostory podléhající zákonu č. 148/1998 Sb. *„o ochraně utajovaných skutečností“* musí splňovat požadavky metodiky NBÚ.

Tab. 6. Přehled ČSN v oblasti systémů kontroly vstupu [4].

Číslo normy	Název normy
ČSN EN 50133-1	Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky
ČSN EN 50132-2-1	Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty
ČSN EN 50132-7	Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace

Norma ČSN EN 50132-7 řeší především vstup a pohyb osob, nicméně je aplikovatelná např. na vjezdy a pohyb vozidel. Pokyny zahrnují široký rozsah systémů vzhledem k počtu přístupových bodů. Norma je doplněna o části dokumentace (projektová, revizní a dokumentace pro údržbu).

Prováděcí projektová dokumentace musí stanovit:

- zabezpečený a kontrolovaný prostor,
- umístění identifikačních zařízení,
- klasifikace přístupových míst,
- umístění ovládacích zařízení,
- propojení využívané mezi komponentami systému – detaily, kabelové trasy,
- schémata, dokumentace ke komponentům.

Interkom je dorozumívací zařízení. Podle provozních a bezpečnostních potřeb používáme audiointerkomy nebo videointerkomy. Instalace interkomů je vhodná u průchodů, které jsou kontrolovány systémem ACS. Pomocí interkomů se může na ostrahu dovolat osoba bez oprávnění k vstupu nebo osoba, která zapomněla své identifikační médium nebo má jiný technický problém, a sdělit ostraze své potřeby [2], [4].

2.6 Mechanické zábranné systémy

Základní dělení MZS:

- MZS obvodové ochrany,
- MZS plášťové ochrany,
- MZS předmětové ochrany.

Mezi MZS obvodové ochrany patří:

- klasické drátěné oplocení,
- bezpečnostní oplocení,
- vrcholové zábrany,
- podhrabové překážky,
- vstupy a vjezdy – turnikety, brány, závory, výsuvné tyče a jiné zábranné prostředky pro průjezd vozidel.

Za MZS plášťové ochrany považujeme:

- stavební prvky budov – stavební konstrukce,
- otvorové výplně – dveře, okna a odolná skla, průlezné otvory, mříže, bezpečnostní fólie.

MZS předmětové ochrany jsou komorové trezory nebo úschovné objekty, trezorové skříně. Prvky MZS plášťové ochrany posuzujeme podle stupně mechanické, balistické nebo požární odolnosti. Příslušnou odolnost definují normy ČSN EN 1522, 1063, 1627 a 1303 [4].

2.7 Detekce zakázaných látek a předmětů

Detekce zbraní a výbušnin se provádí především pomocí detektorů kovových předmětů nebo rentgenů. Detektory kovových předmětů – průchozí rámy nebo ruční detektory – se používají pro kontrolu vstupujících osob. Rentgenové detektory se používají pro kontrolu zavazadel, příchozí pošty a balíků, beden, s cílem odhalit neschválené kovové předměty, výbušniny, hořlaviny [2].

2.8 Biometrie

Biometrické systémy využívají biometrických technologií, které umožňují automatickou identifikaci nebo verifikaci určité fyzické osoby. Biometrické technologie pracují s biometrickými prvky, které jsou:

- univerzální – existují u všech osob,
- jedinečné – musí každou osobu odlišovat,
- stálé – každá fyzická osoba si v průběhu času prvek trvale uchovává.

Biometrické postupy používají stabilní nebo dynamická data nebo charakteristiky chování.

Nejčastěji používané biometrické prvky jsou:

- otisk prstů,
- tvar ruky,
- obličej,
- hlas,
- podpis,
- obraz sítnice,
- obraz duhovky.

Biometrické prvky lze použít pro nejvyšší stupeň zabezpečení. Mezi jejich základní vlastnosti patří neoklamatelnost, zřejmost a spolehlivost, nulové provozní náklady na média, rychlost skenování, praktičnost, efektivnost a příznivá cena ve vztahu k bezpečnosti. Biometrické systémy používají převážně kombinaci znaků pro zvýšení bezpečnosti.

Biometrické údaje získané z biometrických senzorů představují informaci, která je považována za citlivý údaj ve smyslu směrnice 95/46/ES čl. 8, proto je nutné tyto údaje zpracovávat jako údaje citlivé. Dále je nutné respektovat zákon č. 101/2000 Sb. „o ochraně osobních údajů“ – z toho vyplývá povinnost zpracovávat údaje pouze pro dané účely a uchovávat data pouze po nezbytně nutnou dobu.

Proces ověření identity probíhá porovnáním skenované charakteristiky s biometrickým etalonem, což je referenční vzorek. Bývá sejmuto více vzorků najednou (obvykle tři),

z nichž je vytvořen reprezentativní vzorek jejich zprůměrováním. Vzorku je následně přiřazen identifikátor ve formě PIN nebo číslo karty. Ukládání etalonů je možné buď přímo v čtecím zařízení, v přenosných tokenech (čipová karta), v centrální databázi nebo v kombinaci předcházejících způsobů. Pro IT systémy je vhodná kombinace centrální databáze a čtecích zařízení s vnitřní pamětí, čímž se dosáhne funkčnosti systému za všech okolností. V opačném případě je nutné mít záložní řešení pro případ výpadku. Charakteristickými výkonnostními mírami jsou koeficient nesprávného přijetí, zápisu etalonu a doba ověření [2], [5], [11].

2.9 Kategorie datového centra a výpočet SLA

Kategorie datového centra je stanovena normou TIA-942. Ta definuje čtyři kategorie podle dostupnosti stanoveného parametrem A:

- Tier I level
  - jednookruhové WAN připojení (bez zálohy),
  - jednoduchá LAN infrastruktura a DC technologie,
  - dostupnost A 99,671% (maximální doba výpadku < 29 hodin/rok).
- Tier II level
  - dvouokruhové WAN připojení (se záložním připojením),
  - failover LAN infrastruktura a DC technologie,
  - dostupnost A 99,741% (maximální doba výpadku < 23 hodin/rok).
- Tier III level
  - redundantní napájení provozovaných zařízení,
  - redundantní LAN infrastruktura a DC technologie,
  - možnost údržby systémů bez omezení / přerušení provozu,
  - dostupnost A 99,982% (maximální doba výpadku < 90 minut/rok).
- Tier IV level
  - redundantní napájení provozovaných zařízení,

  - fault tolerant infrastruktura,
  - možnost údržby systémů bez omezení / přerušení provozu,
  - dostupnost A 99,995% (maximální doba výpadku < 45 minut/rok).

- Spolehlivost R(t) v čase t je pravděpodobnost, že komponent neselže během časového úseku 0 – t.
- Dostupnost A(t) v čase t je pravděpodobnost, že komponent je v normálním provozu v čase t.
- A(t) > R(t) – pro opravitelné systémy.
- A(t) = R(t) – pro neopravitelné systémy.
- Mean Time Between Failures (MTBF) – střední doba mezi poruchami, MTBF = doba provozu / počet poruch.
- Mean Time To Failure (MTTF) – střední doba do poruchy – pro neopravitelné části MTTF = doba provozu / počet vadných částí.
- Mean Time To Repair (MTTR) – střední doba do opravy
- Dostupnost A = MTBF / (MTBF + MTTR).
- Service Level Agreement (SLA) – oboustranně odsouhlasená dohoda mezi poskytovatelem a odběratelem služeb o úrovni poskytovaných služeb
- Service Level Management (SLM) – proces definice, dojednávání, dokumentace, schvalování a hodnocení úrovně poskytovaných služeb
- Dostupnost sériových soustav As, např. As = 0.9x0.8x0.999x0.99999 = 0.5754.
- Dostupnost paralelních soustav Ap., např. 1-(0.5 x 0.2 x 0.1 x 0.2 x 0.01) = 0.99998.
- Použité vzorce: $As = 1 - \prod_{i=1}^{n} [1 - Ai]$; $As = \prod_{i=1}^{n} Ai$ [5], [13].

3 PREVENCE A DETEKCE POČÍTAČOVÉHO ÚTOKU

Systém detekce narušení (IDS – Intrusion detection system) je definován jako soubor nástrojů, metod a zdrojů, které pomáhají identifikovat, zpřístupnit a hlásit neautorizované a neschválené síťové aktivity. IDS detekuje takové aktivity v provozu, které mohou nebo nemusí být narušeními. Detekce narušení je jednou částí celkového ochranného systému. Mezi další systémy patří firewall, jehož cílem je povolit jen definovaný provoz a zabránit všem ostatním průnikům. Systémy IDS lze umístit před firewall nebo za něj a následně porovnat zaznamenané informace. IDS a IPS provádějí inspekci stavů TCP provozu pomocí tabulek, do kterých zadávají data týkající se ustanovených relací.

IDS spadá do třech kategorií:

- HIDS (Host based IDS) jsou uzlově orientované systémy detekce narušení. Jedná se o software, který je umístěn na uzlovém systému a může skenovat aktivitu všech uzlových zdrojů, aktivity systémového a událostního logu a tyto události porovnává se záznamy závadných událostí obsažených ve znalostní databázi.
- NIDS (Network based IDS) jsou síťově orientované systémy detekce narušení. NIDS se zařazují do sítě sériově a analyzují síťové pakety, z čehož se pak usuzuje, zda se jedná o napadení. Přijímají všechny pakety ve zvláštním segmentu sítě, tak aby bylo možné přijímat pakety i z přepínaných sítí, kde to není implicitně možné. Analyzují datové toky na přítomnost vzorů závadného chování.
- Hybridní systémy jsou kombinace HIDS a NIDS. Monitorují události odehrávající se na uzlovém systému a porovnávají je s NIDS, který monitoruje síťový provoz.

Základním režimem IDS je, že systémy NIDS nebo HIDS pasivně sbírají data, předzpracovávají a klasifikují je a porovnávají je se znalostní databází. Je-li nalezena shoda, generuje se výstraha.

Systém prevence proti narušení (IPS – Intrusion prevention system) v případě výskytu události přijme aktivní opatření podle předepsaných pravidel. Systém IPS je aktivní systém a společně s IDS vytváří kompaktní řešení zabezpečení sítě. IPS mohou být uzlově nebo síťově orientované. Znalostní databáze obsahují předdefinované uživatelské činnosti. Jestliže nějaká činnost není v akceptačním seznamu, IPS ji zabrání ji uskutečnit. Další metody IPS porovnávají kontrolní součty souborů s dobře známými kontrolními součty v

seznamech ještě před tím, než je povoleno tyto soubory spustit. Typický systém IPS se skládá ze čtyř částí:

- normalizátor provozu – přerušuje síťový provoz, provádí analýzu, složení paketů a plní základní blokovací funkce,
- monitor služeb – vytváří referenční tabulku a klasifikuje informaci. Pak dochází k tvarování provozu,
- detekční jednotka – porovnává signálové vzory s referenční tabulkou a stanovuje příslušnou odpověď,
- provozní tvarovací část (tvarovač) – řídí tok informací.

IDS a IPS poskytují systémovému administrátorovi nástroj pro řízení a příležitost kvantifikovat útoky proti síti organizace. IDS a IPS jsou stěžejní částí silných hloubkově ochranných bezpečnostních programů. Organizace jsou proaktivní v očekávání a reakci na možná narušení. Obě technologie pomáhají zabezpečovat ochranu sítě a aplikační vrstvy, pomáhají korelovat a ohodnocovat platnost informací z ostatních programů jako antiviry, firewally a směrovače [1], [3], [11], [12].

3.1 Architektura systému IDS

Architektura je jedním z nejkritičtějších aspektů v detekci a prevenci pro narušení. Každá komponenta musí provádět svoji roli efektivním a koordinovaným způsobem, vyplývajícím z účelného zpracování informací, výstupu a také příslušné preventivní odezvy. Nevhodně navržená nebo implementovaná architektura přináší nežádoucí důsledky – zpomalení sítě, chybějící příslušné či časové odezvy, chybějící data pro zpracování.

Jednovrstevná architektura je nejzákladnější architektura, v níž komponenty sbírají a zpracovávají data zcela samostatně, aniž by je předávaly jako svůj výstup ke zpracování jiným skupinám komponent.

Vícevrstevná architektura zahrnuje komponenty, které si mezi sebou předávají informace.

IDS obsahuje tři primární komponenty:

- senzory,

- analyzátory/agenty,
- manažera.

Senzor provádí sběr dat a předává je agentům, kteří se specializují na analýzu právě jedné funkce. Agent předává informaci o útoku na komponentu manažera, která provede definovanou akci. Vícevrstevné architektury mají vyšší účinnost, komponenty jsou na sobě stavově nezávislé a výpadek jedné nezpůsobí výpadek celého systému.

Architektura peer to peer se liší od vícevrstevné architektury rovnocenným postavením komponent, z nichž každá provádí tentýž druh činnosti a předává informace peer zařízením. Používá se převážně pro síť vzájemně propojených firewallů [1].

3.2 Senzory

Senzory jako kritické prvky architektury IDS a IPS jsou komponentami nejnižší úrovně. Dělí se na dva typy:

- senzory založené na síti,
- senzory založené na uzlu.

V první variantě se senzory používají častěji. Jsou to programy nebo síťová zařízení, která zachytávají data v paketech procházejících lokální sítí. V architektuře záleží na umístění a množství senzorů. Obvykle se používají na významných síťových trasách jako vstupní body WAN (wide area network), v demilitarizované zóně nebo na páteřních trasách.

Programy Tcpdump nebo libpcap velmi efektivně slouží jako senzory. Program zachytává data z paketů a porovnává jejich hlavičky s filtry detekce a prevence. Analyzují data a vyhledávají útočné signatury podobné hackerským signaturám. Záchyt primárních paketů probíhá buď ve smíšeném režimu, kdy síťová karta přijme každý paket, nebo v nesmíšeném režimu, kdy jsou pakety vázány na její MAC adresu a ostatní pakety jsou ignorovány. Nesmíšený režim se uplatňuje v uzlové architektuře.

Senzory vně externích firewallů zaznamenávají informace o internetových útocích na webové, FTP, vnější DNS a poštovní servery.

Senzory založené na uzlu zachytávají data z více sítí, které jsou připojeny právě do tohoto uzlu. Nevýhodou jsou vysoké systémové požadavky na bitovou propustnost senzorů při zpracování dat. Řešením je instalace filtrů, které omezí typ paketů [1].

3.3 Agenti

Agent je skupina procesů, které běží nezávisle a jež jsou naprogramovány k analýze systémového chování a síťových událostí za účelem detekce anomálních událostí. Minimem pro implementaci agenta je začlenění tří funkcí nebo komponent:

- komunikační rozhraní pro komunikaci s ostatními komponentami IPS a IDS,
- odposlouchávač, který na pozadí přijímá data ze senzorů a zpráv z ostatních agentů,
- zasílatel, který data předává komponentě manažera.

Použití agentů v detekci a prevenci proti narušení se ukázalo být největším technickým průlomem. Výhody jsou následující:

- adaptibilita,
- účinnost daná jednoduchostí funkce místo složité implementace více funkcí,
- pružnost,
- nezávislost,
- škálovatelnost,
- mobilita.

V detekci založené na uzlu se agenti umísťují tak, aby každý agent monitoroval právě jeden uzel. V detekci založené na síti se agenti umísťují do pozic, kde jsou nejúčinnější a zároveň nejbezpečnější [1].

3.4 Manažer

Manažer plní funkce správy dat a jejich archivace, generuje výstrahy a rozesílá je definovaným způsobem. Významnou funkcí je korelace událostí za účelem stanovení, zda mají společný zdroj. Řídí a monitoruje ostatní komponenty IDS a IPS. Generuje a distribuuje strategie, což jsou konfigurace pro další komponenty, které následně upraví svůj provoz či chování. Vysoké požadavky jsou kladeny na dostupnost manažera a jeho redundanci, tedy na HW a SW spolehlivost a v neposlední řadě bezpečnost zabraňující kompromitaci systému. Redundanci lze řešit formou clusteru nebo záložního serveru [1].

4 POŽADAVKY NA NÁVRH BEZPEČNÉ POČÍTAČOVÉ SÍTĚ

V návrhu síťové bezpečnosti je nutné dodržovat následující doporučení:

- rozdělit síť na segmenty a podsítě – vytvořit fyzickou izolaci na úrovni IP adres,
- používat firewally mezi segmenty sítě,
- vhodně využívat směrování a přepínání, překlad adres NAT,
- instalovat systémy IDS, IPS,
- instalovat antivirové a anti-spyware skenery, skenery zranitelností,
- zavést zásady zálohování,
- aktualizovat software a implementovat záplaty,
- šifrovat datové přenosy přes veřejné sítě,
- zmenšit útočný povrch (attack surface) systémů – minimalizovat zranitelnosti,
- vyvarovat se přímého a nekontrolovatelného přístupu k internetu a segmentů sítě,
- omezit mobilní systémy a přenosná média – připojovat do karantény, nepřipojovat USB média,
- zajistit fyzickou bezpečnost,
- zajistit autentizaci [5], [6], [10], [12].

4.1 Směrovače, přepínače a mosty

Protokol STP (Spanning tree protocol) specifikován ve standardu IEEE 802.1D řeší problém síťových smyček prostřednictvím adaptivního a dynamického směrování. STP je ústřední prvek přepínaných sítí a zavádí trasy ve formě virtuálních okruhů. Jako body připojení se používají přepínače, které jsou konfigurovány do režimu mostů a účastní se detekce smyček. STP pracuje na linkové vrstvě OSI modelu. V hiearchicky vybudované sítí je kořenový uzel propojen s ostatními uzly a vytváří stromovou topologii. Čistě stromová topologie má za následek, že výpadek uzlu nebo spojení znamená nedostupnost uzlů na nižší hierarchii. Řešením je přidání nových spojení mezi větvemi stromu do kříže. Křížová spojení však zavádějí do sítě také možnost vytvoření smyček. Správným řešením

v síti je vytvoření takové topologické kostry, že neexistují žádné smyčky, ale přitom je v systému k dispozici dostatek redundantních spojení pro případ, že nějaká linka vypadne.

Pro výpočet nejkratší trasy mezi uzly jsou definovány parametry priorita uzlu a identifikátor uzlu (podle mac adresy). STP považuje uzel s nižší prioritou a nižší mac adresou za více preferovaný. V směrovačích a přepínačích Cisco je výchozí hodnota priority nastavena na 32768. Kořenový uzel stromu by měl mít prioritu nižší na 10.

Algoritmus STP kalkuluje trasu sítí tak, aby cena trasy byla co nejnižší. Cena trasy je dána součtem cen (priorit) všech segmentů, které se na trase vyskytují. Každý most v síti má konfigurovatelnou prioritu. Algoritmus STP stanovuje následující porty, které nejsou blokovány:

- Kořenový port (root port) je port přepínače nebo směrovače, přes který vede cesta s nejmenší cenou směrem ke kořenovému uzlu.
- Určený port (designated port) je port vedoucí k některému síťovému segmentu po cestě s nejmenší cenou.

Pokud při kalkulaci cest mají dvě stejnou hodnotu, pak je vybrána ta, která vede přes most s nejnižším identifikátorem. Jedním z atributů pro výpočet cesty s nejmenší cenou je hodnota přiřazená jednotlivým síťovým segmentům na trase. Cena je počítána na základě standardu 802.1D (1998) nebo 802.1t (2001).

Tab. 7. Hodnoty síťových segmentů v protokolu STP [6].

Propustnost segmentu	Hodnota podle 802.1t	Hodnota podle 802.1D
10 Gb/s	2000	2
1 Gb/s	20000	4
100 Mb/s	200000	19

Algoritmus STP používá dynamické metody pro výpočet optimálních tras. Využívá protokol BP (bridge protocol), který funguje na základě vícesměrového vysílání rámců BPDU (bridge procol data unit). Ty obsahují informace o aktuálních cenách segmentů sítě a identifikátorech dostupných uzlů. S pomocí těchto informací může být upravena kořenová trasa v síti.

V rámci protokolu BP jsou definovány tři typy zpráv BPDU:

- konfigurační BPDU (CBPDU),
- notifikace o změně topologie (TCN),
- potvrzeni notifikace o změně topologie (TCA).

Port mostu se nachází v jednom z následujících stavů:

- Naslouchání – příchozí rámce jsou přijímány a zpracovány, ale nic se neodesílá.
- Učení – adresy okolních mostů tohoto portu jsou přidávány do směrovací tabulky, ale žádné rámce se nepředávají. Port ve stavu učení může být zakomponován do aktivní topologie.
- Předávání – na portu je možné přijímat I odesílat síťová data, přitom STP zpracovává všechny příchozí rámce BPDU a reaguje na změny. Všechny porty v kořenovém uzlu a všechny kořenové porty ostatních mostů jsou vždy v režimu předávání, stejně jako všechny určené porty na samostatném segmentu.
- Blokování – konfigurace portu nedovoluje přijímat ani odesílat data, přijímají se jen příchozí rámce BPDU, na jejímž základě je možné stav portu změnit. Všechny porty v uzlu, které jsou propojeny s jiným mostem a nejsou ani kořenové ani určené, musí být v režimu blokování.
- Vyřazení – porty mohou být konfiguračně nebo softwarově zakázány. Tento stav není způsoben chováním algoritmu STP.

Protokol RSTP definován standardem 802.1w a následně 802.1D-2004 zkracuje čas konvergence konfigurace STP. V rámci RSTP jsou zablokované porty rozčleněny na další dva stavy:

- alternativní port přijímá rámce BPDU z ostatních uzlů s vyšší prioritou a je blokovaný.
- záložní port přijímá rámce BPDU z téhož mostu a je také zablokovaný.

Díky těmto stavům je možné při výpadku kořenového portu rychleji ustanovit alternativní trasu. Reakce na selhání kořenové uzlu se zkracuje pod 2 sekundy mezi zprávami HELLO. Záložní port je redundantní linkou ve stejném síťovém segmentu [5], [6], [10], [12].

4.2 Typy a specifikace optických sítí

Gigabitový Ethernet (GbE) je aktuálně platným standardem pro ethernet sítě. Standard IEEE 802.3ae definuje plně duplexní desetigigabitový ethernet pro optická vlákna, kroucené dvojlinky (10 GBase-T) a pro měděné dvojité koaxiální kabely (Twinax). Tento standard se využívá pro vysokorychlostní propojení. Je definováno několik standardních typů modulů pro optické a metalické spojení:

- optické – SR, LR, LRM, ER, ZR a LX4,
- metalické – T, CX4, SFP+ DAC.

Tab. 8. Maximální dosah 10 GbE rozhraní.

Typ	Vlákno	Vzdálenost	Typ	Vzdálenost
SR	MM OM4	400 m	SFP+ DAC	< 10 m
LR	SM	10 km	CX4	< 15 m
LRM	MM OM4	500 m	T	< 100 m
FET	MM OM4	100 m		
ER	SM	40 km		
ZR	SM	80 km		

10 GBase-T se používá na kroucených dvojlinkách (kabel kategorie 6e) o délce max. 100 m a je zpětně kompatibilní s 1 GBase-T. Standard 802.ba definuje 40Gb/s a 100Gb/s ethernet.

4.3 Normy pro IP adresování

Standard RFC1918 definuje rezervované IP adresy – bloky/třídy, které lze použít v privátních IP sítích, oddělených od veřejných sítí. Tyto privátní rozsahy nejsou směrovány do veřejných sítí. Pro komunikaci je nutné použít překlad IP adres NAT (Network Address Translation).

Tab. 9. Rezervované adresy podle RFC1918.

Blok adres	Velikost bloku (počet adres)	Třída / Použití
10.0.0.0 / 8	24 bitů (16 777 216 adres)	A / Privátní
172.16.0.0 / 12	20 bitů (1 048 576 adres)	B / Privátní
192.168.0.0 / 16	16 bitů (65 536 adres)	C / Privátní

Protokol IP verze 6 je nástupcem IP verze 4. Poskytuje větší adresní prostor, lepší granularitu a zabezpečení. Záhlaví je jednodušší, má zabudovaný přirozený mechanismus pro vyřešení kvality služby QoS formou štítkování toků (flow labeling). Definice podsítí není nutné, protože podsítě jsou zahrnuty v prefixu sítě. Vyloučení NAT znamená eliminaci množství chyb v konfiguraci sítí. Problémy s NAT mají mnohé aplikace, hlasové protokoly VoIP, SIP, streaming aplikace nebo P2P. Protokol NDP (Neighbour Discovery Protocol) zajišťuje rozpoznávání sousedů, identifikaci síťových prefixů a automatickou konfiguraci sítě a směrování. Řeší rezoluci adres a nalezení dalšího směrovače. Konfigurace DHCP je irelevantní, protože automatická konfigurace adres je do protokolu přímo zabudovaná a probíhá pomocí dotazů na směrovač. Místní linkové adresy jsou v síti unikátní, tím odpadá problém síťových kolizí.

Adresní prostor má šířku 128 bitů. Hostitelská část adresy je buď přiřazené sekvenční číslo, nebo je odvozena z mac adresy. Identifikátory sítě a hostitele mají stejnou délku 64 bitů.

Příklad adresy: 2001:0db8:3c4d:0015:0000:0000:abcd:ef14 /128

- 2001:0db8:3c4d = globální prefix (48 bitů),
- 0015 = identifikátor podsítě (16 bitů),
- 0000:0000:abcd:ef14 =adresa hostitele (64 bitů).

IP datagramy verze 6 obsahují následující pole:

- verze (Version),
- třída provozu (Traffic Class) - priorita paketu,
- značka toku (Flow Label) – kvalita služby QoS definovaná aplikacemi pracujícími v reálném čase,

- délka datového pole (Payload Lenght) – hodnota určující velikost bloku dat,
- další záhlavní (Next Header) – ekvivalent pole s identifikací protokolu další vrstvy,
- limit hopů (Hop Limit) – maximální povolený počet následujících přeskoků při směrování v síti (jedná se o náhradu time-to-live),
- zdrojová adresa,
- cílová adresa.

Současné nevýhody implementace IP verze 6 jsou v některých aplikačních protokolech, které zabalují do svých přenosů síťové adresy IP. Musí dojít k přepracování, aby dokázaly nést rozdílnou strukturu adres. Do této skupiny patří například FTP nebo NTPv3. Používá-li se komunikace Ipv6 přes IPv4, je nutné použít zapouzdření (tunelování) [5], [6], [10], [12].

4.4 Firewally

Firewally jsou hardwarové nebo softwarové zařízení zajišťující fyzickou izolaci sítí pomocí více síťových rozhraní, pravidel definovaných na protokolové úrovni (protokolová izolace) a jejich uplatňování na provoz, který skrze firewall prochází. Mezi základní funkce firewallu patří:

- Filtrování paketů – na základě pravidel se aplikuje na příchozí nebo odchozí provoz.
- Vstupní filtry na síťovém rozhraní – na základě rozsahu IP adres, protokolů a portů.
- Překlad síťových adres NAT (Network Address Translation) – překlad privátních adres na veřejné.
- Stavová inspekce – kontrola odchozích paketů a zaznamenávání jejich cílů do stavové tabulky. Příchozí pakety jsou porovnány se stavovou tabulkou.
- Inspekce okruhů – kontrola relací proti útokům typu podvržení IP adresy (IP spoofing) nebo odmítnutí služby (DoS).
- Proxy firewally – vytváří dvě oddělená spojení na každé straně firewallu, mezipaměť (cache) a vyžaduje autentizaci na základě identifikace uživatelů.

- Aplikační filtry – technologie hloubkové inspekce paketů DPI (Deep Packet Inspection) – zkoumá datovou část paketů.

Základní členění firewallů:

- Personální – součást operačního systému klientské stanice.
- Firewally ve směrovačích – sekundární funkce firewallu jsou implementovány přímo nad primární směrovací funkcí a jsou omezeny funkcemi nebo výkonností zařízení.
- Hardwarové firewally – jednoúčelová zařízení s funkcí firewallu a omezenou funkcí směrování.
- Serverové firewally – druhý stupeň ochrany přístupu pomocí pravidel definovaných přímo na serveru. Hlavním cílem je omezit zranitelnost uvnitř sítě.
- Bezpečnostní brány – zařízení pracující na aplikační (sedmé) vrstvě.

Firewally oddělují oblasti sítě do zón s různými úrovněmi důvěryhodnosti:

- Internet – jedná se o zóny bez jakékoli důvěryhodnosti.
- Hraniční síť – skládá se zejména ze směrovače, který je viditelný z externí sítě a může provádět překlad adres. Obecně platí, že jediný povolený provoz je do demilitarizované sítě.
- Hraniční firewall – má za úkol komunikaci s demilitarizovanou zónou.
- Demilitarizovaná zóna (DMZ) – je oblast střední úrovně důvěryhodnosti. Obsahuje servery komunikující do internetu jako web servery, Proxy servery, poštovní servery. DMZ sahá od příchozího rozhraní hraničního firewallu po odchozí rozhranní interního firewallu. DMZ je vhodným místem pro uplatnění restrikcí technologie NAP (Network Access Protection).
- Interní firewall – provádí další překlad adres, který skrývá interní privátní sítě. Provoz z DMZ do interní sítě podléhá jiné sadě pravidel, která je méně restriktivní, než jakou má hraniční firewall.Komunikace z DMZ je předána na interní směrovač.
- Firewall typu Proxy server - může nabízet služby na aplikační vrstvě, analyzovat typ paketů a směrovat provoz na odpovídající aplikační server.

- Interní síť LAN – privátní síť se skládá z důvěryhodných serverů, počítačů a dalších systémů nebo podsítí.

Bezestavové filtry – jsou nejjednodušší paketové filtry nebo firewally, ve kterých se zkoumají pakety na pole typu zdrojová a cílová adresa, protokol TCP/UDP a číslo portu a podle filtru jsou povoleny nebo zamítnuty.

Stavové filtry – analyzují každé TCP spojení, jehož součástí je příslušný paket, a informace o spojení zahrnují do rozhodovacího algoritmu, zda je paket součástí povolené relace nebo zakládají novou relaci, přičemž porovnávají konfigurační sadu pravidel - filtrů. Ve stavovém filtru probíhá proces „stavová inspekce paketů (SPI, Statefull Packet Inspection). Stavové filtry řeší a odhalují používání libovolných jiných portů pro příslušné standardní aplikace typu FTP, HTTP, identifikují tzv. přesměrování portů, porovnávají relaci s tabulkou stavů a čísly portů podle tabulky. Tabulka stavů obsahuje hlavní atributy každé relace – zdrojovou a cílovou adresu, čísla portů a sekvenční čísla paketů, která odečítá. Položka v tabulce stavů se vyskytuje pouze po dobu trvání relace. Registrace spojení v stavové tabulce spočívá v mechanismu zasílání paketů SYN, ACK mezi firewallem a iniciátorem. Nevýhodou tohoto mechanismu je záplava firewallu množstvím SYN paketů v případě DoS (Denial of service) útoku a přetečení stavové tabulky firewallu.

Aplikační filtrování – mechanismus, který zkoumá aplikace a protokoly, jejíchž prostřednictvím byl paket vytvořen a odeslán. Je schopný rozpoznat, zda komunikace na daném portu nese znaky odpovídající aplikačnímu protokolu. Na základě nálezů mohou aplikační filtry provoz zablokovat, přesměrovat nebo jeho obsah změnit. Využívá technologie DPI a porovnává data s databází signatur útoků.

Implicitní zákaz komunikace – je princip nastavení výchozího stavu zařízení, že žádná komunikace není povolena [5], [6], [11], [12].

4.5 Typy zranitelností

Součástí bezpečného návrhu a provozu sítě je uvědomění si zranitelností sítě – slabých míst k napadení. Odhalení síťových zranitelností lze zajistit pravidelnými prověrkami sítě pomocí nástrojů pro analýzu rizik – skenerů zranitelností (vulnerability scanner). Funkce spočívá ve zjištění otevřených portů na dostupných IP adresách, nalezení seznamu operačních systémů a otestování známých zranitelností. Firma SIG vyvíjí standard CVVS

(Common Vulnerability Scoring System – společný systém hodnocení zranitelností), kterým se měří závažnost zranitelností na síti. Jeho součástí je zjištění skutečné podstaty zranitelného místa, uvědomění si hrozeb z něj plynoucích a stanovení hodnoty a metriky plynoucí z typu nasazení a stavu okolního prostředí. Metodiku CVVS implementuje na internetu on-line kalkulátor, který vystavuje americká národní databáze zranitelností NVD (National Vulnerability Database). Příkladem databáze softwarových zranitelností je MBSA (Microsoft Baseline Security Analyzer).

Základní a nejčastější typy vnějších útoky:

- Dostupnost systému – počítačové prvky v síti je možné přetížit všesměrovým vysíláním ICMP paketů, jejichž výsledkem je záplava odpovědí na systém oběti – smurf útok.
- Odepření služby DoS – při tomto typu útoku je služba zahlcena požadavky útočníka. Obvyklým příkladem je útok na DNS servery.
- Distribuované útoky DoS (DDoS) – provádí je koordinovaně větší množství napadených systémů.

Útoky zvenku nebo zevnitř sítě:

- Autentizace – podvržení autentizačních údajů.
- Data při přenosu – datový komunikační provoz může být v průběhu přenosu zachycen a pozměněn – útok Man in the middle (muž uprostřed).

Vnitřní útoky:

- Trójské koně – poskytují útočníkovi možnost ovládat systémy uvnitř sítě.
- Zadní vrátka – forma spustitelných programů, které provádějí škodlivé akce. Jedna z forem je tzv. rootkit, který jsou uchován na systémové úrovni ve formě ovladačů nebo modulů v jádře operačního systému.
- ARP spoofing – útok na klientské zařízení prostřednictvím ARP protokolu. Hlavním cílem je, aby se útočník mohl vydávat v lokální síti za jinou stanici. Pro úspěšné provedení útoku musí útočník s IP adresou 192.168.100.x obelstít klientské zařízení (oběť) s adresou 192.168.100.y a dosáhnout toho, že útočníkova stanice bude brána pro veškerou komunikaci, která má původní IP adresu 1.

Následně je třeba stejnou metodou obelstít síťové zařízení, aby pakety určené pro oběť přeposílalo na stanici útočníka. A posledním nastavením je přeposílání paketů (IP forwarding), které zajistí, aby komunikace probíhala dál a nevzbuzovala pozornost.

Bezpečnostní opatření by se měla soustřeďovat na tři základní úrovně zabezpečení:

- Ohodnocení rizik a prevence – nejefektivnějšími preventivními technologiemi pro ošetření rizik jsou řízení přístupu uživatelů, kryptografie a firewally.
- Detekce hrozeb – mezi systémy pro detekci hrozeb patří antivirové skenery, systémy detekce průniku IDS, audit událostí a heuristická analýza záznamů o událostech.
- Reakce na incidenty – při zjištění průniků a dalších typů útoků je třeba adekvátně reagovat – systémy IPS [2], [3], [6], [11], [12].

II. PRAKTICKÁ ČÁST

5 LOGICKÝ DESIGN

Zajištění bezpečnosti datového centra nebo jen počítačové sítě je komplexní záležitost. Zahrnuje oblasti, které spolu úzce souvisí – fyzický a logický design, fyzická a systémová bezpečnost. Logický design musí respektovat a splňovat základní požadavky, jako jsou spolehlivost a dostupnost, robustnost a rozšiřitelnost, soulad s legislativními požadavky, dodržení standardů a norem.

Návrh logického designu byl koncipován s ohledem na bezpečnostní aspekty. Jsou v něm využívány teoretické základy z předchozích kapitol, na kterých je postavena struktura praktické práce, která obsahuje následující části:

- Analýza rizik.
- Návrh bezpečnostní politiky.
- Návrh počítačové sítě s ohledem na bezpečnostní požadavky.
- Návrh zónového uspořádání počítačové sítě.

5.1 Analýza rizik

Analýza rizik by měla proběhnout nejlépe v existujícím reálném prostředí organizace, která spravuje datové centrum. Přestože se v nejbližším okolí taková organizace nachází, nebylo možné ji využít pro účely zpracování diplomové práce. Aby analýza rizik nebyla provedena jen na imaginárním datovém centru, byla provedena modelaci prostředí a byly stanoveny následující výchozí parametry datového centra:

- Samostatná budova vyhrazená pouze pro účely datového centra.
- Blíže nespecifikované rozměry ani požadavky na podlahovou plochu.
- Počet podlaží, stavební ani konstrukční provedení není předem stanoveno.
- Budova se nachází v lokalitě na okraji města, částečně obydlené, v dosahu běžné dopravní infrastruktury.
- Datové centrum využívá velká organizace s počtem zaměstnanců >1000, ročním obratem přesahujícím 100mil EUR.
- Organizace sídlí v několika lokalitách, které jsou propojeny vyhrazenou sítí WAN.

- Datové centrum je centrální a zároveň jediné místo, vyhrazené pro informační systém, pro zpracování a ukládání dat organizace.

Výchozí parametry byly nastaveny tak, aby v přeneseném menším měřítku odpovídaly i menším organizacím, které obvykle vlastní vyhrazenou místnost – serverovnu.

Pro analýzu byla použita metoda CRAMM Express. Prvním krokem analýzy rizik byla identifikace aktiv a jejich ohodnocení. Identifikace aktiv proběhla kvalifikovaným posouzením a přímým pohovorem s experty z oboru IT, kteří mají zkušenosti s provozem datových center nebo serveroven.

Pro ohodnocení aktiv byla použita stupnice 1 až 5 podle tabulky. Hodnota je měřena mírou následků v případě ohrožení důvěrnosti dat, integrity a dostupnosti aktiv. Typické riziko zahrnuje ztrátu, zničení, smazání, poškození, vyzrazení dat. Hodnota je vyjádřena slovně a finančním dopadem kalkulovaným procentem z ročního provozního zisku organizace (EBIT).

Tab. 10. Stupnice ohodnocení aktiv

Hodnota aktiva	Obchodní dopad	Finanční dopad
5	Hrozba nepřežití	>60% EBIT
4	Vážná škoda	10~60% EBIT
3	Důležitá škoda	1~10% EBIT
2	Malý dopad	0,01~1% EBIT
1	Zanedbatelný dopad	<0,01% EBIT

Je zřejmé, že identifikace datových aktiv jsou pro organizace hlavním předmětem analýzy a jak je uvedeno níže v tabulce, lze je rozdělit podle významu pro organizaci a klasifikovat každou kategorii samostatně. Primární podstata datového centra je zpracování a ukládání dat. Z toho důvodu je nezbytné všechna data klasifikovat nejvyšší hodnotou. Stejným způsobem byly hodnoceny i aplikace. Fyzická aktiva reprezentují všechna ostatní aktiva, která nejsou datová ani aplikační. Zajišťují efektivní ochranu těchto aktiv a nabývají

hodnoty, která je odvozena na základě hodnoty datových nebo aplikačních aktiv a dále zohledňují náklady na obnovu zařízení (nákup HW, instalace, konfigurace).

Tab. 11. Identifikace aktiv datového centra.

Typ aktiv	Identifikovaná aktiva	Hodnota aktiv
Datová aktiva	Data veřejná (www stránky)	1
	Data interní (intranet – standardní dokumenty)	2
	Data důvěrná (účetní, výrobní, zákaznická)	4
	Data tajná (smlouvy, strategie, finanční)	5
Datová aktiva (D)	Data organizace (zákazníka) v datovém centru	5
Aplikační aktiva	Aplikace veřejné (www stránky)	1
	Aplikace interní (intranet)	2
	Aplikace kritické (FI, BW, DW, SCM)	4
	Aplikace strategické a tajné (CRM, ERP)	5
Aplikační aktiva (A)	Aplikace organizace (zákazníka)	4
Fyzická aktiva	Server fyzický 1 aplikace (SF)	4
	Server virtuální 1 aplikace (SV)	3
	Server HOSTITEL pro více aplikací (H)	4
	LAN infrastruktura (směrovač, firewall, přepínač)	4
	WAN infrastrukture (směrovač, okruhy)	3
	Datová úložiště (DS)	5
	Zálohovací knihovny, zařízení (ZK)	5
Prostory	Kabeláž LAN, WAN (K)	3
	Bezpečnostní zařízení CCTV, ACS (BZ)	5

	Poplachové zařízení PZS, EPS (PZ)	5
	Hasící zařízení (SHZ)	3
	Komunikační systémy (KS)	3
	Přenosová zařízení poplachových systémů (KP)	5
	Systémy primárního napájení (AC)	5
	Systémy záložního napájení (UPS)	5
	Systémy záložního napájení (DA)	5
	Klimatizace (KL)	5
Služby koncovému uživateli	Přístup k datům a aplikacím (P)	3

V další fázi se analýza zaměřila na identifikaci hrozeb a zranitelností, která ohrožují jednotlivá aktiva. Byla opět použita metoda rychlého hodnocení podle metodiky CRAMM Express, které je založeno na expertním posouzení úrovně hrozeb. Úroveň se stanovuje mírou pravděpodobnosti a využívá se slovní vyjádření pravděpodobnosti, které je srozumitelnější pro respondenty.

Úroveň hrozeb je stanovena škálou 1 až 5:

1. velmi nízká hrozba (pravděpodobnost <0,2),
2. nízká hrozba (pravděpodobnost 0,2 – 0,39),
3. střední hrozba (pravděpodobnost 0,4 – 0,59),
4. vysoká hrozba (pravděpodobnost 0,6 – 0,79),
5. velmi vysoká hrozba (pravděpodobnost 0,8 – 1).

Tab. 12. Identifikace hrozeb a zranitelností.

Hrozby	Zranitelnost	Pravd.
Externí náhodné		

Přírodní hrozba (povodeň, bouřka apod.)	Fyzické poškození zařízení vodou	2
Blackout / výpadek napájení (primární i záložní zdroj)	Nedostupnost systémů v DC	2
Selhání komunikace, technická závada u operátora	Nedostupnost DC přes WAN	2
Požár, výbuch v okolí	Fyzické poškození zařízení ohněm	1
Výbuch v okolí	Fyzické poškození zařízení destrukcí	1
Externí úmyslné		
Požár úmyslně založený	Fyzické poškození zařízení ohněm	2
Výbuch úmyslně založený	Fyzické poškození zařízení destrukcí	2
Teroristický útok, sabotáž	Fyzické poškození zařízení, budovy	2
Infiltrace komunikace (narušení, zachycení, selhání)	Nedostupnost DC přes WAN	3
Logická infiltrace (hacking, viry, falšování identity)	Vnější hackerské útoky (zneužití dat, nedostupnost služby)	5
Interní náhodné		
Závady zařízení	Nedostupnost služby, dat, aplikace, sítě, technologických systémů	4
Lidské chyby (uživatelů, administrátorů, operátorů)	Nedostupnost služby, dat, aplikace, sítě	4
Poškození vodou	Fyzické poškození zařízení	2
Požár	Fyzické poškození zařízení	2
Interní úmyslné		
Logická infiltrace	Vnitřní hackerské útoky, zneužití dat,	3

(hacking, viry, falšování identity)	nedostupnost služby	
Infiltrace komunikace (narušení, zachycení, selhání)	Nedostupnost DC přes WAN	3
Závady zařízení	Nedostupnost služby, dat, aplikace, sítě, technologických systémů	2
Lidské chyby (uživatelů, administrátorů, operátorů)	Nedostupnost služby, dat, aplikace, sítě	2
Poškození vodou	Fyzické poškození zařízení	1
Požár	Fyzické poškození zařízení	1

Posouzení zranitelností jednotlivých aktiv jednotlivými hrozbami bylo složitější pro zpracování. Byla použita první metoda, která předpokládá maticové zpracování. Každý respondent posuzoval vliv dané hrozby na zranitelnost aktiva. K posouzení byla použita pouze tříbodová škála:

1. nízký vliv hrozby na zranitelnost aktiva (pravděpodobnost <0,33),
2. střední vliv hrozby na zranitelnost aktiva (pravděpodobnost 0,34 – 0,66),
3. vysoká vliv hrozby na zranitelnost aktiva (pravděpodobnost 0,67 – 1).

Byla vytvořena matice zranitelností. Pro výpočet rizika byl použit vzorec 1.6 a výsledek byl přenesen do finální matice rizik. Obě kompletní matice se vzhledem ke svému rozsahu nacházejí v příloze P1.

Riziko je vyjádřeno tříbodovou škálou a pro snadnější orientaci se využívá barevné rozlišení úrovně rizika:

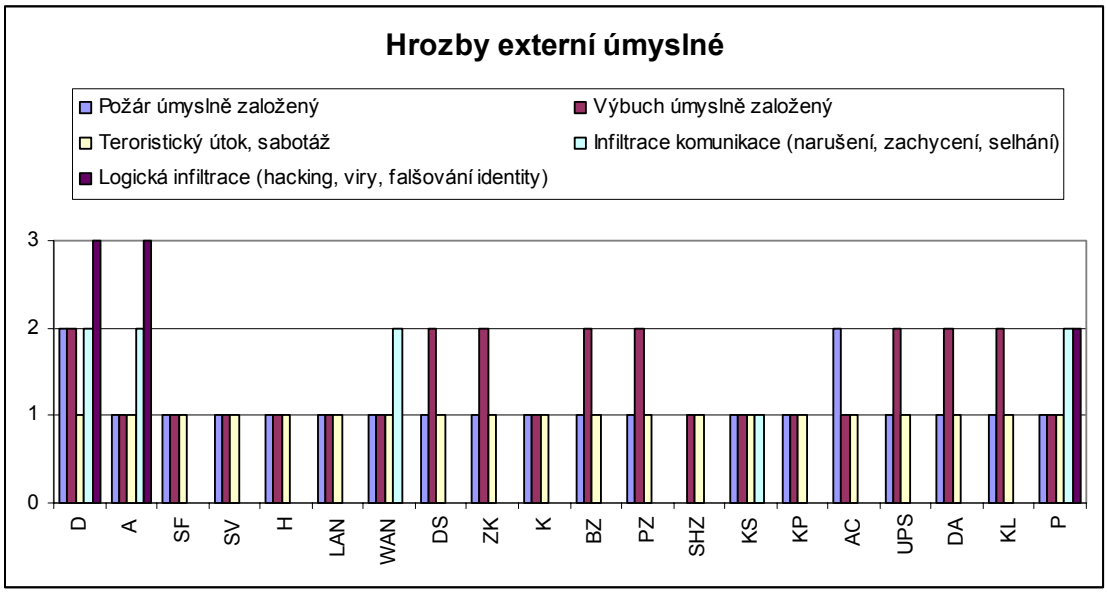
- zelená – nízké riziko (vypočtená hodnota 1 až 25),
- žlutá – střední riziko (vypočtená hodnota 26–50),
- červená – vysoké riziko (vypočtená hodnota 51–75).

Závěrem každé analýzy musí být návrh na řešení. Opatření jsou detailně popisována v následujících kapitolách.

5.1.1 Hrozby s vysokým rizikem

Nejprve je nutné se zaměřit na hrozby s vysokým rizikem. Podle matice rizik se jedná o následující hrozby:

1. Hrozba logické infiltrace (hacking, viry, falšování identity) – vnější hackerské útoky s cílem zneužití dat a nedostupnosti služby zaměřené na data a aplikace.



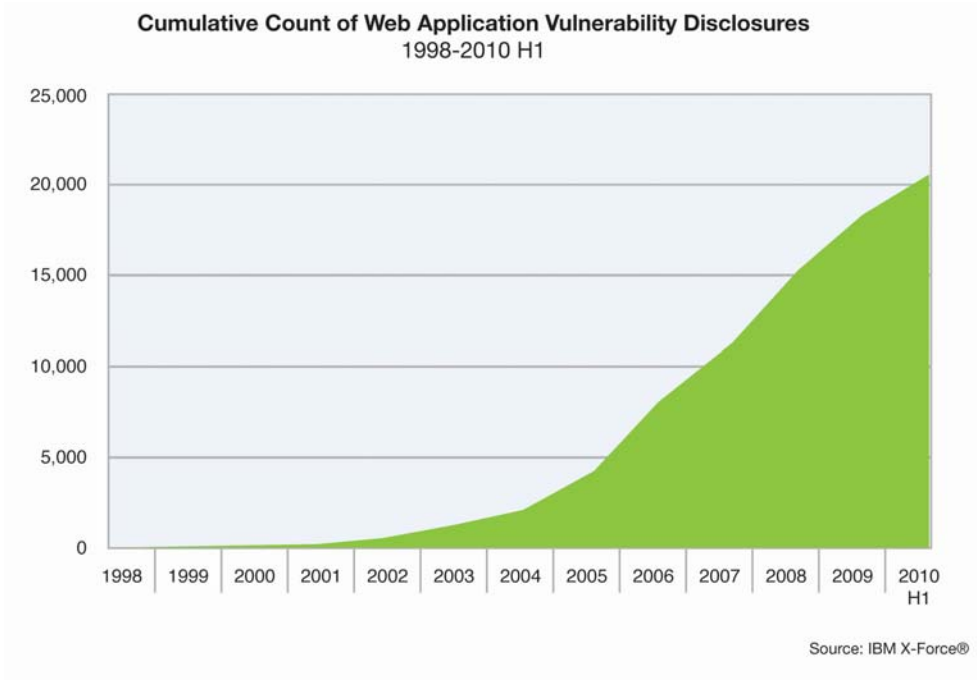
Graf 1. Rizika externí úmyslné hrozby.

Kritické jsou rostoucí útoky zaměřené na webové aplikace, služby a data. Uvedený graf musí být hnací silou organizace řešit a prosazovat informační bezpečnost v rámci celé organizace. Tyto útoky zahrnují SQL injection útoky, cross-site scripting (XSS), útoky DoS, různé techniky, jako je procházení adresářů. Útočníci používají tyto typy útoků na zobrazení nebo získání neoprávněných informací, nebo se pokouší změnit soubory, adresáře, uživatelské informace a ostatní součásti webových aplikací [23].

Opatření:

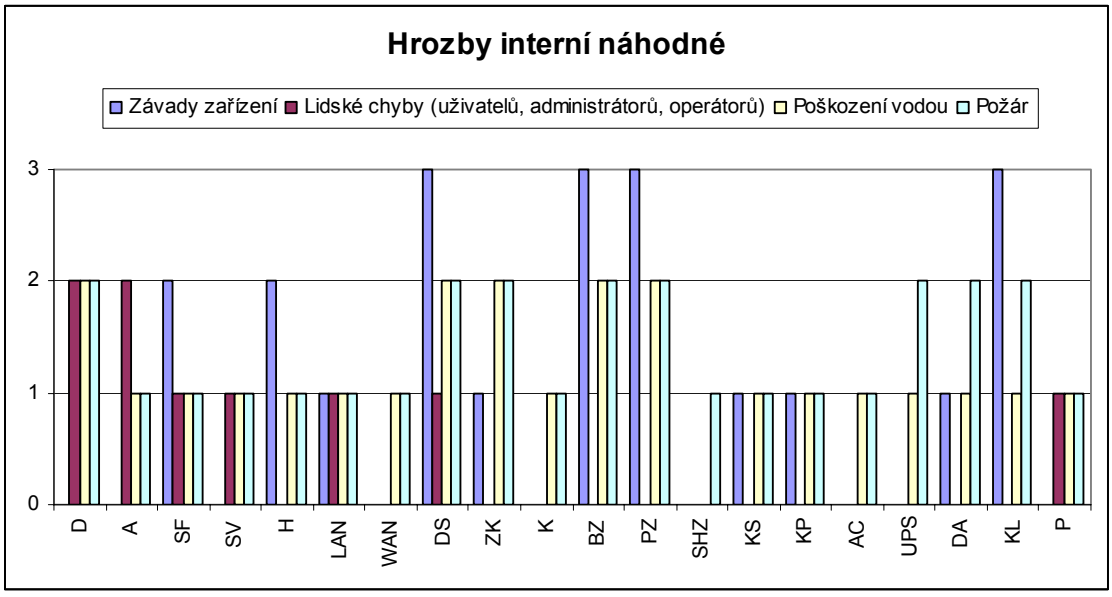
- Zónové uspořádání sítě (logické a fyzické).
- Implementace firewallů a IPS systémů.
- Implementace a dodržování systémových politik.

- Implementace bezpečnostních standardů serverů.



Obr. 5. Nárůst zranitelností aplikací [23].

2. Hrozba závady na zařízeních – datová úložiště, bezpečnostní a poplachové systémy a klimatizace.



Graf 2. Rizika interní náhodné hrozby.

Opatření:

Protože se jedná o interní náhodné hrozby, které nelze nikdy vyloučit, bude nutné stanovit únosnou míru spolehlivosti – pravděpodobnost bezporuchového provozu vyjádřenou procentem z celkové doby provozu zařízení. Požadavek na nižší bezporuchovost s sebou nese vyšší finanční náročnost řešení. Technické řešení vychází ze stanovené míry spolehlivosti.

5.1.2 Hrozby se středním rizikem

Tyto hrozby jsou četnější, a proto jsou větším problémem pro organizace.

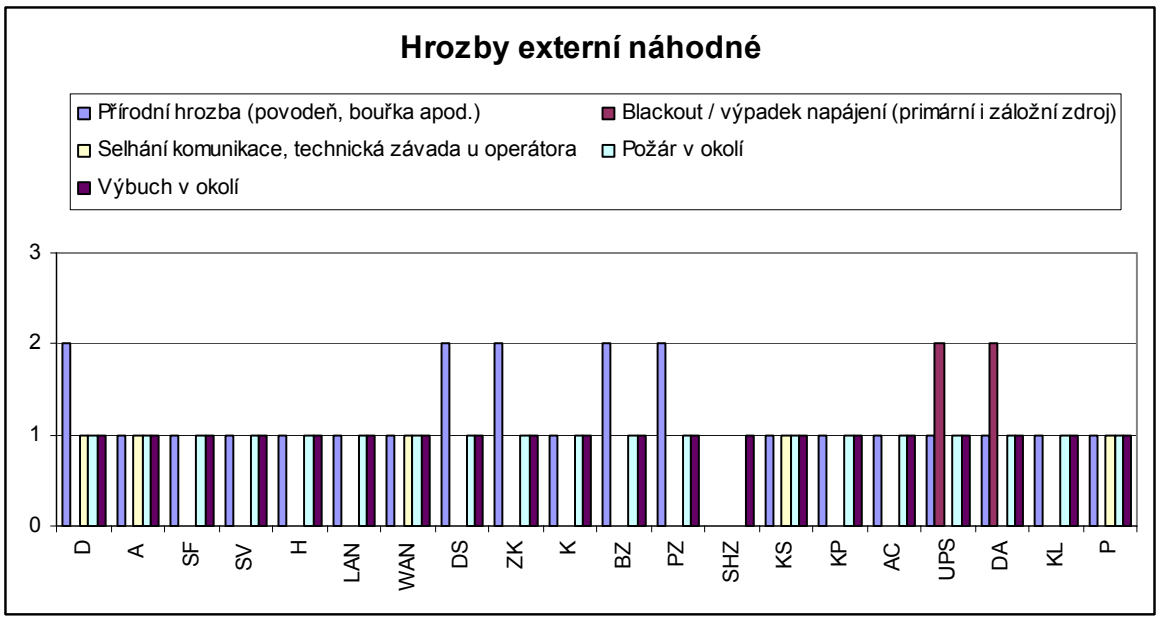
Protiopatření jsou velmi nákladná a ne vždy jednoznačně účinná.

Do této kategorie spadají typické externí náhodné hrozby:

- přírodní hrozba – povodeň a poškození zařízení vodou,
- blackout – výpadek primárního i sekundárního napájení,

nebo externí úmyslné,

- úmyslný výbuch – fyzické poškození zařízení nebo budovy,
- teroristický útok, sabotáž, poškození zařízení,
- infiltrace komunikace.



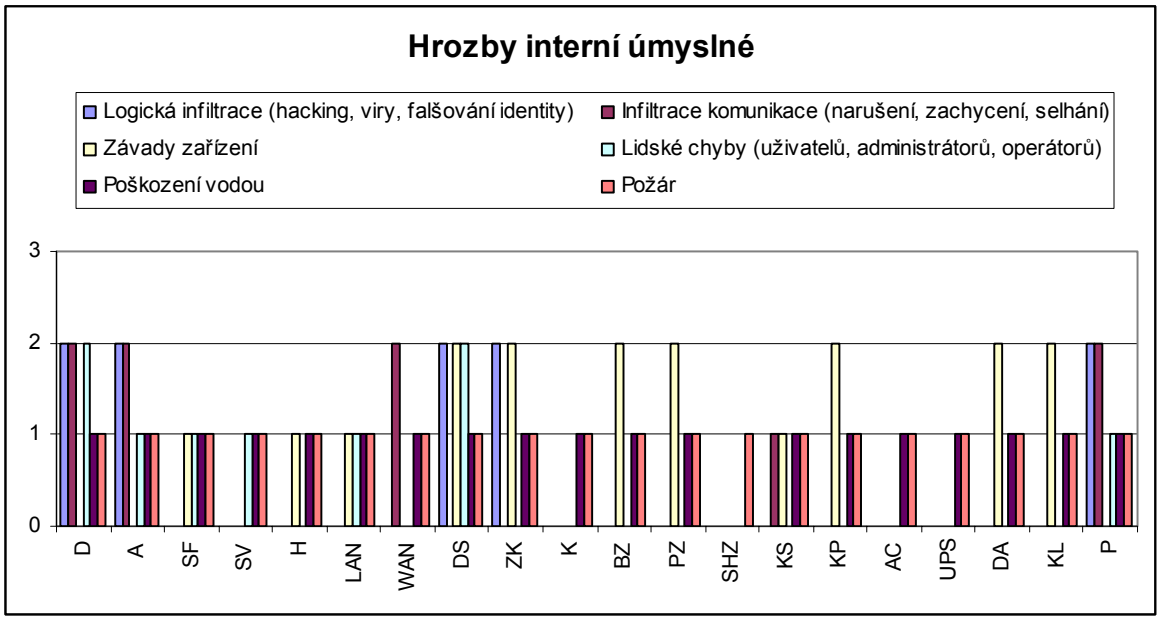
Graf 3. Rizika externí náhodné hrozby.

A v neposlední řadě se jedná o celou škálu interních úmyslných:

- vnitřní logická infiltrace (hacking, viry, falšování identity) – vnitřní hackerské útoky zaměřené na HW, data i aplikace,
- vnitřní infiltrace komunikace – s cílem odříznout DC od externí komunikace a zachycení komunikace,
- úmyslné technické závady – bezpečnostní a poplachové systémy, datová úložiště a zálohy,

anebo náhodných hrozeb:

- požár,
- poškození vodou,
- lidské chyby.



Graf 4. Rizika interní úmyslné hrozby.

5.2 Návrh bezpečnostní politiky

Bezpečnost informací a systémů lze dosáhnout implementací soustavy opatření ve formě pravidel, postupů, procedur a hardwarových funkcí nebo nastavení. Je nezbytné nejprve stanovit bezpečnostní požadavky.

K tomu existují tři hlavní zdroje:

- Analýza a hodnocení rizik, která organizaci hrozí.
- Požadavky dané ze zákonů, norem a standardů, které organizace musí splňovat.
- Konkrétní principy, cíle a požadavky, které si organizace vytvořila pro podporu své činnosti – tedy vnitřní normy a předpisy.

Návrh BP datového centra je specifický svým úzkým zaměřením na systémy instalované v datovém centru, které se liší od běžného uživatelského prostředí organizace. Při návrhu je nutné vycházet i z opatření, která jsou považovaná jako základ nejlepších praktik pro zajištění bezpečnosti a implementaci systémů.

Návrh BP vychází z analýzy rizik. Výpočet míry rizika pomáhá identifikovat a stanovit správné a dostatečné úsilí na potlačení hrozeb.

Standardní postup, používaný obecně při tvorbě a implementaci BP organizace, byl zredukován vzhledem k faktu, že práce není zaměřena na konkrétní organizaci. Nejsou aplikovány následující části:

- předběžná studie,
- realizace a tvorba bezpečnostní dokumentace nižší úrovně,
- průběžná realizace osvěty – udržování bezpečnostního povědomí zaměstnanců.

Výstupem BP je návrh řady opatření, která se následně uplatňují v logickém návrhu, v návrhu fyzické bezpečnosti a návrhu systému řízení zranitelností. V práci jsou aplikovány základní oddíly bezpečnosti dle ČSN ISO/IEC 17999:2005 a ISO27000.

Návrh BP řeší interní prostředí z pohledu organizace:

- síť v datovém centru, určenou k administraci a instalaci systémů,
- vzdálený přístup do datového centra,
- interní síť mimo datové centrum, tedy ve vzdálených administrativních lokalitách organizace.

Cílem BP je kromě jiného eliminovat nebo minimalizovat hrozby, aplikovat protiopatření. Z provedené analýzy rizik je patrné, že vnitřní logická infiltrace (hacking, viry, falšování identity) a vnitřní infiltrace komunikace jsou hrozby středního rozsahu, kterým lze

předcházet právě implementací vhodné BP. Všeobecným cílem BP je zamezit rizikům neoprávněného přístupu k informacím a aktivům, zamezit nebezpečí virových infekcí, znepřístupnění služeb, sledování a modifikování komunikace v interní síti.

BP je rozčleněna do několika sekcí – samostatných politik.

Systémová bezpečnostní politika: Interní síť

- Interní síť je oddělena od internetu prostřednictvím firewallu a demilitarizované zóny. DMZ je oddělena od internetu externím firewallem a od interní sítě interním firewallem, který slouží jako jediný přístupový bod do interní sítě.
- V interní síti jsou vytvořeny speciální segmenty odpovídající příslušným VLAN, které jsou rovněž od sebe odděleny firewally. Síť je rozdělena na bezpečnostní zóny a odděleny od sebe jsou jednotlivé segmenty serverů.
- Existuje jedna DNS architektura, která zpracovává požadavky na více typů adres.
- Používání lokálních LMHOST souborů je povoleno v případě, že DNS službu nelze na segmentu sítě implementovat nebo že tuto službu vyžaduje příslušná aplikace.
- Využití DHCP mechanismu není povoleno pro adresování serverů.
- Bezpečnostní technická opatření pro eliminaci interních útoků.

Systémová bezpečnostní politika: Servery

- Každý server má rozhraní pro přístup do sítě definované standardem pro příslušný segment sítě.
- Každý server má svého správce a ten je zodpovědný za implementaci bezpečnostní politiky na tomto serveru.
- Každý server musí provádět zálohování dat na úrovni systému. Postup a periodicita zálohování je popsána v dokumentu Politika: Řízení zálohování.
- Na serveru musí běžet pouze přesně specifikované aplikace. Musí být prováděno pravidelné testování systému podle příslušných testovacích plánů, vedena evidence konfigurace systému a jejich změn.

- Administrátorská hesla musí být uložena odděleně od serveru a musí se pravidelně měnit. Doporučuje se využití speciálního SW na správu hesel.

Systémová bezpečnostní politika: Práce v síti

- Pro práci v síti lze používat pouze takové vybavení, které bylo schváleno IT oddělením organizace.
- Přístup do internetu je povolen pouze k pracovním účelům přes příslušné rozhraní např. proxy server.
- Je zakázáno ukládat na diskové prostory v rámci interní sítě data nepracovního charakteru.
- Je zakázáno do jakéhokoliv komponentu prostředí interní sítě instalovat či k němu připojovat jakékoliv hardwarové komponenty bez předchozího souhlasu IT oddělení nebo administrátora systému.
- Je zakázáno do jakéhokoliv komponentu prostředí interní sítě instalovat jakýkoliv SW bez předchozího souhlasu IT oddělení nebo administrátora systému.
- Je zakázáno jakkoliv měnit konfiguraci serverů nebo pracovních stanic – vypínání antivirové ochrany, odebírat či přidávat komunikační služby, měnit nastavení logování či dokonce odstraňovat nebo editovat logy v systému.
- Každý uživatel je osobně odpovědný za všechny úkony provedené v interní síti, které byly autorizovány jeho jménem a heslem. Proto musí uživatelé dodržovat následující pravidla:
    - přístupová hesla musí uživatel zachovávat v utajení,
    - je přísně zakázáno používat účet a heslo jiného uživatele,
    - uživatel je povinen měnit periodicky každých xx dní svá přístupová hesla, pokud toto není řízeno automaticky na úrovni systému, v případě vyzrazení hesla neprodleně,
    - v případě podezření na zneužití hesla, tuto skutečnost neprodleně ohlásit pracovišti IT,
    - při volbě přístupových hesel je uživatel povinen dodržovat související předpisy a pravidla.

- Porušení výše uvedených bezpečnostních politik se považuje za hrubé porušení pracovní kázně a má za následek disciplinární řízení.

Systémová bezpečnostní politika: Systémy pro vzdálený přístup

- Pro vzdálený management serverů slouží jeden přístupový bod. Vzdálený přístup využívá bezpečnostních protokolů typu IPSec. Všechna komunikace je vedena přes DMZ a je monitorována.
- Je zakázáno pro vzdálený přístup používat jakékoliv jiné zařízení, které nebylo schváleno IT oddělením.
- Zařízení pro vzdálený přístup smí používat pouze autorizovaný zaměstnanec nebo pověřený pracovník třetí strany a nesmí provozovat nepovolené operace.
- Je třeba dodržovat systémové požadavky bezpečnostní politiky pro šifrování informací, VPN, bezdrátovou komunikaci a řízení přístupu.
- Bezpečný vzdálený přístup musí být přísně kontrolován prostřednictvím použité silné autentizace s použitím jednorázového hesla generovaným tokeny nebo s použitím elektronických certifikátů.
- Zaměstnanci nesmějí nikomu sdělovat žádné informace o přístupových účtech ani heslech, ani rodinným příslušníkům.
- Počítače nesmějí být současně připojeny do jiných sítí prostřednictvím jiných rozhraní nebo VPN tunelů.
- Používání internetu, internetového emailu nebo sociálních sítí není povoleno a musí být příslušným SW pro vzdálený přístup automaticky zablokováno.
- Povoleno je pouze používání firemní komunikačních kanálů.
- Všechna zařízení pro vzdálený přístup musí mít aktualizovaný antivirový SW a musejí obsahovat personální firewall.

Systémová bezpečnostní politika: Bezpečnostní pravidla pro vzdálený přístup

- Uživatel, kterému je umožněn privilegovaný přístup prostřednictvím VPN, je odpovědný za to, že tento přístup do interní sítě neposkytne neautorizovanému uživateli.

- Pokud je aktivní VPN spojení, musí být veškerá komunikace stanice směrována do VPN tunelu a vše ostatní blokováno.
- Vícenásobné tunely nejsou povoleny.
- VPN výchozí brána je řízena a nastavována VPN SW a uživatel nemá oprávnění ji měnit.
- Všechny pracovní stanice využívající VPN spojení musí obsahovat aktualizovaný antivirový SW. Počítače, které nejsou ve správě organizace, nesmějí VPN tunel využívat.
- Všechny VPN tunely musí být automaticky ukončeny po 30 minutách nečinnosti.

Systémová bezpečnostní politika: Síťové prvky – směrovače

- Síťový prvek nesmí mít lokálně definovaný uživatelský účet. Směrovače musí využívat autentizaci prostřednictvím služby TACACS, RADIUS nebo ACE.
- Musí být vypnuty následující protokoly:
    - IP direct broadcast,
    - příchozí pakety s invalidními adresami dle RFC1918 musí být zahazovány,
    - TCP small services,
    - UDP small services,
    - All source routing,
    - Web servis běžící na síťovém směrovači.
- Musí být dodrženy standardy pro SNMP verze 2 a 3.
- Každý směrovač musí upozorňovat uživatele na neoprávněnost neautorizovaného přístupu (banner).

Systémová bezpečnostní politika: Síťové prvky – obecně

- Konfigurace síťových zařízení musí být porovnávána se standardem pro bezpečnou konfiguraci stanoveným pro každý typ síťového zařízení používaný v organizaci. Konfigurace zabezpečení těchto zařízení by měly být dokumentovány, přezkoumány a schváleny příslušným oddělením IT. Jakékoliv odchylky od

standardní konfigurace nebo aktualizace do standardní konfigurace by měly být zdokumentovány a schváleny v systému řízení změn.

- Poslední stabilní verze firmware nebo síťového operačního systému (IOS) musí být nainstalována do 30 dnů od doby, kdy aktualizace byla publikována dodavatelem zařízení.
- Síťová infrastruktura by měla být administrována a řízena přes síťová připojení, která jsou oddělena od produkční sítě organizace. Je nutné definovat oddělenou VLAN nebo úplně oddělené fyzické připojení.
- Definujte síťovou architekturu, která odděluje vnitřní systémy od DMZ a extranet systémů. DMZ systémy by nikdy neměly obsahovat citlivá data a interní systémy by nikdy neměly být přímo přístupné z Internetu.
- Každé zařízení musí mít nastaveno logování nebo audit protokolů a přístupů. Záznamy musí obsahovat datum, časové razítko, zdrojové adresy, cílové adresy, a různé další užitečné prvky každého paketu a / nebo transakce.

Systémová bezpečnostní politika: Internet

- Pro práci s internetem lze používat pouze takové vybavení, které bylo schváleno IT oddělením organizace a které má nainstalovaný aktualizovaný antivirový SW, bezpečnostní aktualizace a personální firewall.
- Přístup do internetu je povolen pouze k pracovním účelům přes příslušné rozhraní např. proxy server.
- Je zakázáno stahovat nebo kopírovat z internetu do prostředí organizace jakákoliv data nepracovního charakteru.
- Je zakázáno stahovat nebo kopírovat z internetu do prostředí organizace jakákoliv data pracovního charakteru, pokud se jedná o neschválený, nelicencovaný, nebo jinak nebezpečný, infikovaný či škodlivý SW.
- Je zakázáno používat sociální sítě, diskusní servery a konference a sdělovat jakékoliv informace obsahující know-how nebo interní informace organizace.

- Při komunikaci v konferencích v rámci dotazů o pomoc není možné uvádět konkrétní informace o sítích, adresách a konfiguracích serverů nebo síťových prvků.

Systémová bezpečnostní politika: Správa hesel

- Je nutné změnit přednastavená hesla typu *cisco, password*.
- Běžný uživatel nesmí užívat přístup typu root, privilegovaný přístup, administrátorský přístup.
- Politika obsahuje základní parametry a postupy pro tvorbu hesel dle tabulky.

Tab. 13. Politika nastavení hesel.

Systémová hodnota	Doporučená nastavení
Zapamatovat historii hesla	4 poslední hesla.
Životnost hesla	Max. 90 dní.
Délka hesla	Min. 8 znaků (kombinace velkých a malých písmen, čísel, znaků).
Počet neúspěšných přihlášení	5
Délka zamknutí	Účet je uzamčen, odemknutí provede administrátor.

Předmětem normy ISO 27000 jsou i následující politiky, které se dále dělí na kategorie.

Systémová bezpečnostní politika: Řízení přístupu k síti

Cíl: Předcházet neautorizovanému přístupu k síťovým službám

- Kategorie: Politika užívání síťových služeb

Opatření: Uživatelé musí mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni.

- Kategorie: Autentizace uživatele externího připojení

Opatření: Přistup vzdálených uživatelů musí být autentizován.

- Kategorie: Identifikace zařízení v sítích

Opatření: Pro autentizaci připojení z vybraných lokalit a přenosných zařízení musí být zváženo použití automatické identifikace zařízení.

- Kategorie: Ochrana portů pro vzdálenou diagnostiku a konfiguraci

Opatření: Fyzický a logický přístup k diagnostickým a konfiguračním portům musí být bezpečně řízen.

- Kategorie: Princip oddělení v sítích

Opatření: Skupiny informačních služeb, uživatelů a informačních systémů musí být v sítích odděleny.

- Kategorie: Řízení síťových spojení

Opatření: U sdílených sítí, zejména těch, které přesahují hranice organizace, musí být omezeny možnosti připojení uživatelů. Omezení musí být v souladu s politikou řízení přístupů a s požadavky aplikací.

- Kategorie: Řízení směrování sítě

Opatření: Pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace, musí být zavedeno řízení směrování sítě.

5.3 Návrh bezpečné počítačové sítě

Návrh bezpečné počítačové sítě předpokládá dodržení standardů definovaných normami ISO27000 a 17799:2005. Základní standardy jsou definovány v následujících doporučeních.

5.3.1 Minimalizace útočného povrchu

Důležitým principem návrhu bezpečné sítě je minimalizace takzvaného útočného povrchu (attack surface) systému nebo sítě. Profil útočného povrchu se skládá z následujících prvků:

- protokoly běžící v síti nebo systému (TCP, UDP, další),
- otevřené porty odpovídající dané službě,
- síťová rozhraní, která odpovídají na dotazy,
- dostupné služby nebo přístupy,
- autentizace do systému, která je integrovanou součástí služby.

Součástí návrhu jsou doporučené standardní přístupy, protokoly a služby, jejímž použitím se sníží útočný povrch na minimum.

Tab. 14. Snížení útočného povrchu.

Služba	Síťové rozhraní	Protokol	Standardní porty
Vzdálený přístup – UNIX server	SSH – terminál	TCP	22
Vzdálený přístup – Windows server	RDP over SSL – vzdálená plocha	TCP	443
Vzdálený přístup – serverová konzole	HTTPS – RSA konzole	TCP	443
Vzdálený přístup – síťový prvek	SSH – terminál	TCP	22
Vzdálený přenos dat – UNIX server	SFTP, SCP	TCP	443
Vzdálený přenos dat – Windows server	SFTP, WINSCP	TCP	443
Vzdálený přenos dat – serverová konzole	Mapování virtuálních disků	TCP	443

Naopak nedodržením těchto doporučení se zvyšuje riziko útoku na systém nebo síť. Podle průzkumů jsou operační systémy Windows zastoupeny z devadesáti procent. Tento fakt

zvyšuje snahu útočníků proniknout právě do těchto systémů. V případě pozitivního průniku získávají přístup nad velkou částí systémů. [5]

Tab. 15. Zvýšení útočného povrchu.

Služba	Síťové rozhraní	Protokol	Standardní porty
Vzdálený přístup – UNIX server	TELNET – terminál	TCP	23
Vzdálený přístup – Windows server	RDP – vzdálená plocha	TCP	3389
Windows server	Windows File and Printer Sharing.	TCP/ UDP	139
Windows server	Windows NetBIOS	TCP/ UDP	135, 445, >1025
Vzdálený přístup – serverová konzole	HTTP – RSA konzole	TCP	80
Vzdálený přístup – síťový prvek	TELNET – terminál	TCP	23
Vzdálený přenos dat – UNIX server	FTP	TCP	21
Vzdálený přenos dat – Windows server	FTP	TCP	21
Vzdálený přenos dat – serverová konzole	Mapování virtuálních disků	TCP	80

5.3.2 Doporučení pro implementaci serverové bezpečnosti

Předpokladem vytvoření bezpečného serverového prostředí je dodržení bezpečnostních standardů a doporučení:

- používat serverové firewally, povolit jen aplikační porty, zakázat PERMIT ALL,
- nepřipojovat nové servery do produkční sítě, ale použít nejprve testovací síť,
- nepřipojovat systémy, které byly ve veřejné síti, do důvěryhodné vnitřní sítě,
- blokovat nepoužívané porty a vypnout nepotřebné služby (telnet, SMTP, FTP, Finger, Netstat, Systat, Chargen, Echo, DNS, RPC) [5]
- nepoužívat služby NetBIOS, Windows File and Printer Sharing,
- aktualizovat aplikační SW a implementovat záplaty pomocí Windows Update,
- používat aktualizovaný antivirový SW,
- používat bezpečnou verzi služeb využívající kryptovaný přenos (SFTP, SSH),
- používat silná hesla,
- monitorovat výkonnost systému a změny,
- používat HIDS nebo HIPS systémy pro kritické servery,
- zálohovat systémy.

Podle standardů definovaných v ISO 17799:2005 byla vytvořena tabulka doporučených síťových bezpečnostních nastavení pro servery.

Tab. 16. Standard ISO 17799 pro servery.

Systémová hodnota / Parametr	Popis	Doporučená hodnota
X-Windows access control	TCP/IP X-Windows	Je-li X-Windows service aktivní, přístup je řízen účtem.
REXD daemon	TCP/IP REXD	Musí být zakázán.

Adresáře pro Anonymous FTP přístup	TCP/IP Anonymous FTP	READ přístup nesmí být poskytnut do adresářů, které obsahují utajovaná data.
Nastavení oprávnění k adresářům přes Anonymous FTP	TCP/IP Anonymous FTP	Každý adresář může povolit přístup pro čtení či zápis anonymním uživatelům, ale ne obojí.
Proces řízení příjmu dat od Anonymous FTP	TCP/IP Anonymous FTP	Soubory, které byly uloženy do adresáře k zápisu, musí být kontrolovány (antivirová kontrola, kontrola nevhodného materiálu) před přesunem do adresáře povolujícího čtení.
Adresáře pro TFTP (Trivial File Transfer Protocol) přístup	TCP/IP Trivial FTP (TFTP)	Přístup přes TFTP je povolen pouze do adresářů s veřejnými daty.
ECHO, CHARGEN, FINGER, DISCARD, SYSTAT, DAYTIME, NETSTAT, WHO,	Denial of Service ochrana	Zakázat na všech serverech v zóně internet.

ECHO, CHARGEN, RSTATD, TFTP, RWALLD, RUSERD, DISCARD, DAYTIME, BOOTPS, FINGER, SPRAYD, PCNFSD, NETSTAT, RWHO, CMSD, DTSPCD, TTDBSERVER, Telnet, FTP	Denial of Service ochrana	Zakázat na všech aplikačních serverech, pokud to nevyžaduje aplikace.
SNMP služba	SNMP	Jméno komunity „public“ není povoleno, je-li SNMP aktivní
SNMP služba	SNMP	Jméno komunity „private“ není povoleno, je-li SNMP aktivní
HKLM\SYSTEM\ CurrentControlSet\Services \ Tcpip\Parameters\ (registry subkey)	Registry subkeys	Name: SynAttackProtect Type: REG_DWORD Value: a value of 1 is required

5.3.3 Doporučení pro implementaci síťové bezpečnosti

Předpokladem vytvoření bezpečné počítačové sítě je dodržení bezpečnostních standardů a doporučení na všech úrovních sítě:

- používat internetové a zónové firewally,
- rozdělit síť na segmenty a podsítě – vytvořit fyzickou izolaci na úrovni IP adres,

- vynucovat silná hesla,
- aktualizovat software a implementovat záplaty,
- šifrovat datové přenosy přes veřejné sítě,
- zmenšit útočný povrch (attack surface),
- omezit mobilní systémy a přenosná média – nepřipojovat USB média,
- zařízení připojovat nejprve do karantény.

Tab. 17. Standard ISO 17799 pro servery.

Systémová hodnota / Parametr	Popis	Doporučená hodnota
Individuální účty nebo autentikační servery		Používat TACACS+
SMNP Community jméno	SNMP v 3.0 zajišťuje silnější bezpečnostní mechanismy pro autentizaci	Použít SNMP v3
Community string délka	Kde není možné použít SNMP v3	Minimálně 8 znaků, mix písmen a znaků.
Kontrola přístupu	Kde není možné použít SNMP v3	Přes IP adresu
Privilegovaný mód	IOS	enable secret {password}
Heslo pro: • Console (con)	IOS	line con 0 password {password}
Heslo pro: • telnet ports (vty)	IOS	line {port} password {password} pro každou linku
System Access Logs	Authentication, Authorization and Access logs.	Use TACACS+

System Access Logs	IOS	LOGování úspěšných a neúspěšných pokusů, pokud zařízení nativně podporuje protokolování.
IOS System logs (Use a Log server to direct logs to.)	An IP address or a host name to the log server should be provided in the agreed to setting. Note: Cisco 1900 switches does not support logging.	logging {IP address}
Session timeout for: • Console (con) • telnet ports (vty)	Nesmí být nastaveno 0 0	Maximum 30 min.
Směrovač	Zakázat službu source routování	IP Source Routing musí být zakázán.
Směrovač, přepínač	Zakázat nepotřebné služby	Zakázat DHCP, HTTP, BOOTP server, Domain-lookup, finger, pad, CDP, ospf name-lookup
Směrovač, přepínač	Povolit důležité služby	service password-encryption ip classless ip subnet-zero
Síťové filtry	ACL filter	ACL musí být použito k omezení administrativního přístupu k zařízení.
Denial of Service ochrana	IOS	no service tcp-small-servers no service udp-small-servers

Upozornění	Business Use Notice	Příkaz Banner
Protokol pro administraci	Hesla používaná v ověřování autorizovaných userids nesmějí být přenášeny v clear text podobě přes internet, veřejné sítě, nebo bezdrátová zařízení.	Používat SSH přístup
Kryptování hesla	Heslo musí být kryptováno	Nejsilnější metoda pro Service password encryption

Podle standardů definovaných v ISO 17799:2005 byla vytvořena tabulka doporučených bezpečnostních nastavení pro síťová zařízení.

5.3.4 Bezpečný koncept přepínaní a směrování

Síťová bezpečnost nevychází jen z bezpečnostních požadavků. Hlavní význam je kladen i na funkční bezpečnost – spolehlivost, odolnost proti výpadkům síťových prvků a rychlou konvergenci sítě při výpadku. Síťové segmenty jsou od sebe odděleny směrovači, firewally nebo přepínači.

Doporučená implementace parametrů přepínání platná pro IOS verze 12.2:

- nepoužívat automatickou konfiguraci VLAN (DTP), manuálně definovat VLAN na jednotlivých rozhraních,

```
SW-ACC1(config)#interface range TenGigabitEthernet 1
SW-ACC1(config-if-range)#switchport mode trunk
SW-ACC1(config-if-range)#switchport nonegotiate
SW-ACC1(config-if-range)#switchport trunk native vlan 999
SW-ACC1(config-if-range)#switchport trunk allowed vlan 100,200
```

- používat VTP transparentní mód, směrovač přesto definovat do příslušné VTP domény včetně hesla,

```
SW-CORE1(config)#vtp domain DATACENTER
SW-CORE1(config)#vtp password D@tAC3nt!R
SW-CORE1(config)#vtp mode transparent
```

- používat algoritmus Rapid PVST+ pro rychlejší výpočet optimálních tras,

```
SW-ACC1(config)#spanning-tree mode rapid-pvst
```

- povolit BPDU Guard na portech určených pro koncové stanice,

```
SW-ACC1(config-if-range)#spanning-tree bpdu guard enable
```

- implementovat Root Guard na porty, které se nesmějí stát root porty,

```
SW-ACC1(config)#interface range TenGigabitEthernet 2
SW-ACC1(config-if-range)#spanning-tree guard root
```

- implementovat Loop Guard na všechny porty switche, které mohou být v *blocking* stavu, aby se zamezilo vytvoření smyčky po vypršení *max age time* času,

```
SW-ACC1(config)#interface range TenGigabitEthernet 2
SW-ACC1(config-if-range)#spanning-tree guard loop
```

- modifikovat priority STP pro preferované cesty a kořenové přepínače,

```
SW-CORE1(config)#spanning-tree vlan 100,200 priority 4096
```

- zakázat nepoužívané služby na VLAN rozhraních

```
SW-CORE1(config-if)#no ip redirects
SW-CORE1(config-if)#no ip unreachables
SW-CORE1(config-if)#no ip directed-broadcast
SW-CORE1(config-if)#no ip proxy-arp
SW-CORE1(config-if)#no ip mask-reply
SW-CORE1(config-if)#no cdp enable
```

- povolit služby na VLAN rozhraních

```
SW-CORE1(config-if)# ip route-cache policy
```

- příklad konfigurace fyzického portu, která eliminuje L2 zranitelnosti

```
interface GigabitEthernet0/1
switchport access vlan 100
switchport trunk native vlan 999
switchport mode access
switchport nonegotiate
switchport port-security
switchport port-security maximum 4
switchport port-security violation restrict
switchport port-security aging time 1
switchport port-security aging static
no ip address
no keepalive
no cdp enable
```

Přepínání mezi segmenty sítě na distribuční nebo core vrstvě probíhá mezi různými VLAN pomocí virtuálních rozhraní. Je doporučené implementovat ACL filtry nebo firewally mezi jednotlivé segmenty. Failover řeší protokol HSRP.

Doporučená implementace parametrů směrování:

- implementovat virtuální rozhraní pro jednotlivé VLAN na kořenovém přepínači,

```
SW-CORE1(config)#interface vlan 100
SW-CORE1(config)#ip address 192.168.100.2 255.255.255.0
```

- povolit směrování pouze na kořenovém přepínači,

```
SW-CORE1(config)#ip routing
```

- implementovat HSRP na každém virtuálním rozhraní, nastavit priority,

```
SW-CORE1(config)#interface vlan 100
SW-CORE1(config)#standby 100 IP address 192.168.100.1
```

```
SW-CORE1(config)#standby 100 priority 100
SW-CORE1(config)#standby 100 preempt
SW-CORE1(config)#standby 100 timers 5 10
SW-CORE1(config)#standby 100 authentication D@tAC3nt!R
```

- implementovat ACL filtry na jednotlivé VLAN na kořenovém přepínači.

```
SW-CORE1(config)#ip access-list extended IN-RRRRMMDD
SW-CORE1(config-ext-nacl)#deny ip any any fragments log-input
SW-CORE1(config-ext-nacl)# permit <protocol> <ip sa address> <ip sa mask> <sp/range #> <ip da address> <ip da mask> <dp/range #>
SW-CORE1(config-ext-nacl)# deny ip any any log-input
```

5.3.5 Implementace IP rozsahů

Pro účely datového centra dle stanovených podmínek jsou vyhovující privátní IP rozsahy a preferována je IP verze 4. V případě velkého datového centra, kde se předpokládá možná aplikace cloud prostředí pro více organizací, je vhodný IP adresní rozsah /8. Výhodou je možnost implementace až 256 prostředí třídy /16 – tedy 256 zákazníků menšího až středního rozsahu. Pro datové centrum, určené pouze pro jednu organizaci středního až většího rozsahu, je vhodný rozsah /12, který zřetelně oddělí např. jednotlivé divize až 16 adresami s rozsahem /16, a pro každou divizi zachová adresní prostor /16 s 256 VLAN. Malé organizace si vystačí s IP rozsahem /16 s maximálním počtem 256 logických segmentů (VLAN), z nichž každý disponuje 256 adresami. V rámci datového centra je vhodné využívat i kombinaci uvedených tříd pro oddělení logických bezpečnostních zón.

Tab. 18. Doporučená implementace IP rozsahů.

Kategorie	IP Třída – CIDR blok	Počet CIDR bloků	Počet dostupných VLAN y
Velké DC	A – 10.0.0.0 / 8 *Př.* **10**.x.y.z	256 (0~255) *Př.* 10.**100**.y,z	256 VLAN pro jeden blok *Př.* 10.100.**20**.z

Střední DC	B – 172.16.0.0 / 12 *Př.* **172.x**.y.z	16 (16~31) *Př.* 172.**25**.y,z	256 VLAN pro jeden blok *Př.* 172.25.**20**.z
Malé DC	C – 192.168.0.0 / 16 *Př.* 192.168.y.z	Nelze definovat blok.	256 VLAN (0~255) *Př.* 192.168.**20**.z

5.4 Návrh zónového uspořádání počítačové sítě

Privátní sítě jsou od veřejných sítí odděleny firewallem. Ten zajišťuje nejenom ochranu organizace, ale řeší směrování k hraničnímu BGP směrovači a dostupnost sítí pomocí překladu adres (NAT) směrem do veřejných sítí.

Nachází-li se organizace na více geografických místech, pak je nutné privátní síť rozprostřít i do těchto lokalit. To lze provést tunelováním přes veřejnou síť, nebo využitím vyhrazených WAN linek. Preferovanou variantou jsou vyhrazené linky, které jsou sice dražší než propojení přes veřejnou internetovou síť, ale poskytují garantovanou dostupnost služby, definovanou šířku pásma, propustnost a umožňují přenášet i jiné protokoly, které jinak nejsou kompatibilní se standardní internetovou sítí podporující pouze IP protokol. Tím hlavním důvodem však je, že poskytují organizaci vyšší ochranu oddělením sítě od veřejných sítí, u nichž je dle provedené analýzy střední riziko infiltrace komunikace.

Vyšší ochranu privátních sítí lze dosáhnout vytvořením fyzických síťových segmentů, které tvoří logické sítě podle požadované funkčnosti:

- segment pro aplikační servery pro produkci, vývoj a testování,
- segment pro internetové servery,
- segment pro VPN přístupové body,
- segment pro datové servery a úložiště,
- segment pro middleware a clustrové servery,
- segment pro web servery.

Každý z těchto segmentů má svoji bezpečnostní politiku.

Tab. 19. Segmentace privátní sítě.

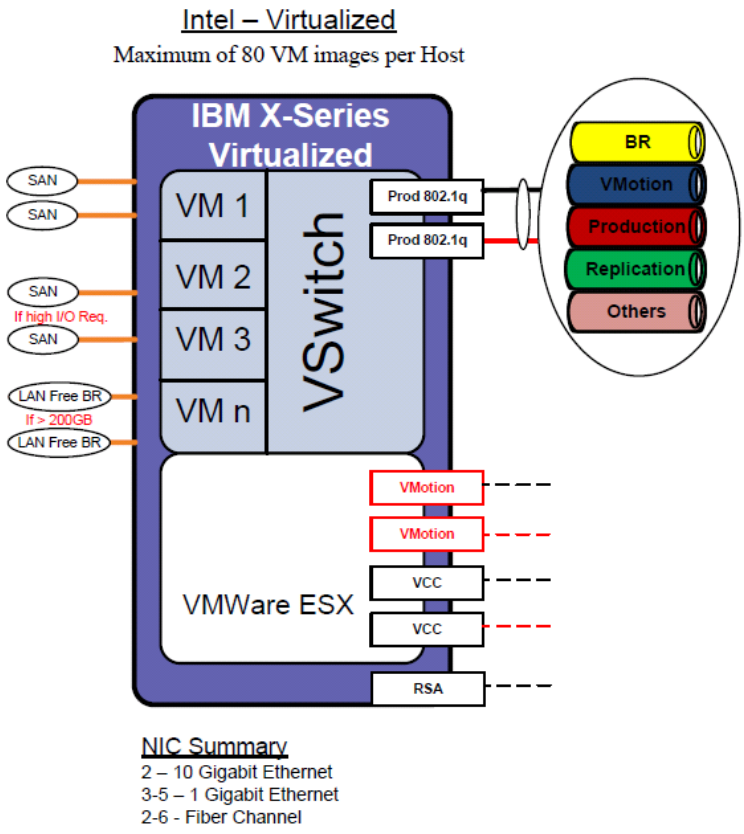
Segment	Typy serverů	Politika zóny
Aplikační servery	Produkce	Servery
	Vývoj	Servery
	Testování	Servery
Datové servery	SQL a Oracle servery	Data
Datová úložiště	Disková pole	Data
	Páskové knihovny	Data
Middleware servery	VMWare host	Servery
	Citrix servery	Servery
Prezentační servery	WEB servery pro aplikace	Intranet
	WEB servery pro intranet	Intranet
	WEB servery pro internet	DMZ
Internetové servery	Proxy server	DMZ
	Poštovní servery	DMZ
VPN přístupové body	VPN gateway	Internet
	VPN server	DMZ
WAN	Směrovače pro připojení vzdálených lokalit.	WAN
Interní síť	Pracovní stanice	Intranet
Administrace	Pracovní stanice	Management

Politika zóny vychází z bezpečnostních požadavků na příslušný segment sítě. Definuje systém technických opatření, režimové zásady a požadavky na implementaci.

Tab. 20. Definice zónové politiky.

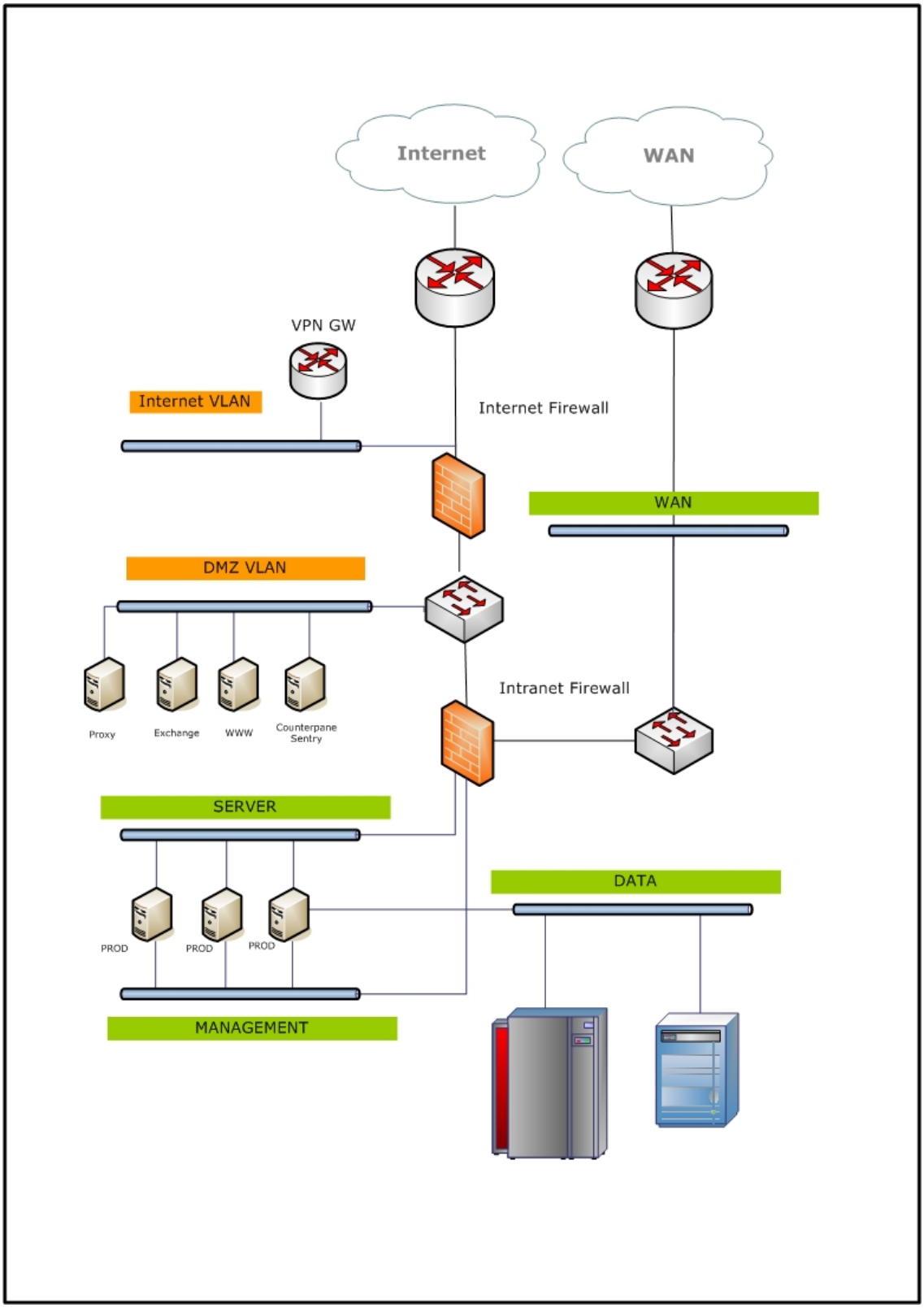
Politika zóny	Technická opatření	Režimové zásady
Interní síť (intranet)	Implementace VLAN, firewally mezi VLAN, směrování s ACL, Autentikace do sítě, mechanismus odpojení od sítě.	Oddělení logických segmentů, minimalizovat riziko vnitřního útoku. Silná autentikace. Monitorování všech protokolů přes IDS, vyhodnocování deviací.
Servery	Implementace VLAN, firewally mezi VLAN.	Oddělení segmentů pro produkci / vývoj / testování, otevřít jen potřebné TCP porty.
Data	Implementace jumbo paketů, vysokorychlostní ethernet.	Vyhrazený segment pouze pro přenos dat, přístupný jen ze serverů a oddělený od ostatních sítí.
DMZ	Sendvičová implementace mezi firewally, implementace NAT.	Vyhrazený segment pro inbound a outbound přístup do internetu pouze přes firewall.
Internet	Implementace směrovače a malého segmentu veřejných IP adres.	Vyhrazený segment pro přístup do internetu. Monitorování webových aktivit a tunelování.
WAN	Implementace směrovače, VPN tunelů, přímé směrování do VPN.	Použití silného kryptování ve VPN.
Management	Přístup SSH pro účely administrace serverů.	Použití silného kryptování pro SSH.

U fyzických serverů se předpokládá implementace více síťových adapterů, z nichž každý je připojen do příslušného VLAN segmentu. Pro virtuální servery se využívá architektura, která podporuje vytváření vnitřních virtuálních přepínačů a využití 802.1q trunk protokol k distribuci VLAN přes jeden fyzický adaptér. Segmenty jsou pak distribuovány uvnitř virtuálního přepínače k jednotlivým virtuálním adaptérům serveru. Tuto architekturu lze uplatnit u VMWare ESX serverů. Bezpečnost toho řešení je dostačující, dochází k fyzickému oddělení na úrovni VLAN uvnitř trunk adaptéru.



Obr. 6. Implementace VLAN ve virtuálním přepínači [24].

Finální návrh zohledňuje uvedené segmenty a politiky. Každý server je fyzicky i logicky připojen do tří nezávislých VLAN, které jsou od sebe odděleny firewallem. WAN připojení do vzdálených lokalit prochází rovněž přes firewall. Datový segment je zcela oddělený. Tím bylo dosaženo maximálního zvýšení bezpečnosti v části sítě, která je pro organizaci kritická.



Obr. 7. Logický design počítačové sítě.

6 FYZICKÝ DESIGN

Při návrhu a výstavbě datového centra je nutné uvažovat v delším časovém horizontu minimálně pěti let a velmi dobře plánovat. Neplánované změny generují vyšší náklady při navýšení příkonů, posílení klimatizace nebo instalaci většího počtu optických kabelů. Velikost, příkon a dispoziční členění DC se zásadně nerozhoduji na základě dnešního stavu infrastruktury, ale vždy je nutné popsat stav s výhledem minimálně na pět let. To souvisí se strategickým plánem organizace a správnou komunikací během přípravy projektu.

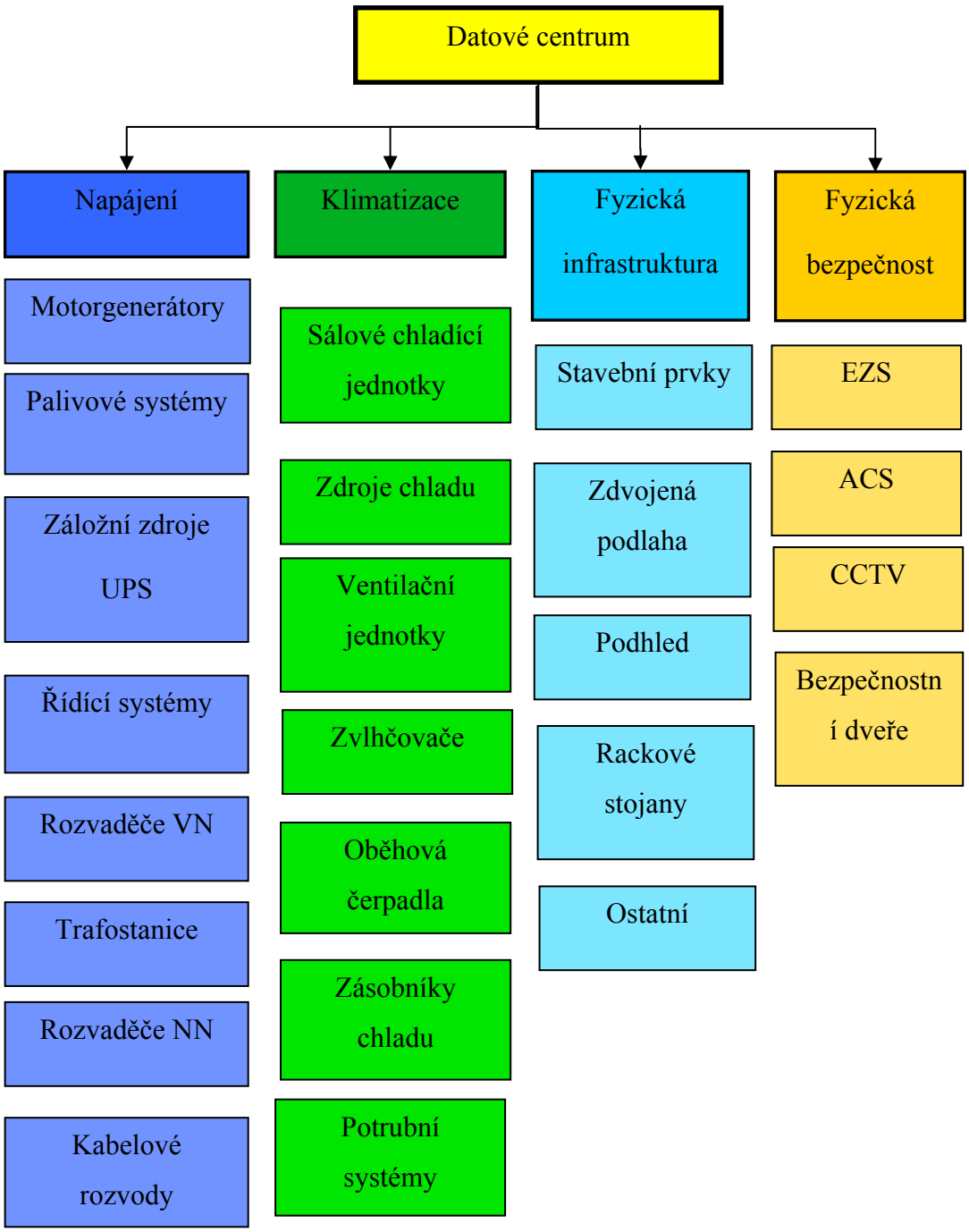
Při plánování systému je nutné si uvědomit, že jeden systém ovlivňuje druhý a vazby nejsou na první pohled jasné. Například populární zvyšování teploty vysoko nad 20 °C na vstupu do datových rozvaděčů sice umožní využití freecooling po delší období roku, a tak ušetřit energii na chlazení, ale zároveň se tím sníží životnost elektroniky a lze způsobit vyšší počet poruch. Je tedy vhodné ověřit požadované provozní podmínky zařízení a sladit je společně s návrhem chlazení. DC je nutné nejprve klasifikovat, do které Tier třídy bude patřit, a tomu přizpůsobit celý projekt. Některé parametry jsou pro provoz více a jiné méně podstatné, ale vyžaduje-li organizace certifikaci DC, důsledné dodržování všech parametrů pro zařazení do této třídy je nezbytné. Za vyšší klasifikaci platí zákazník vyšší nájem v případě hostingu. V případě organizace ta nemusí docenit vyšší třídu, ale zvýšení nákladů na vybudování a provoz může být enormní.

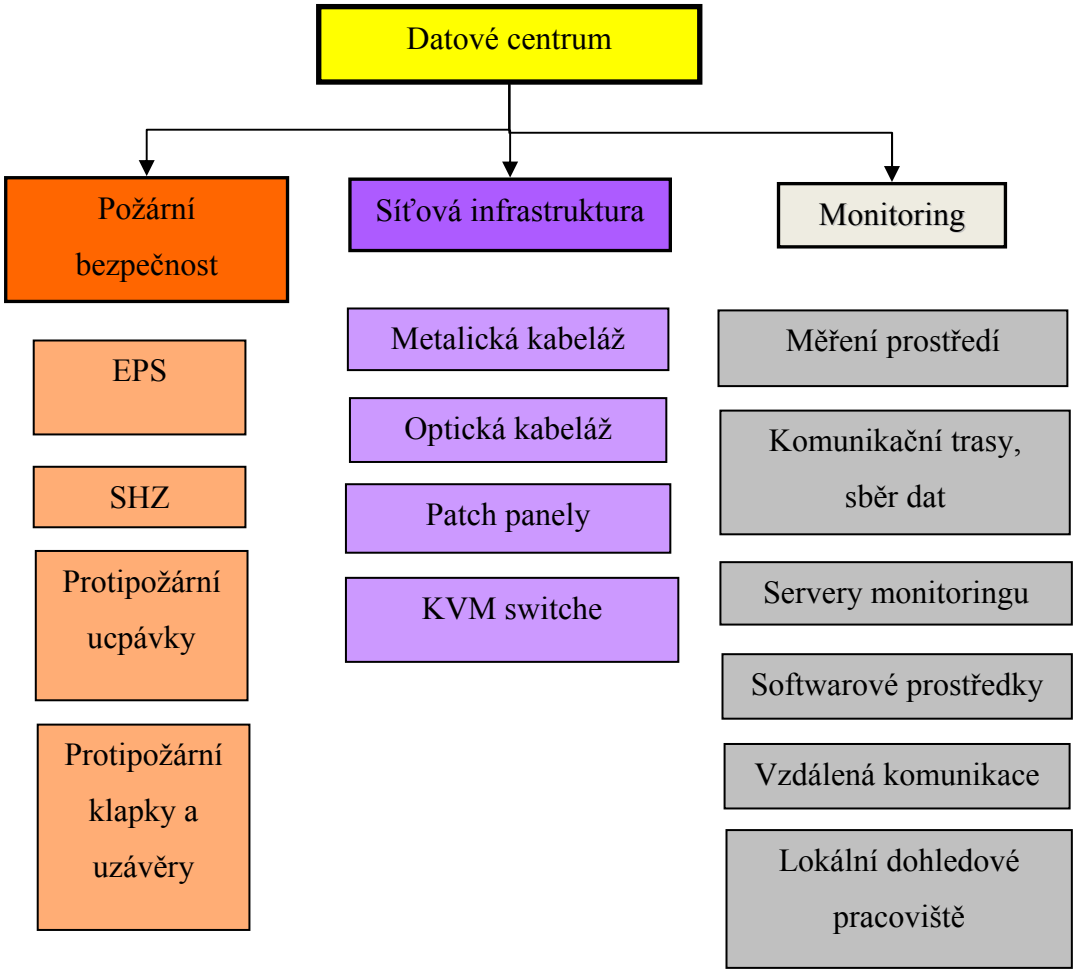
Podle nastavených výchozích parametrů je datové centrum samostatná budova, ve které se nachází zabezpečená oblast, určená pro zpracování citlivých dat organizace. Odpovídající kategorie je Tier III.

Návrh se zabývá následujícími oblastmi fyzického designu:

- fyzická bezpečnost a bezpečnost prostředí, mechanické prostředky,
- návrh zónového uspořádání datového centra,
- technické prostředky ochrany,
- režimová opatření,
- fyzický layout bezpečné počítačové sítě.

Systémy nezbytné pro provoz datového centra jsou uvedeny v následujícím grafickém přehledu.





6.1 Fyzická bezpečnost a bezpečnost prostředí

Cílem fyzické ochrany je zajistit ochranu aktiv organizace, ochranu zabezpečených oblastí proti jednotlivým hrozbám identifikovaným při analýze, a definovat patřičná protiopatření. Bezpečnost obecně by měla vycházet ze schváleného bezpečnostního projektu. Ten obsahuje stavební a konstrukční provedení budovy, technické prvky zabezpečení. Vlastní realizaci by měla předcházet předrealizační příprava, kdy se definují požadavky vyplývající z právních předpisů, závazných standardů, požadavků státních orgánů, pojišťoven, zadavatele, s ohledem na budoucí certifikaci podle norem ISO 27000.

V následujícím přehledu byla navržena opatření proti jednotlivým hrozbám.

Budova DC – hrozba teroristického útoku.

Opatřeni:

- Stavební konstrukce budovy musí být odolná proti hrozbě teroristického útoku. Teroristický útok je nejprve nutné definovat rozsahem a použitými prostředky, následně stavební konstrukci pláště dimenzovat proti tomuto útoku.
- Minimálním požadavkem je použití takové stavební konstrukce, která je odolná proti dostupným střelným zbraním a výbušným zbraním. Z toho vyplývá, že zcela nedostačující je ochrana serveroven, které by se nacházely v prosklených budovách nebo např. za sádrokartonovou stěnou. Železobetonová konstrukce je schopna odolávat ručním granátům nebo střelným zbraním. Pokud zadání obsahuje požadavek na odolnost proti pádu letadla, pak opatřením je vybudování datového centra v podzemních podlažích.
- Vyšší ochranu budovy lze dosáhnout zvýšenou perimetrickou ochranou. Posunutím perimetru do dostatečné vzdálenosti od budovy je vytvořena další překážka, jejíž překonání vyžaduje dodatečný čas a pomocí technických prostředků může být útočník včas odhalen. Pokud útočník nemá přímý přístup k budově, nemůže např. použít nástražný výbušný systém, který by dokázal zničit budovu. Použitím tohoto opatření lze snížit požadavky na odolnost konstrukce pláště.
- Zvýšenou ochranu je nutné věnovat kabelovým kanálům, datovým trasám a inženýrským sítím v případě sabotáže. Je nutné eliminovat riziko sabotáže umístěním těchto sítí do podzemních kanálů, šachet, které jsou skryté veřejnosti. Samozřejmostí je použití mechanických zábranných prostředků, aby neoprávněná osoba nemohla fyzicky vniknout např. šachtou do budovy. Doporučuje se použití EZS v těchto prostorách, pokud jsou odděleny od hlavní budovy.
- Zvláštní pozornost je potřeba věnovat umístění a stavebnímu provedení zásobníků paliva pro dieselové agregáty. V případně nadzemního umístění se zvyšuje riziko sabotáže, proto je nutné tyto zásobníky dostatečně chránit. Ideální je podzemní umístění.

Budova a zařízení DC – přírodní hrozby.

Opatřeni:

- Ochranu proti povodni, záplavám z přívalových dešťů a obecně poškození zařízení DC vodou, která by pronikla zvnějšku, lze minimalizovat nebo zcela eliminovat vhodným umístěním budovy mimo záplavové území.
- Riziko poškození vodou snížit stavebně konstrukčním provedením odvodnění, ochranou utěsněním budovy a instalací čerpadel. Je nutné instalovat zpětné klapky u kanalizace.
- Podlaha datového centra musí být dvojitá. Doporučuje se instalovat přívody kabelů NN shora. Datové nízkonapěťové a optické kabely lze vést i podlahou, doporučené jsou však horní kabelové kanály.

Obr. 8. Dvojitá podlaha a instalace kabelů.

- Ochrana proti blesku, vnějšímu požáru patří mezi standardní opatření dané bezpečnostním projektem stavby. Použité materiály a technologie musí dosahovat příslušné požární odolnosti.
- Poškození kabelových tras VN, datových tras a ostatních zařízení inženýrských sítí, v případě povodně nebo záplavy, je nutné eliminovat vodotěsným uložením. Umístění řídících, ovládacích zařízení, rozvaděčů NN, VN a trafostanic je nutné v bezpečné nadzemní výšce.

- Nebezpečím pro životní prostředí se stávají zásobníky paliva, proto je nutné dodržovat normy pro ochranu životního prostředí a zabránit průniku či průsaku paliva do spodních vod.

Obr. 9. Naftové hospodářství [14].

Fyzický bezpečnostní perimetr – hrozba sabotáže, útoku.

Opatření:

- Při ochraně prostor DC musí být používány bezpečnostní perimetry konstrukce s vysokou průlomovou odolností, aby poškození nebo zničení nebylo možné, nebo aby překonání překážky bylo časově náročné.
- Odolnost perimetru by měla být na podobné úrovni jako plášťová odolnost. Zcela nevyhovující je použití čtvercového, cyklónového nebo svařovaného pletiva. V případě DC, kdy je stanoven požadavek na odolnost proti průniku těžkým vozidlem, je vyhovujícím typem použití železobetonových stěn nebo zátaras, stěn z ocelových mřížových konstrukcí nebo kombinace.
- Dodatečným opatřením je použití terénních nerovností nebo betonových zátaras, které zabrání příjezdu vozidla do bezprostřední vzdálenosti perimetru.
- Pro přístup osob a příjezd vozidel do vnitřního prostoru za perimetrickou ochranou slouží turnikety a brány. Ty by se neměly stát slabým místem, proto musí být jejich konstrukční provedení přizpůsobenu celkové koncepci. Vjezdové brány by měly být vybaveny zdvojenou ochranou – použitím dodatečných zásuvných sloupů nebo sklopných zábranných systémů (hydraulických).

- Perimetr musí být dohlížen fyzickou ostrahou pomocí CCTV systémů, aby byly odhaleny útoky již ve fázi přípravy.
- Narušení perimetru musí být detekováno elektronickými systémy.

Budova a zařízení DC – hrozba výpadku napájení, nevyhovující kvality.

Charakteristika napětí a kvalita elektřiny se řídí energetickým zákonem 458/2000 Sb. a ČSN EN 50160. Pro některé charakteristiky napětí stanovuje norma pro odběrná místa z distribuční soustavy:

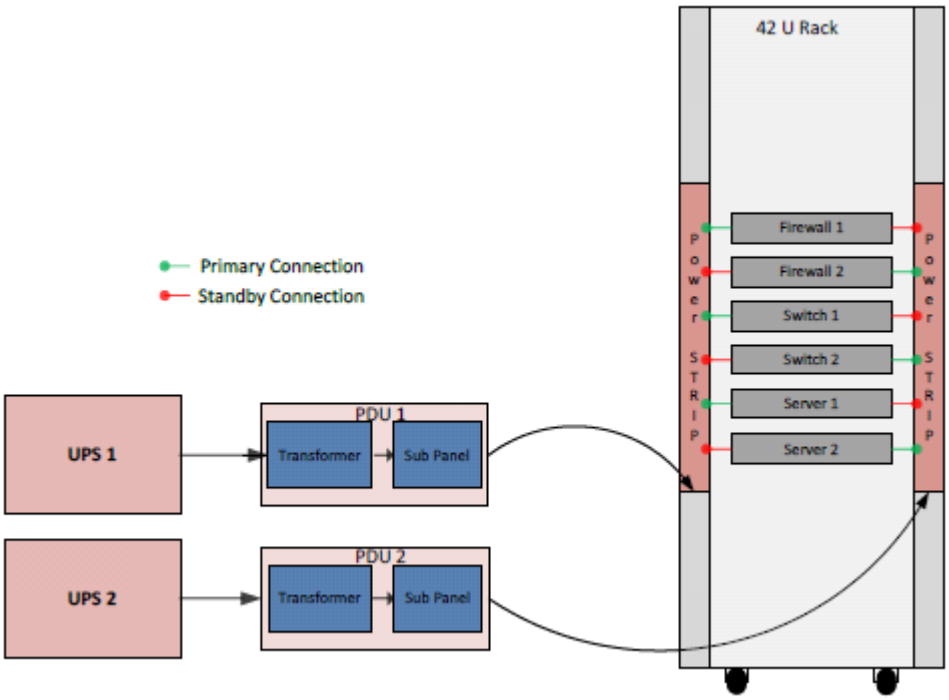
- zaručované hodnoty,
- měřicí intervaly,
- doby pozorování,
- mezní pravděpodobnosti splnění stanovených limitů.

Pro zbývající charakteristiky uvádí ČSN EN 50160 pouze informativní hodnoty:

- kmitočet sítě,
- velikost napájecího napětí,
- odchylky napájecího napětí,
- rychlé změny napětí,
- velikost rychlých změn napětí,
- krátkodobé poklesy napájecího napětí,
- krátkodobá přerušení napájecího napětí,
- dlouhodobá přerušení napájecího napětí,
- dočasná přepětí o síťovém kmitočtu mezi živými vodiči a zemí,
- přechodná přepětí mezi živými vodiči a zemí,
- nesymetrie napájecího napětí,
- harmonická napětí,
- meziharmonická napětí,
- úrovně napětí signálů v napájecím napětí.

Opatření:

- Výpadek napájení je kritický pro DC. Základní ochranou je zdvojení všech napájecích okruhů. DC musí být připojeno ke dvěma nezávislým přívodům VN 22kV s vlastní trafostanicí. Velmi malé DC lze připojit jen NN. Musí být zdvojeny rozvodny a rozvaděče NN kvůli možnosti požáru nebo poruchy.
- Je nutné správně stanovit požadavky na odběr z distribuční sítě, stanovit parametry dle normy ČSN EN 50160, a tyto parametry vyjednat smluvně s distributorem.
- Je doporučené provádět měření pomocí přenosných a zabudovaných analyzátorů kvality elektřiny.
- Každé zařízení v DC je připojeno na dva nezávislé okruhy.



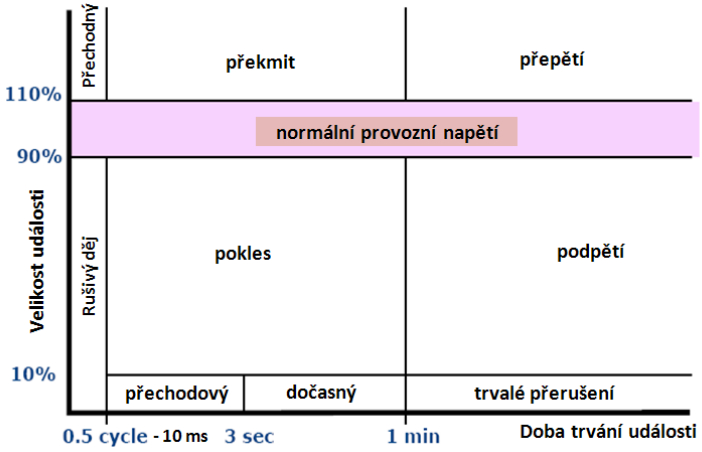
Obr. 10. Systém duálního napájení.

- Nemá-li zařízení dva napájecí zdroje, nesplňuje standard IET pro datové centrum. Lze však instalovat dynamické napájecí přepínače, které jsou připojeny ke dvěma okruhům, z nichž je pak dané zařízení napájeno.

- Pro případy blackoutu, kdy dochází k selhání veřejné energetické sítě, je nutné nainstalovat duální motorgenerátory požadovaného výkonu. Instalace MG podléhá stavebnímu zákonu, zákonu o ochraně ovzduší a zákonu o ochraně životního prostředí. V případě vnější instalace je nutná hluková studie.

Obr. 11. Motorgenerátor [14].

- Systémy UPS lze použít pouze při krátkodobém výpadku napájení. Systémy UPS v režimu on-line však zvyšují kvalitu napětí a regulují překmity, poklesy, přepětí a podpětí. Umístění akumulátorů by mělo být v prostředí se stálou teplotou (klimatizovaná místnost), tím se výrazně prodlouží doba zálohy.



Obr. 12. Provozní stavy napětí [25].

Obr. 13. Umístění baterií UPS [14].

Budova a zařízení DC – hrozba selhání komunikace.

Opatřeni:

- Instalovat duální datové a komunikační okruhy od nezávislých operátorů.

Prostory a zařízení DC – hrozba náhodných závad, SLA.

Opatření:

- Náhodné závady nelze zcela eliminovat. V souladu se standardy Tier III a Tier IV je nutné instalovat redundantní zařízení, která jsou navzájem propojena a poskytují vzájemnou zastupitelnost v době údržby nebo pro případ poruchy.
    - Pasivní paralelně redundantní systémy (standby redundant system) , kdy v provozu je pouze jedna část, ostatní zůstává v klidu do poruchy funkční části.
    - Aktivní paralelně redundantní systémy – všechny části pracují paralelně, Pure system (nesdílený, úplný) – při selhání jedné části se chybovost zbytku nezmění, Shared system (sdílený) – při selhání jedné části se chybovost zbytku zvýší.
- Instalovat zařízení, jejíchž dostupnost A je na požadované úrovni Tier datového centra. Každá komponenta s nižší hodnotou dostupnosti se stává kritickým místem v celém řetězci.

Tab. 21. Dostupnost A zařízení v DC [25].

Část, zařízení	Dostupnost **A**	**MTBF [h]**	**MTTR [h]**
Svorky	0,999999944	68975031	3,8
Jistič, stykač	0,999999121	2502878	2,2
PDU	0,99989974	1484737	297,4
Distribuční rozvaděč	0,99999881	2770328	3,1
STS	0,99989917	71701	7
Spotřebič 1 přívod	0,99969546	62353	19
Spotřebič 2 přívody	0,99999990	181323663	18
UPS	0,999968037	250288	8
DA	0,999845	55000	8
Síť (trafo, VN, NN)	0,999444	9000	5

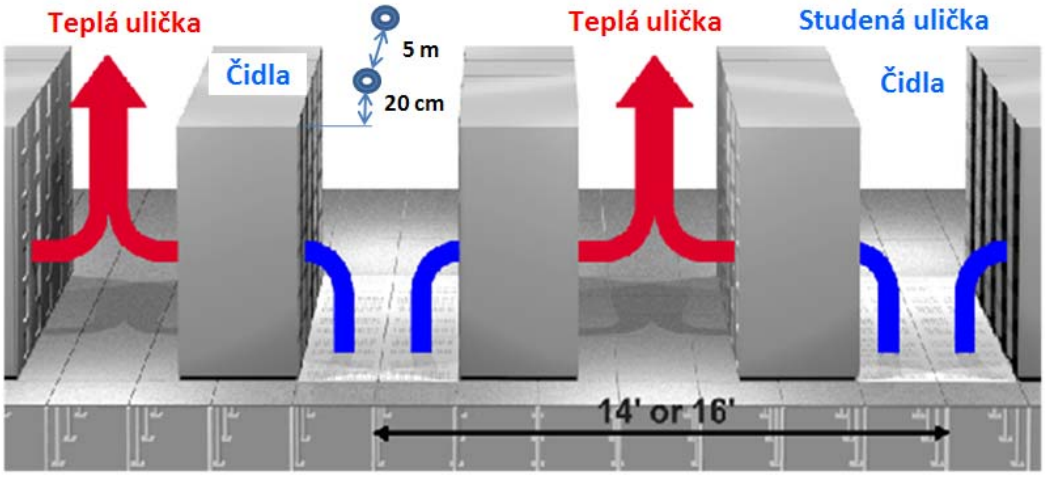
Prostory a zařízení DC – hrozba úmyslných závad

Opatření:

- Úmyslné závady je nutné zcela eliminovat. V souladu se standardy Tier instalovaná duální zařízení poskytují vzájemnou zastupitelnost v případě poruchy úmyslně způsobené.
- Je nutné přijmout taková fyzická opatření, aby se neautorizovaný personál nedostal k fyzickému zařízení a nemohl s ním neodborně nebo úmyslně manipulovat. Veškerá technologická zařízení (napájení, klimatizace, UPS) se musí nacházet v oddělených prostorách s omezeným přístupem.
- LAN a WAN komponenty, kabeláž a rozvody musí být v uzamykatelných rozvaděčích popřípadě v krytých kabelových trasách.
- V neposlední řadě je nutné stanovit a dodržovat režimová opatření, která zamezí pohybu neautorizovaných osob.

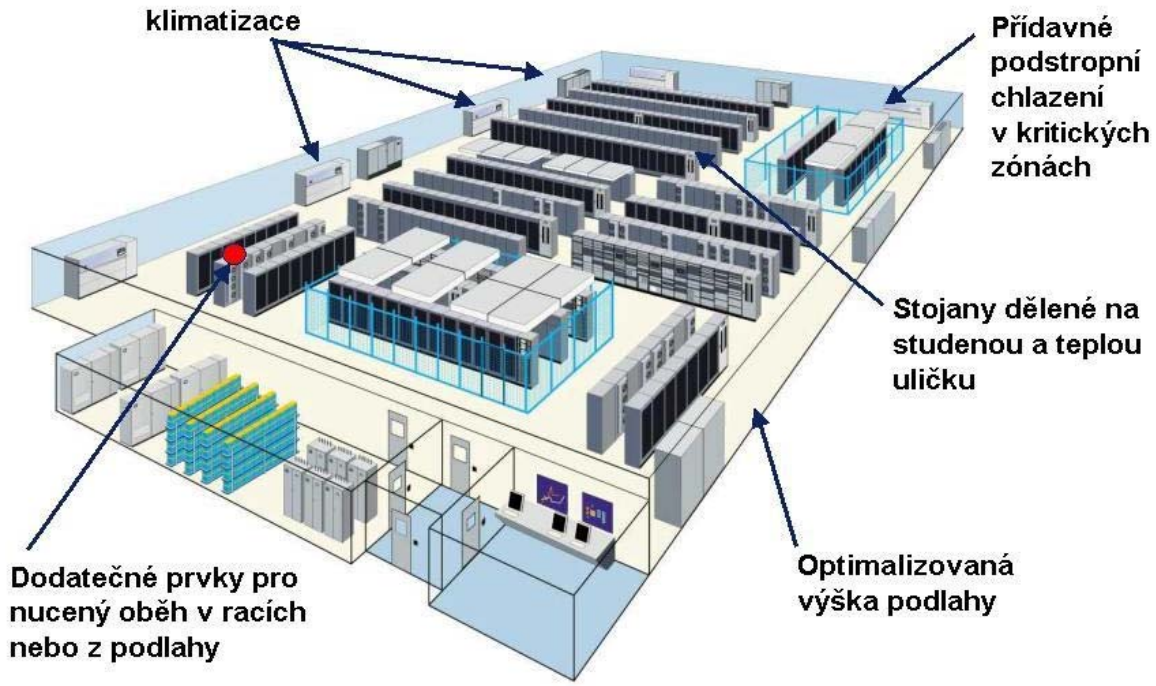
6.2 Klimatizace

Podle nejnovějších standardů na ekologická zelená datová centra je doporučen přechod od původního principu „studené místnosti“ k principu „teplá a studená ulička“. Klimatizační jednotky mají vyšší efektivitu při vyšším rozdílu teploty nasávaného a vyfukovaného vzduchu.



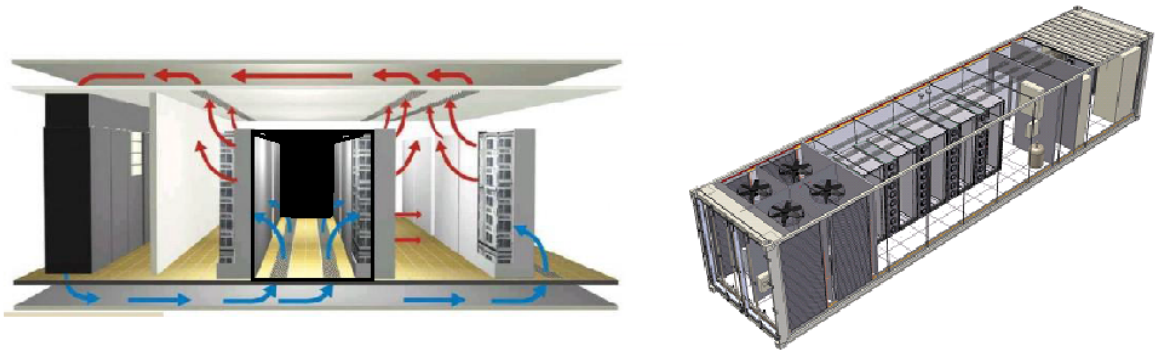
Obr. 14. Princip chlazení v DC [25].

Častou chybou je odkrývání čtverců v teplé uličce z důvodu vysoké teploty, což způsobí promísení teplého a studeného vzduchu a snížení teploty místnosti. Snížení rozdílu teplot zvyšuje výrazně spotřebu energie klimatizací. Pro sledování prostředí na datových sálech je důležité správné umístění čidel.



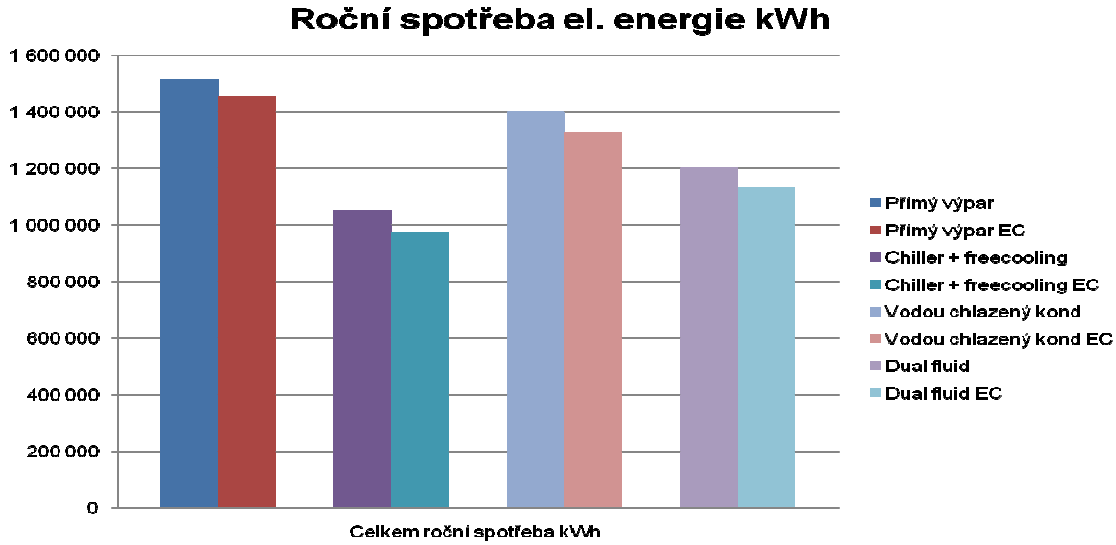
Obr. 15. Chlazení v klasickém DC [25].

Inovací v chlazení s cílem snížit spotřebu energie klimatizací jsou tzv. uzavřené studené uličky. Princip spočívá v hermetickém utěsnění chladné zóny, chladný vzduch prochází zařízením je vyháněn ventilátory do prostoru vně uličky. V místnosti pak dochází k minimálnímu míšení teplého a studeného vzduchu. Teplý vzduch z místnosti odchází stropními průduchy do oddělených klimatizačních sálů.



Obr. 16. Chlazení v uzavřené uličce [25].

Vhodná technologie chlazení závisí na klimatických podmínkách. Pro území ČR je nejvýhodnější nepřímý freecooling, využívající tzv. chladící věže (Chiller) a výměníku kapalina – vzduch.



Obr. 17. Energetická náročnost chlazení [25]

.

6.3 Návrh zónového uspořádání datového centra

Zónové uspořádání bylo definováno i v logickém designu, kde se týká vytvoření bezpečných segmentů sítě s cílem eliminovat nežádoucí přístup ze segmentu do segmentu. Stejná podstata je nutná v případě fyzického návrhu DC. Jde o vytvoření technologických, logických datových a bezpečnostních zón a stanovení režimových opatření. Z obr. 15 je patrné, že je nutné vybudovat několik oddělených technologických místností:

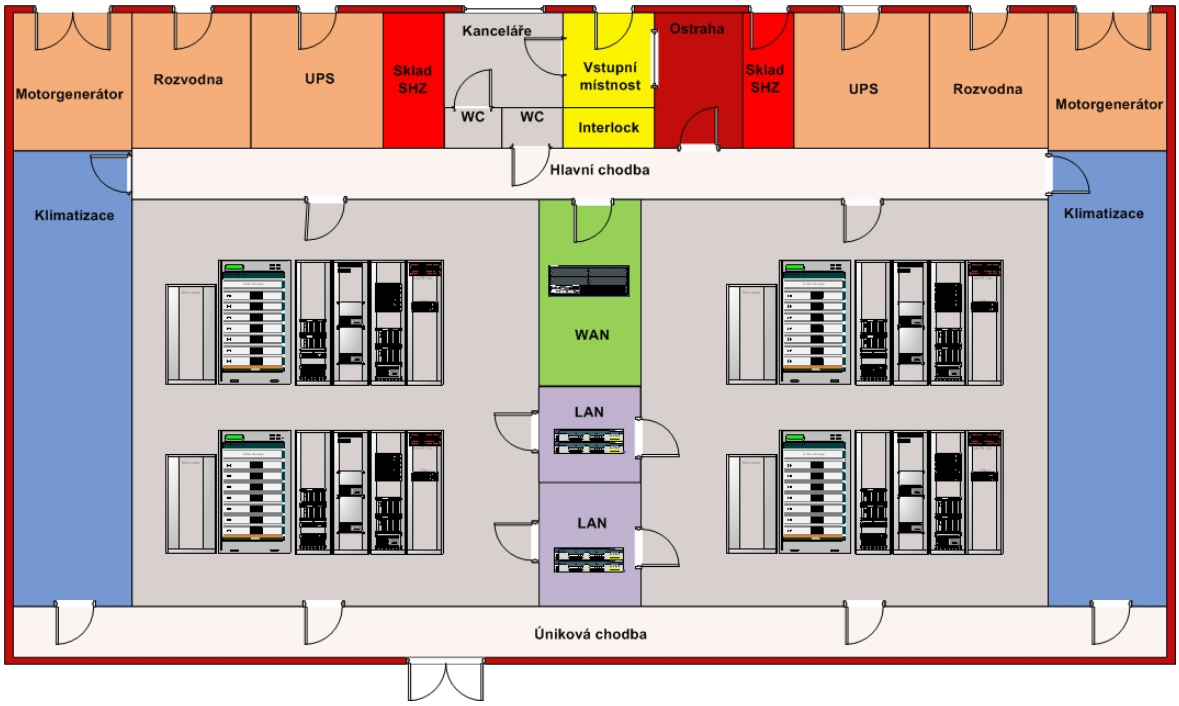
- trafostanice, rozvodny, místnosti s UPS,
- strojovna MG a sklad paliva,
- místnosti vzduchotechniky,
- místnost zabezpečovací techniky (EZS) a dohledové centrum ostrahy,
- místnost technologií pro EPS, SHZ,
- chodby, únikové chodby, výtahy, vstupní prostory, sklady.

Pro IT systémy je nutné vytvořit a od sebe oddělit:

- komunikační místnost určenou pouze pro WAN operátory,
- místnost určenou pro archivaci dat,
- místnost hlavního sálu DC pro umístění IT zařízení organizace nebo zákazníků.

Datová úložiště DS mohou být umístěna ve stejné místnosti jako servery. Je nutné však fyzicky oddělit zařízení pro archivaci dat (páskové knihovny, záložní DS), aby v případě požáru v jedné místnosti data zůstala zachována ve druhé. Případně lze zajistit uložení archivačních médii na úplně jiném místě nebo v trezoru.

Pro WAN operátory je určena samostatná místnost popř. část hlavního sálu, která však musí být fyzicky oddělena. Jedná se o opatření eliminace hrozby úmyslného poškození, neoprávněné manipulace se zařízením a logické infiltrace.



Obr. 18. Zónové uspořádání DC.

Stejné opatření lze aplikovat v hlavním sále DC, kde jednotlivé rozvaděče můžou být uzamčeny. Je nutné zavést klíčový režim nebo instalovat čtečky karet na každý rozvaděč.

Druhá varianta je fyzické umístění rozvaděčů do ohraničených prostorů (klecí), do kterých má přístup pouze zodpovědný personál. Toto řešení sebou přináší malou flexibilitu a mnohdy neefektivní využití plochy DC.

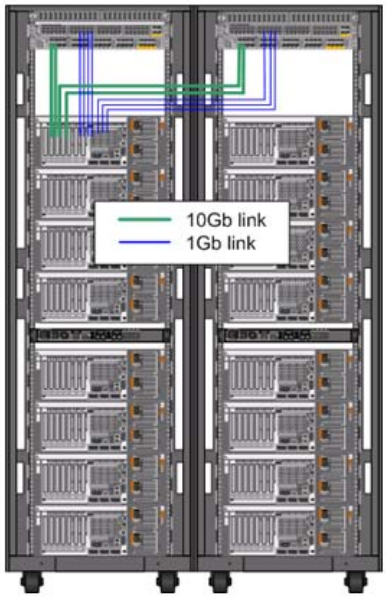
Racky pro umístění LAN technologií a racky s patch panely pro kabeláž musí být vždy uzamčeny, protože se jedná o kritickou část celé infrastruktury. Doporučuje se instalovat EZS (čidlo s magnetickým kontaktem) do těchto racků.

6.4 Kabeláž v DC

Návrh optické kabeláže vychází z rozměru sálu, vzdálenosti mezi LAN místností a nejvzdálenějším přípojným bodem, na použitém typu připojení serverů a umístění směrovačů. Při použití metalických kabelů kategorie 6e je maximální vzdálenost 100m a jsou-li rozměry DC menší, pak lze instalovat do každého serverového racku patch panel, který je vyveden do LAN místnosti. Servery jsou připojeny přímo do panelu, stejně jako porty směrovače. Tato metoda s sebou přináší riziko závad, protože fyzická trasa se skládá celkem ze tří kabelů a několika konektorů. Výhodou je však přehlednost, rychlé a jednoduché připojení serveru.

Doporučená a často používaná druhá metoda předpokládá natažení jednoho kabelu délky max. 100 metrů mezi server a směrovač. Tato metoda se využívá i pro optické kabely, kde je vzdálenost až 400m v případě použití MM kabelů a 10Gb připojení.

Větší DC (>100m) vyžadují instalaci směrovačů přístupové třetí vrstvy přímo v serverových rozvaděčích nebo v podružných LAN rozvaděčích umístěných přímo v serverovém sále. Tyto směrovače jsou pak připojeny k distribučním směrovačům, které se již nacházejí v LAN místnosti, optickým kabelem 10Gb. Doporučená instalace směrovačů je pak v horní části serverového racku.



Obr. 19. Instalace směrovačů Top of Rack.

Ethernet 10 Gb je aktuálně platným standardem pro vysokorychlostní propojení serverů. Je definováno několik standardních typů modulů pro optické a metalické spojení. Nejlevnější varianta je Twinax kabel.

Obr. 20. Twinax kabel pro 10 GbE.

6.5 Režimová opatření fyzické bezpečnosti

Se zónovým uspořádáním velmi úzce souvisí režimová opatření, která doplňují bezpečnostní opatření.

- Vstupem přes perimetr se osoba dostává do bezpečnostní zóny 0. Tento prostor je trvale monitorován a nadbytečný pohyb je nežádoucí. Z této zóny se lze dostat ke vstupním dveřím do budovy DC, nebo k rampě k naložení a vyložení nákladu.
- Vstup přes bránu perimetru je možný pouze na základě identifikace vstupující osoby – systém ACL, interkom.
- Vjezd vozidel do prostoru perimetru je povolen pouze za doprovodu ostrahy. Ostraha otevírá bránu, následně bránu zavírá a teprve potom deaktivuje sklopný zábranný systém, který umožní vozidlu pokračovat směrem k rampě. Zvláštním režimovým opatřením je, že vozidlo musí couvat.

Obr. 21. Situační schéma DC.

- Vstupní místnost je přístupná pouze na základě identifikace vstupující osoby – systém ACL.
- Vstupní místnost má klasifikaci bezpečnostní zóny 1. V této místnosti je prováděna fyzická kontrola osob, zda nepřenáší výbušniny, zbraně a jiné zakázané předměty a zda nevynáší z DC nepovolená média.
- Pracoviště ostrahy není z bezpečnostních důvodů přístupné ani zvenku, ani ze vstupní místnosti. Pracovník ostrahy vykonávající fyzickou kontrolu musí procházet interlockem.
- Prostor interlocku slouží k přístupu do druhé bezpečnostní zóny. Přístup přes interlock je povolen pouze jedné osobě. Kontrola je prováděna vážením osoby. Materiál ani zařízení nelze přenášet přes interlock. Povolený je pouze laptop do váhy 5 kg. Prostor interocku je trvale monitorován ostrahou.
- Osoba vyžadující dozor může projít přes interlock, ale nedostane se již do zóny 3, do které ji musí doprovodit osoba s oprávněním vstupu a provádějící dozor.
- Chodba se nachází v druhé bezpečnostní zóně, stejně jako prostory klimatizace.
- Prostory sálů jsou třetí bezpečnostní zóna. Jedna osoba může mít povolen přístup do sálů se servery a omezen přístup se záložními daty.
- Vstup do sálů je pouze přes hlavní chodbu. Z každého sálu vede úniková cesta směrem k únikové chodbě. Únikovou cestu a chodbu lze využít jen v případě požáru.
- Úniková chodba slouží zároveň jako prostor k transportu zařízení a materiálu z rampy do prostoru datového centra. Zařízení, které je dopraveno do prostor únikové chodby, zde může zůstat po nezbytnou dobu, přičemž pohyb osob je v tomto prostoru zakázán. Dveře jsou blokovány a nelze otevřít dveře na rampu a zároveň dveře do sálu. Dveře do sálu nelze otevřít ani v případě, je-li zaznamenán pohyb osob v únikové chodbě. Osoby mohou vyzvednout zařízení nebo materiál pouze v případě, že vstupují ze sálu do chodby, a to za přítomnosti ostrahy.
- Prostor pro nakládku a vykládku (rampa) je monitorován. Pohyb materiálu směrem do vnitřních prostor je pod trvalým dohledem ostrahy.

- Technické energetické místnosti jsou přístupné pouze z vnějšku budovy, není nutné propojení s vnitřními prostory. Tím je usnadněno zásobování, technická kontrola a údržba, popřípadě zásah hasičů v případě požáru.
- Energetické místnosti jsou přístupné zvenku, ale je nutné použít ID karty pro identifikaci osob a zároveň použít klíč, jinak nelze bezpečnostní dveře otevřít. Toto opatření neplatí v případě požáru.
- Manipulaci s klíči provádí ostraha. Ostraha vydává klíče přes okýnko ze vstupní místnosti.
- Prostory klimatizací jsou přístupné pouze z vnitřních prostor, jelikož se nacházejí v hermeticky uzavřeném prostoru DC.
- Prostory kanceláře jsou přístupné pouze ze vstupního prostoru.
- Technický personál WAN operátorů má přístup pouze do WAN místnosti. Propojení WAN racků s LAN je pomocí optický patch panelů, proto není nutné, aby měli přístup do LAN místností.
- LAN místnost lze obsluhovat z obou sálů DC. Přístup je omezen pouze pro síťové administrátory.
- Prostory hlavních sálů jsou přístupné pouze administrátorům serverů. Sály jsou fyzicky oddělené z důvodu instalace odlišných zařízení. Např. aplikační servery se nacházejí v levém sále, ale záložní data se nacházejí v pravém sále. Je nutné dodržovat toto fyzické oddělení pro případ požáru v jednom ze sálů.

Kategorie: Kontrola vstupu osob

- ACL systém na vstupu přes perimetr do zóny 1. Každá osoba musí mít ID kartu.
- ACL systém pro přístup do zóny 1 – vstupní místnost. Zde dochází k fyzické kontrole osoby ostrahou. Pokud je osoba identická s osobou na ID kartě, je povolen přístup do interlocku. Ostraha povoluje vstup do interlocku.
- Ostraha po ověření vydává bezpečnostní klíče od technologických místností.
- Vstup přes interlock je řízen pouze systémem ACL a ostraha nemá oprávnění tento systém deaktivovat. Ostraha může otevřít dveře pouze směrem ven, nikoliv dovnitř.

Ostraha však autorizuje přístup přes první dveře interlocku, bez autorizace je ID karta odmítnuta.

- Vstup ze zóny 2 (chodba) do sálů je již řízen systémem ACL. Aby bylo zabráněno průchodu dvou osob současně, jsou vstupní dveře monitorovány systémem CCTV. Porušení tohoto pravidla je sankcionováno.

Ostraha objektu – kategorie Tier 3 – klasifikace dat „přísně tajné“:

- Nejméně 2 osoby v objektu 24 hodin.
- Jedna osoba musí vždy zůstat v prostorách velínu ostrahy!
- Jedna osoba zajišťuje činnosti ve vstupní místnosti – provádí fyzickou kontrolu vstupujících osob, řeší technické problémy s přístupem resp. zasahuje v případě alarmu uvnitř budovy.
- Denní provoz vyžaduje zvýšenou obsluhu u vjezdové brány a rampy – 1 vyhrazená osoba.
- V případě požadavku na přístup osoby vyžadující dozor nebo při zvýšeném pohybu osob uvnitř DC je nutné povolat dodatečnou osobu.

6.6 Technické prostředky fyzické bezpečnosti

Technické prostředky fyzické bezpečnosti jsou předmětem samostatných projektů a subdodávek infrastruktury datového centra. Zásady návrhu, všeobecné požadavky a normy, jsou popsány v teoretické části práce. Praktické návrhy protiopatření byly uvedeny v 6.1. Tato část je zaměřena na kompaktní shrnutí a upřesnění požadavků s ohledem na identifikovaná rizika.

MZS obvodové:

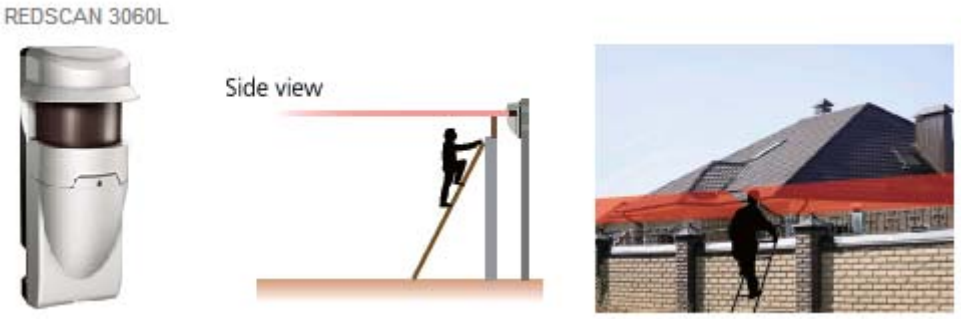
- Železobetonová obvodová stěna, betonové zátarasy, terénní nerovnosti.
- Vstupní turniket s ACL kontrolou vstupu, doplněný interkomem s kamerou.
- Vjezdová brána se sklopným zábranným systémem, doplněná interkomem s kamerou.

MZS plášťové:

- Bezpečnostní dveře do technologických místností, celokovové, s hydraulickým otevíráním a zavíráním, se speciálními zámky, odjištění klíčem a ID kartou, mechanismem nouzového mechanického otevření v případě požáru.
- Bezpečnostní dveře u rampy, celokovové, odjištění ID kartou, mechanismem nouzového mechanického odblokování v případě požáru.
- Prosklení z místnosti ostrahy a kanceláře – bezpečnostní tvrzené sklo Connex (nerozbitné, neprůstřelné), tloušťky 3 x 8 mm, se speciální folií mezi skly.
- Bezpečnostní mříže u všech průlezných otvorů – průduchy vzduchotechniky na střeše, datové kanály, kanály inženýrských sítí.

Technické prostředky PZS:

- PZS pro stupeň zabezpečení 4.
- Laserové detektory perimetrické ochrany (Optex RLS-3060L) nebo infračervené závory.



Obr. 22. Laserový detektor Optex[17]

- Detektory otevření u všech dveří technologických místností, dveří v zóně 2 a 3. ID karta aktivuje a deaktivuje alarm. Alarm je deaktivovaný v případě přítomnosti jedné osoby uvnitř zóny. ID kartu je nutné použít i při opuštění zóny, kdy dojde k aktivaci alarmu.
- Detektory pohybu PIR u průchodů inženýrských sítí a vzduchotechniky.

- Laserové detektory nebo infra závory v podhledech a dvojitých podlahách, pokud nejsou stavebně zajištění proti průlezu.
- Prostorová ochrana chodeb, sálů, technologických místností použitím kombinovaných PIR/MW detektorů. Zvláštní režim je nastaven u nouzového východu a rampy.
- Magnetické kontakty u racků vyvolají alarm v případě neoprávněného otevření. Deaktivace ID kartou nebo klávesnice a PIN.
- Systém SAS u ostrahy obsluhující vjezdovou bránu a rampu. Je nutné počítat s variantou, že vjížděné vozidlo a osoba je útočník nebo terorista.

Technické prostředky CCTV:

- CCTV systém perimetrické ochrany / ostrahy s integrovanou detekcí pohybu. Přehledové kamery vnějšího prostoru.
- Detailní kamery sledování vstupů, vjezdů.
- Přehledové kamery na chodbách a sálech.

Technické prostředky ACS:

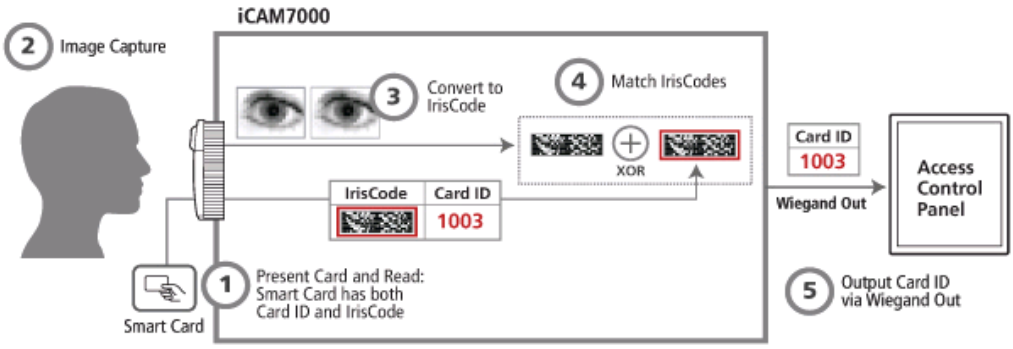
- Vstup přes turniket perimetru a do zóny 1 autentikací ID kartou,
- Vstup do zóny 2 autentikací ID kartou + PIN nebo biometrická data.
- Vstup do zóny 3 autentikací ID kartou. Dohled detailní kamerou.

Povolení pro přístup do datového centra nelze získat v prostorách DC. Je nutné vytvořit elektronickou žádost, kterou schvaluje organizace. Následně je povolen přístup do jednotlivých zón. Bez tohoto povolení se osoba nemůže dostat ani přes vstupní turniket perimetru.

Součástí procesu získání povolení se doporučuje vytvoření profilu žadatele. Ten obsahuje osobní údaje, váhu, fotografii obličeje, biometrické údaje typu tvar obličeje, scan oka nebo očního pozadí.

Pro biometrickou identifikaci lze použít systém společnosti IrisID, iCAM7000 nebo iCAM7010.

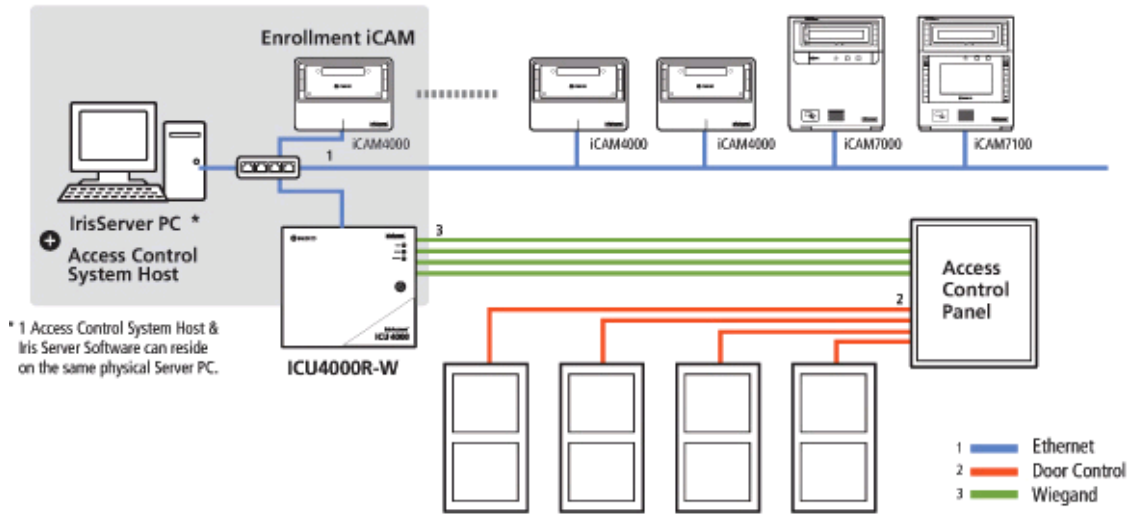
Obr. 23. Biometrický oční skener[16].



Obr. 24. Princip skeneru [16.]

Systém se skládá z následujících komponent:

- počítač se SW pro skenování a vytváření profilu žadatele,
- ústředna ICU4000R-W se sběrnicí Wiegand,
- dveřní ovládací modul,
- oční skener kombinovaný s čtečkou ID karet.



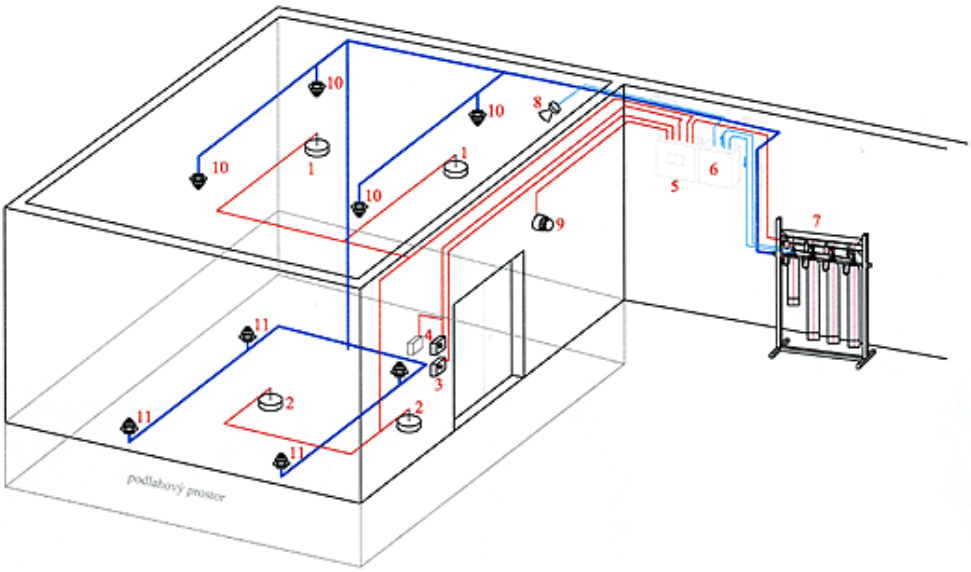
Obr. 25. Systém IrisID iCAM7000 [16].

Technické prostředky PZS:

- Nutné jsou oddělené požární zóny, certifikované dveře, průchodky, certifikovaný EPS a SHZ systém.

Obr. 26. Plynové SHZ FM200[14].

- Doporučené hašení pro prostory DC je plynem, který umožní rychle obnovit provoz a nezkrátí životnost IT technologie. Použít lze CO_2, dusík, argon nebo směsi plynů.
- Požadavkem je hermetické uzavření prostor, instalace uzavíracích klapek vzduchotechniky a poplachový systém, který upozorní osoby uvnitř DC k okamžitému opuštění prostor.
- SHZ se skládá z následujících komponentů:



Obr. 27. Komponenty SHZ [15].

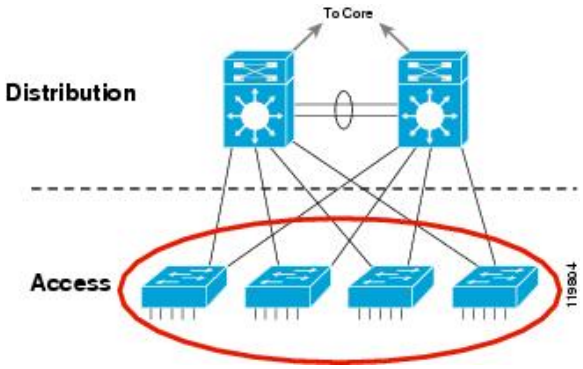
Tab. 22. Komponenty SHZ [15].

1	Automatický hlásič požáru – stropní
2	Automatický hlásič požáru – podlažní
3	STOP tlačítko
4	Tlačítkový spínač – spínač SHZ
5	Centrála EPS / SHZ – eventuálně hasicí jednotka
6	Zpožďovací zařízení
7	Baterie s láhví hasiva
8	Plynová houkačka

9	Houkačka/kombinovaná houkačka/záblesková světla
10	Hasicí trysky / hrdla – strop
11	Hasicí trysky / hrdla – podlaha

6.7 Fyzický design bezpečné počítačové sítě

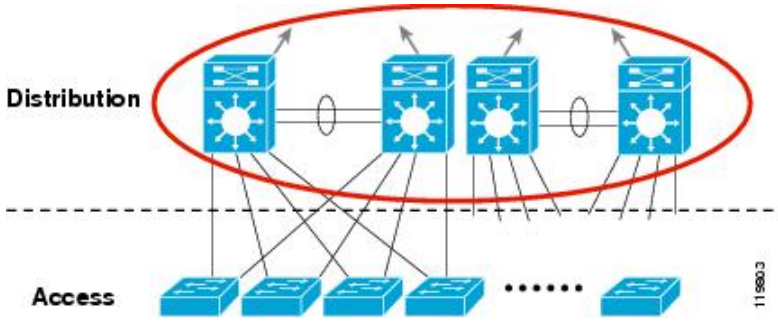
Doporučená fyzická topologie vychází ze standardního třívrstvého modelu. Primární funkcí přístupového vrstvy je poskytnout přístup koncovému uživateli sítě – serverům. Tato vrstva provádí přepínání, propojuje logické layer-2 broadcast domény a poskytuje fyzickou izolaci skupinám uživatelů, aplikací a serverů. Výhodou je vysoká kapacita portů a nízká cena těchto přepínačů. Doporučená zařízení jsou Cisco řady 3700, 4900 nebo Nexus 2200.



Obr. 28. Přístupová vrstva [18].

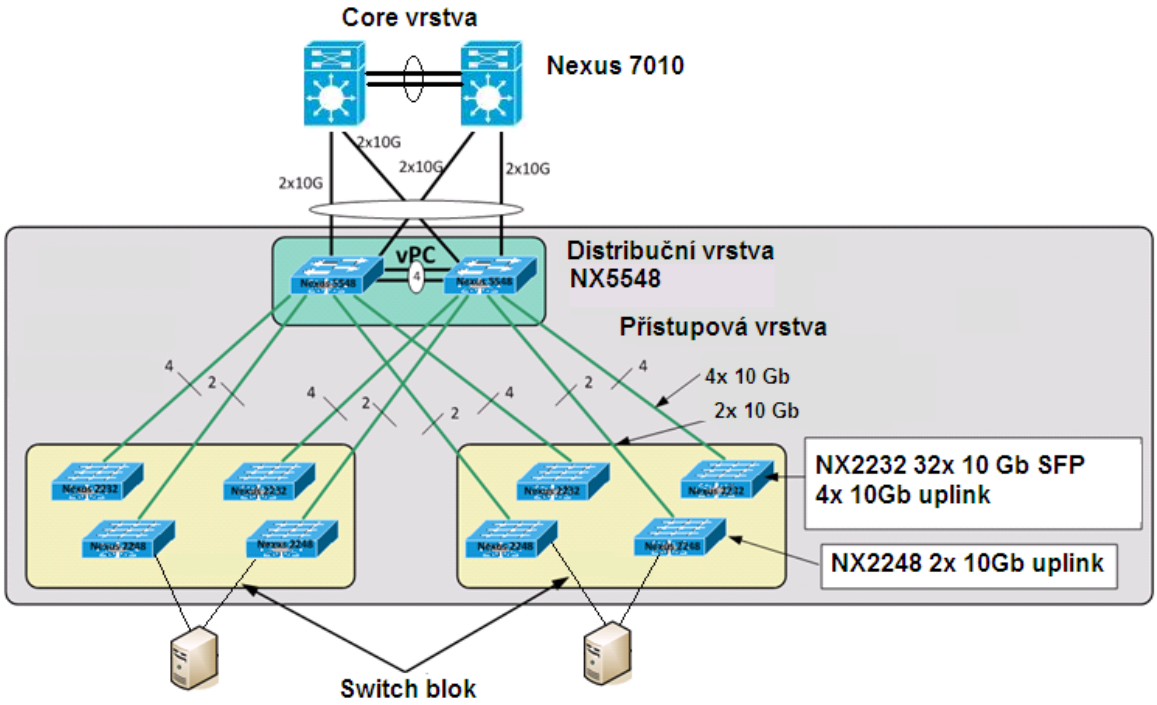
Agregace přístupové vrstvy probíhá v distribuční vrstvě. Podmínkou je velká propustnost sběrnice zařízení, vysoká přepínací rychlost, možnost implementace virtuálních přepínačů (Cisco VSS) nebo virtuálních port-channelů (Cisco vPC). Primárním cílem distribuční vrstvy je zajistit rychlou, bezvýpadkovou komunikaci mezi servery v rámci VLAN rozprostřené přes více přístupových přepínačů. Distribuční a přístupové přepínače spolu tvoří fyzický celek, tzv. switchblok. Doporučená zařízení jsou Cisco řady 5500, 6500 nebo Nexus 5500.

Core vrstva se využívá ke směrování mezi VLAN, k implementaci firewallů, ACL a směrování do WAN a internetu. Core vrstva musí mít stejnou výkonnost jako distribuční vrstva, proto se mnohdy používají stejné typy zařízení jako v distribuční vrstvě. Plní však jinou funkci než je prostá distribuce, tvoří jádro celé sítě. Doporučená zařízení jsou Cisco 6500 nebo Nexus 7000.



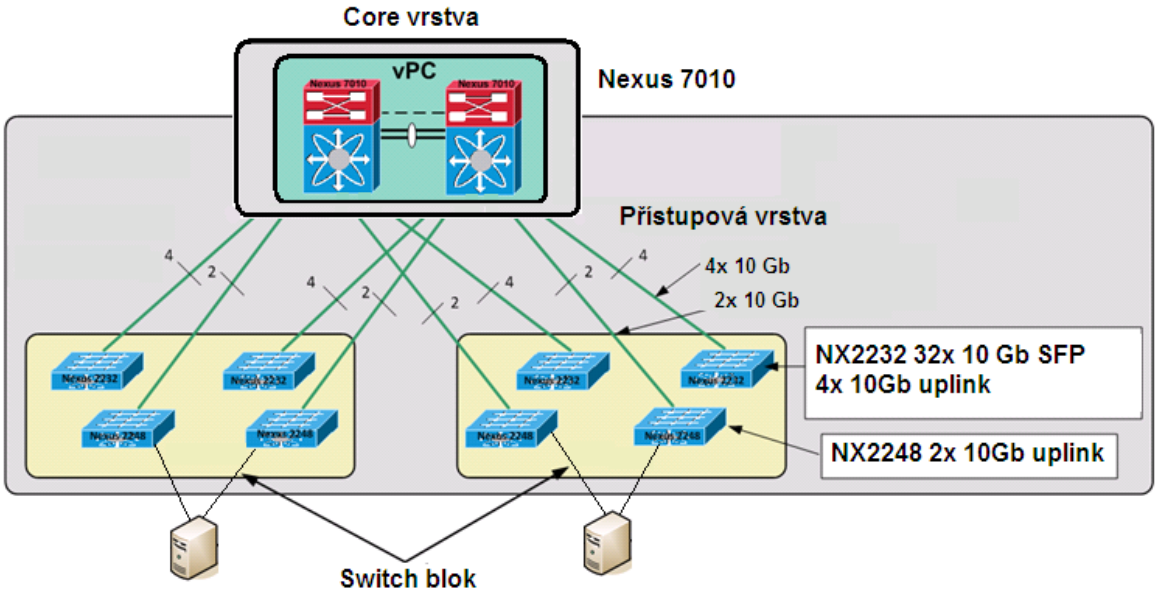
Obr. 29. Distribuční vrstva [18].

Switchblok se skládá ze dvou typů přepínačů – NX2232 pro 10 Gb a NX2248 pro 1 Gb porty. Toto je nejefektivnější varianta. Zařízení, které kombinuje oba typy portů, je finančně nevýhodné – jednalo by se o modulární NX5548.



Obr. 30. Návrh 3-vrstvého modelu.

U menšího DC je možné vyloučit distribuční vrstvu a nahradit ji core vrstvou. Z pohledu výkonnosti ani logických funkcí to nebude mít negativní dopad, zredukuje se však možný počet switchbloků a výrazně se omezí možnost budoucího růstu sítě. Uvedený L3 návrh zobrazuje 24 potřebných 10 Gb uplink portů pro dva switchbloky. Kapacita jednoho core přepínače NX7010 je maximálně 256 portů. Ke dvěma NX7010 pak můžeme připojit max. 20 switchbloků, pokud vypustíme distribuční vrstvu. Vzniklý 2vrstvý model je stále dostačující pro stanovené podmínky Tier III datového centra, protože poskytuje redundanci a failover architekturu.



Obr. 31. Návrh 2-vrstvého modelu.

7 SYSTÉM KONTROLY BEZPEČNOSTI

Zvýšení bezpečnosti počítačové sítě, kromě výše uvedených fyzických a logických opatření, lze dosáhnout implementací systémů aktivní ochrany:

- aktivní ochranou datových toků pomocí systému detekce narušení (IDS a IPS),
- aktivním preventivním prováděním kontroly zranitelností (Vulnerability scanning).

Automatická detekce je tedy nedílnou součástí celé bezpečnostní koncepce a návrhu moderní počítačové sítě.

7.1 Návrh systému IDS a IPS

Návrh řešení by měl vycházet z aktuálních a dostupných produktů. Architektura a produkty Cisco, popisované v doporučené literatuře, jsou již zastaralé – jednalo se o architekturu SAFE Blueprint nebo mikroanalytický server hrozeb TAME. Jediné dostupné informace lze proto najít na webových stránkách výrobců. Orientace v produktech není snadná, vzhledem k velkému množství produktů. Jedná se o náročný proces vyžadující technickému porozumění dané problematice. Návrh by měl vycházet z analýzy produktů.

7.2 Analýza produktů

Analýzy produktů se zaměřila na produkty dvou výrobců – Cisco a IBM. Obě firmy nabízejí řady zařízení pro malé, střední, velké organizace nebo datová centra. Pro účely DC navrhované kategorie Tier III lze použít pouze modelovou řadu Enterprise.

IBM Security Network IPS Throughput Metrics

	Remote	Perimeter			Core		10GbE Core
Model	GX4004-v2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
Inspected Throughput	200Mb	800Mb	1.5Gb	2.5Gb	4Gb	8Gb	23Gb+
Protection Interfaces	4 x 1G	4 x 1G	8 x 1G	8 x 1G	8 x 1G	16 x 1G	8 x 10G

Obr. 32. IPS zařízení firmy IBM [26].

Small Office and Branch Office | Internet Edge | **Enterprise Data Center**

Cisco ASA firewalls protect networks of all shapes and sizes, with consistent security across hybrid infrastructures — physical, virtual, and cloud. These solutions combine the most deployed firewall in the industry with a full complement of next-generation network security services. They protect corporate networks while providing employees with secure access to data — anytime, anywhere, using any device.

Read more about the Cisco ASA firewalls for large enterprises and data centers.

Cisco ASA Model	ASA 5585-X with SSP10	ASA 5585-X with SSP20	ASA 5585-X with SSP40	ASA 5585-X with SSP60	ASA Services Module
					
Stateful Inspection throughput (max[1])	4 Gbps	10 Gbps	20 Gbps	40 Gbps	20 Gbps
Stateful Inspection throughput (multiprotocol[2])	2 Gbps	5 Gbps	10 Gbps	20 Gbps	16 Gbps
Next-Generation throughput[3] (multiprotocol)	2 Gbps (with ASA CX SSP-10)	5 Gbps (with ASA CX SSP-20)	9 Gbps (with ASA CX SSP-40)	13 Gbps (with ASA CX SSP-60)	Not available
IPS throughput[4] (multiprotocol)	2 Gbps (with IPS SSP-10)	3 Gbps (with IPS SSP-20)	5 Gbps (with IPS SSP-40)	10 Gbps (with IPS SSP-60)	Not available
Concurrent sessions	1,000,000	2,000,000	4,000,000	10,000,000	10,000,000
Connections per second	50,000	125,000	200,000	350,000	300,000
Packets per second (64 byte)	1,500,000	3,000,000	5,000,000	9,000,000	5,000,000
3DES/AES VPN throughput[5]	1 Gbps	2 Gbps	3 Gbps	5 Gbps	2 Gbps

Obr. 33. IPS zařízení firmy Cisco [19].

Analýza porovnává nabízené funkce a technické parametry u vybraných zařízení nejvyšší kategorie. Klíčový parametr srovnání výkonnosti je propustnost paketové stavové inspekce modulu IPS. Oba navrhované modely nabízejí stejnou funkcionalitu. Samozřejmostí je failover architektura, která umožňuje ze dvou HW boxů vytvořit jeden redundantní. Výsledky srovnání jsou uvedeny v následující tabulce.

IBM GX7800

Cisco ASA 5585-X IPS

Obr. 34. Analyzované IPS zařízení.

Tab.23. Srovnání IPS produktů Cisco a IBM.

Hodnotící parametr	IBM model GX7800	Cisco ASA 5585-X IPS SSP-60
Funkce	IPS, IDS	IPS, IDS
Propustnost paketové inspekce IPS	20 Gbps	10 Gbps
Počet rozhraní	16x 10GbE SFP	8x 10 GbE SFP 16x 1GbE TX
Velikost	3U	2U
Počet virtuálních IDS/IPS politik	4096	4 senzory, každý 1020 politik
Počet monitorovaných portů IDS mód	16	8x 10 GbE SFP 12x 1 GbE
Počet monitorovaných portů IPS mód	8	4
Vulnerability detekce	ANO	ANO
Detekce protokolové anomálie	ANO	ANO

Detekce tunelování	ANO	ANO
Detekce nestandardních portů	ANO	ANO
DoS detekce	ANO	ANO
DoS prevence	ANO	ANO
Detekce stavových paketů	ANO	ANO
Počet síťových a aplikačních protokolů	313	neomezeno
Uživatelsky definované signatury	ANO	ANO
Kopírování předdefinovaných signatur	ANO	ANO
Orientační cena	230 000 $	170 000 $

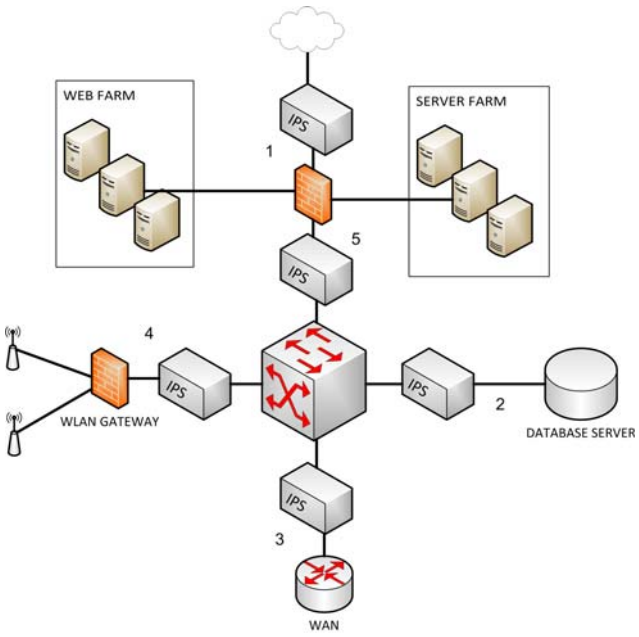
Závěr srovnání:

Zásadní rozdíl je ve výkonnosti a v celkovém počtu portů. Neméně významný údaj je parametr celkového počtu portů, které lze využít pro inspekci IPS. Z porovnání těchto klíčových parametrů vychází produkt IBM jako vhodnější a lepší. Srovnání cenové není relevantní vzhledem k výkonovým rozdílům.

7.3 Návrh topologie

Návrh je postaven na nové technologii IPS, která do značné míry zahrnuje funkcionalitu systému IDS. Hlavní odlišnost IPS od IDS spočívá v tom, že systém negeneruje pouze výstrahu. Technologie IPS zcela změnila způsob umístění systémů detekce narušení, způsob jak zachycuje a analyzuje pakety, přesnost detekce, konečný výsledek a způsob použití nástroje.

IPS je umístěn ve stejné linii jako firewall, všechny pakety musí projít tímto zařízením. IPS detekuje stav relace, není omezen na jednosměrné toky, může blokovat provoz téměř v reálném čase v případě potřeby. Snížil se počet falešně negativních a falešně pozitivních detekcí, konfigurace a ladění systému jsou mnohem jednodušší a efektivnější. Protože většina nových řešení IPS je postavena na platformě vyhrazených HW zařízení, které mají nízkou latenci, vysokou výkonnost a minimální dopad na propustnost a výkonnost sítě, nedochází již k narušení (zpomalení) komunikace jako tomu bylo dříve. V případě poruchy má většina systémů IPS zaveden systém provozu bypass, který umožňuje přeposílat veškerý provoz, pokud senzor nefunguje správně. Návrh implementace IPS předpokládá architekturu založenou na síti – tedy síťového IPS.



Obr. 35. Obecné schéma síťového IPS [23].

Standardní návrh umístění IDS a IPS systému vychází ze zónového uspořádání sítě a je zaměřen na následující segmenty:

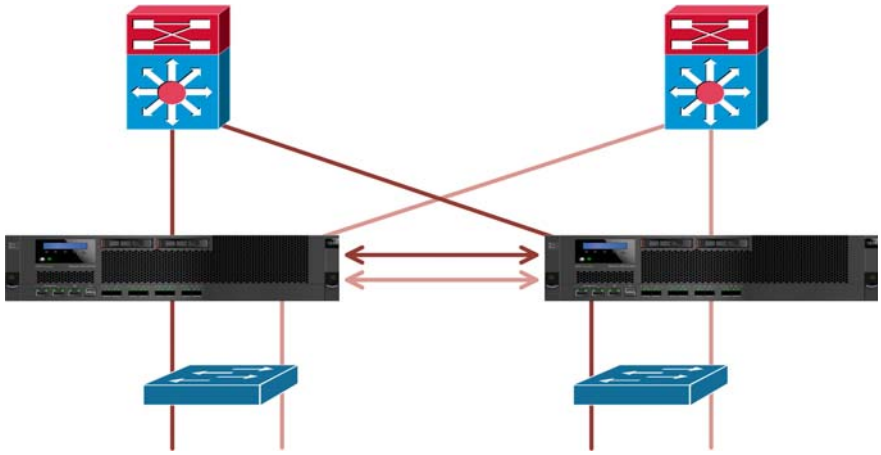
- přístupová linka do internetu – systém IDS nebo IPS,
- segment vzdáleného přístupu VPN a DMZ – systém IPS,
- linka připojení hlavních sítí LAN (směrem do serverové zóny) – systém IPS.

Detekce útoků směrem z internetu zahrnuje rozmístění IDS senzoru vně firewallu, aby zaznamenával útočné pokusy. Předpokladem je, že síťový perimetr (internetový firewall) je bezpečný a detekce útoků se bude zaznamenávat pouze pro účely stanovení bezpečnostních hrozeb a analýzy útočných typů. Nevýhodou zmíněného nastavení je, že produkuje velké množství logovacích souborů. Naproti tomu umístění IPS je nutné uvnitř sítě za síťový perimetr a provedení automatizované odezvy v případě pozitivního útoku, pokud by prošel přes síťový perimetr.

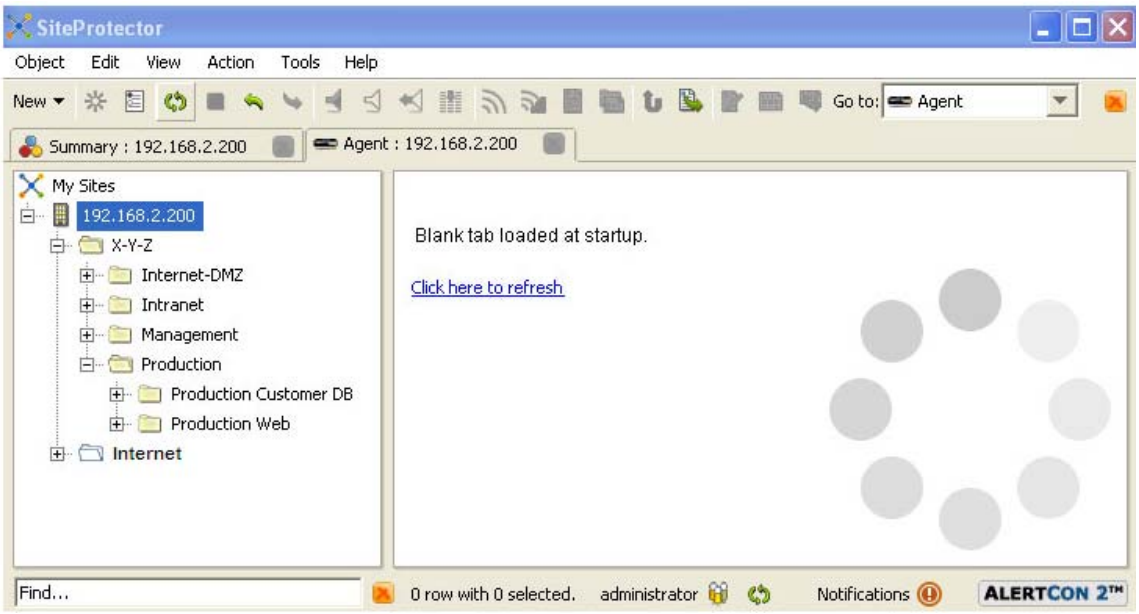
Kombinace IDS, IPS vně a uvnitř perimetru je klíčové a umožňuje porovnávat všeobecné útoky s aktivní ochranou firewallu a vnitřním systémem IPS. Nevýhodou řešení je finanční náročnost a požadavek na vytvoření expertního týmu incidentní odezvy.

Naopak levnější varianta, umístění IPS systému pouze do vnitřní části za perimetr, je více automatická a může ji obsluhovat jeden administrátor. Nevýhodou jsou omezené informace, které má k dispozici, což se může negativně projevit v případě cílených, opakovaných útoků.

Fyzický design předpokládá instalaci dvou IBM GX7800 zařízení v clusteru, které dokáží vytvořit až 8 oddělených logických segmentů (2 fyzické porty pro segment). Každý segment má jeden příchozí a jeden odchozí port.

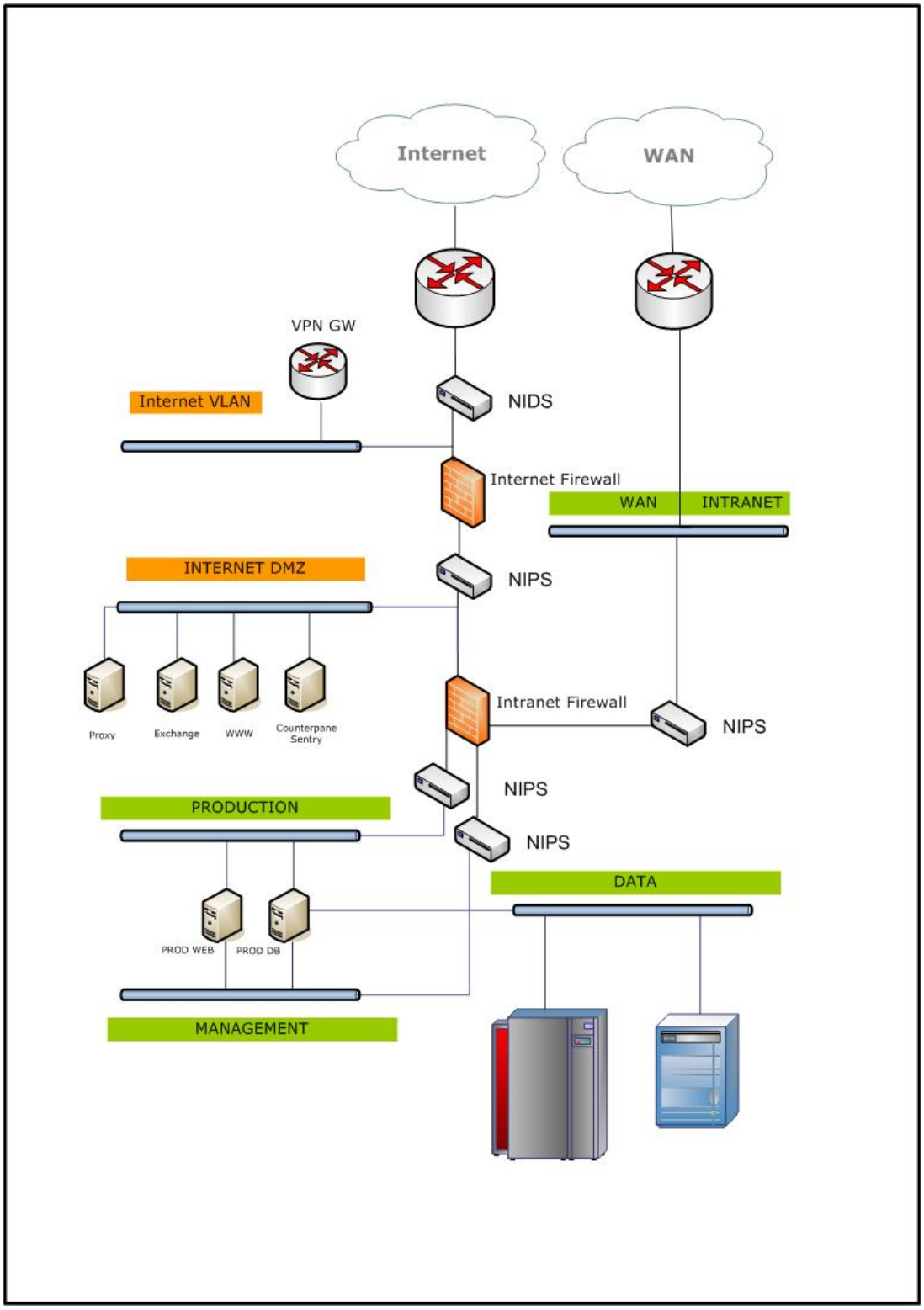


Obr. 36. Fyzické zapojení IPS [26].



Obr. 37. Konfigurace segmentů IPS [26].

Logický design respektuje doporučení a navrhuje celkem 4 logické jednotky IPS a jednu IDS vně perimetru. IPS vytváří 4 oddělené segmenty (site) – produkce, management, intranet a DMZ. IDS vytváří 1 segment internet. Celkem je nutné vytvořit 5 segmentů, čemuž odpovídá 10 fyzických portů GX7800.



Obr. 38. Logický design implementace IPS.

7.4 Konfigurace odezev IPS systému

Automatizované odezvy se odehrávají automaticky po detekování specifické události. V systému IPS je možné nastavit anebo revidovat pravidla pro automatizované odezvy.

Možné typy nastavení automatizovaných odezev:

- Zrušení spojení (Canceling) – zahrnuje ukončení veškeré komunikace na portu, pokud útok vyhovuje specifickému řetězci známého útoku. Bude však ovlivněn pouze jednotlivý uzel a útočník může zaútočit na jiný.
- Přiškrcení (Throttling) – technika, která se používá proti skenování portů. Přidává zpoždění do odezvy na toto skenování, a když frekvence uvedené činnosti narůstá, úměrně tomu se prodlužuje i zpoždění. Mnoho skenerů spoléhá na časování a toto přidané zpoždění může přerušit většinu skriptem řízených skenů.
- Vyhýbání se (Shunning) – je proces identifikace útočníka a odepření jakéhokoliv síťového přístupu nebo služby útočícímu systému. Falešná detekce znamená, že pomocí útoků s předstíranou IP adresou může útočník účelově zablokovat legitimní služby.
- Odstřelení relace (Reset) – se používá, když je detekována útočná signatura. IPS vyšle falšovaně nastavený reset bit na oba konce aktuálního spojení, vyrovnávací paměť bude vyprázdněna a spojení ukončeno.

Ruční odezvy jsou druhou variantou odezev. Každý útok je jiný a administrátor IPS vyhodnocuje proměnné, které nemají automatizované odezvy v sobě integrovány. IDS a IPS technologie vyžadují lidskou reakci vzhledem k tomu, že tyto nemůžou být nikdy dokonalé. Aby byl možné provádět manuální odezvu na incident, je zapotřebí mít platnou metodologii a tým, který je součástí procesu incidentní odezvy.

Proces manuální incidentní odezvy se skládá z následujících kroků:

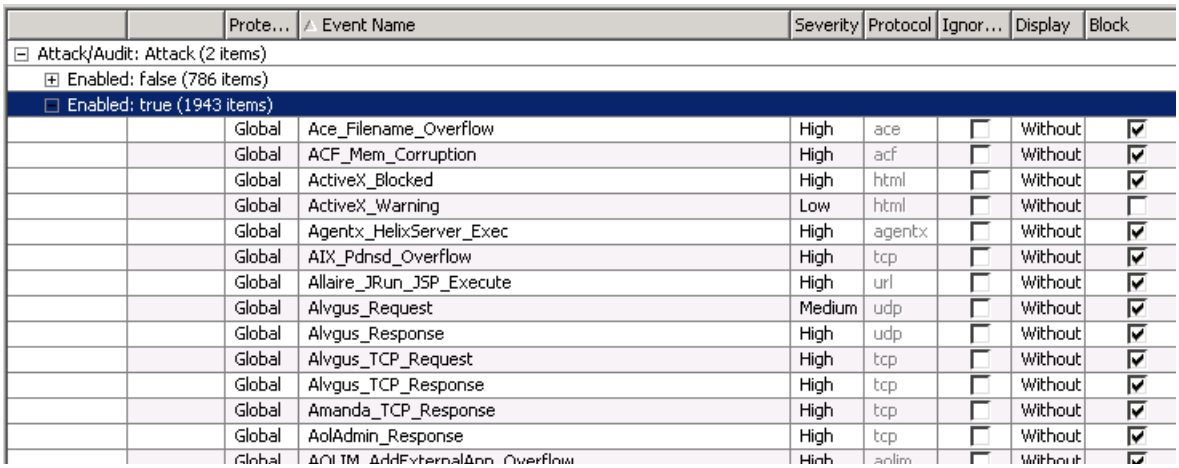
- provedení kvantitativní analýzy rizik – hodnocení napadených aktiv, pravděpodobnosti útoku, ztráty v případě útoku a ocenění rizika,
- návrhu metodologie,
- vytvoření týmu odezvy, který bude tuto metodologii praktikovat.

Návrh metodologie incidentní odezvy:

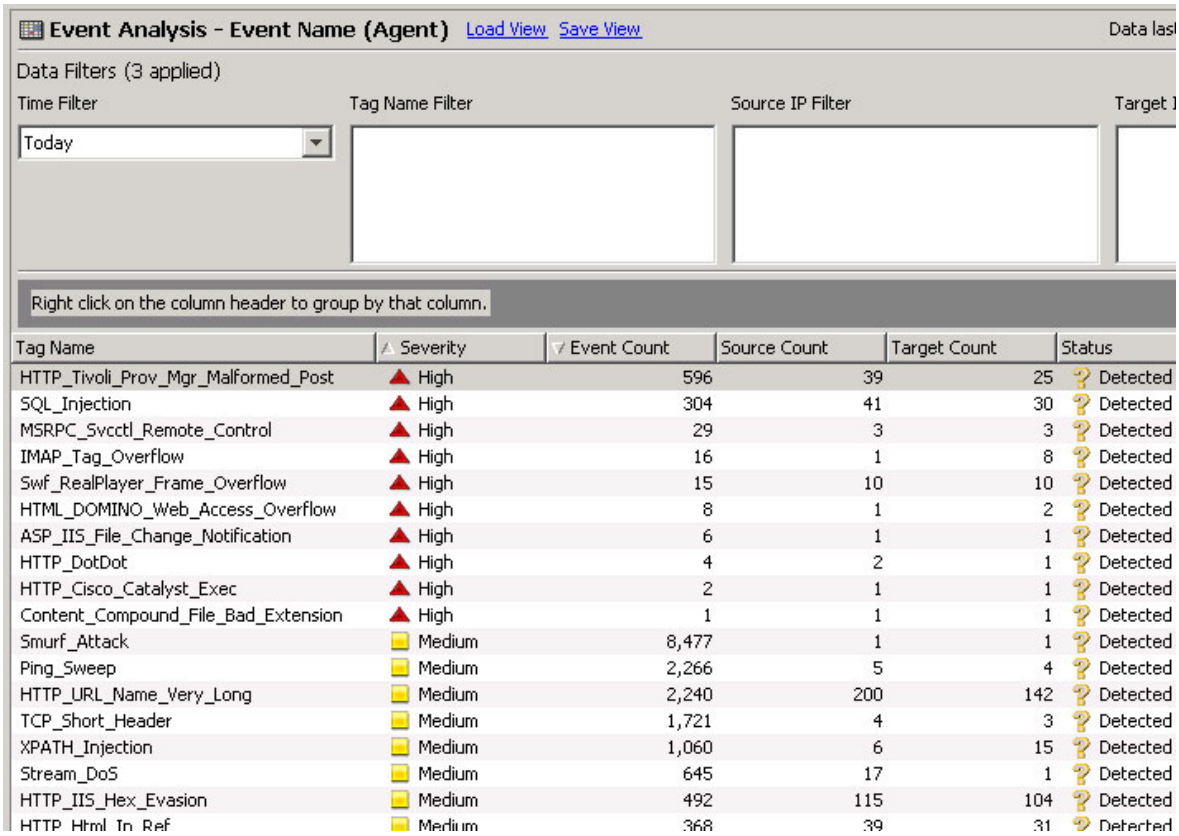
- Přípravná fáze – shromáždit kvalitní dokumentaci a informace o sítích, uzlech, IP adresách, záznamech o předcházejícím skenování zranitelnosti a seznam operačních systémů na jednotlivých uzlech.
- Detekce je první reakční fáze v případě incidentu detekovaném systémem IDS nebo IPS. Incident je nutné zaznamenat s časovým razítkem, obsahem napadení a cílem. Je zapotřebí stanovit rozsah a dopad útoku na organizace.
- Izolace – přepokládá učinit rozhodnutí a stanovit činnosti, jak zabránit příčinám širšího poškození a jejich likvidace.
- Likvidace – proces eliminace hlavní příčiny incidentu.
- Zotavení – nastává, když se systém vrátí do svého normálního funkčního stavu. Uskutečněné procesy a procedury přivedly systém do normálního stavu.
- Pokračování v činnosti - je fáze, kdy se revidují předešlé kroky, a analyzuje se případná možnost vylepšení. Fáze zahrnuje ujištění se, že zavedením všech předchozích kroků dojde ke zmírnění následků uvedeného typu útoků v případě, že se odehrají znovu. Příkladem jsou bezpečnostní záplaty, které se implementují jako prevence proti známým zranitelnostem.

Metodologie incidentní odezvy předpokládá vznik týmu incidentní odezvy a koordinaci uvedených činností. Předpokladem jsou vyškolení experti a jejich dostupnost v době incidentu.

IBM Site protector je SW určený k administraci IPS zařízení IBM. Konzole obsahuje několik předdefinovaných analýz, které lze použít k dalšímu zkoumání z mnoha pohledů a úrovně detailů. Tyto pohledy mohou pomoci provést první kroky strategie analýzy událostí.



		Prote...	Event Name	Severity	Protocol	Ignor...	Display	Block
⊟ Attack/Audit: Attack (2 items)								
⊞ Enabled: false (786 items)								
⊟ Enabled: true (1943 items)								
		Global	Ace_Filename_Overflow	High	ace	☐	Without	☑
		Global	ACF_Mem_Corruption	High	acf	☐	Without	☑
		Global	ActiveX_Blocked	High	html	☐	Without	☑
		Global	ActiveX_Warning	Low	html	☐	Without	☐
		Global	Agentx_HelixServer_Exec	High	agentx	☐	Without	☑
		Global	AIX_Pdnsd_Overflow	High	tcp	☐	Without	☑
		Global	Allaire_JRun_JSP_Execute	High	url	☐	Without	☑
		Global	Alvgus_Request	Medium	udp	☐	Without	☑
		Global	Alvgus_Response	High	udp	☐	Without	☑
		Global	Alvgus_TCP_Request	High	tcp	☐	Without	☑
		Global	Alvgus_TCP_Response	High	tcp	☐	Without	☑
		Global	Amanda_TCP_Response	High	tcp	☐	Without	☑
		Global	AolAdmin_Response	High	tcp	☐	Without	☑
		Global	AOLIM_AddExternalApp_Overflow	High	aolim	☐	Without	☑



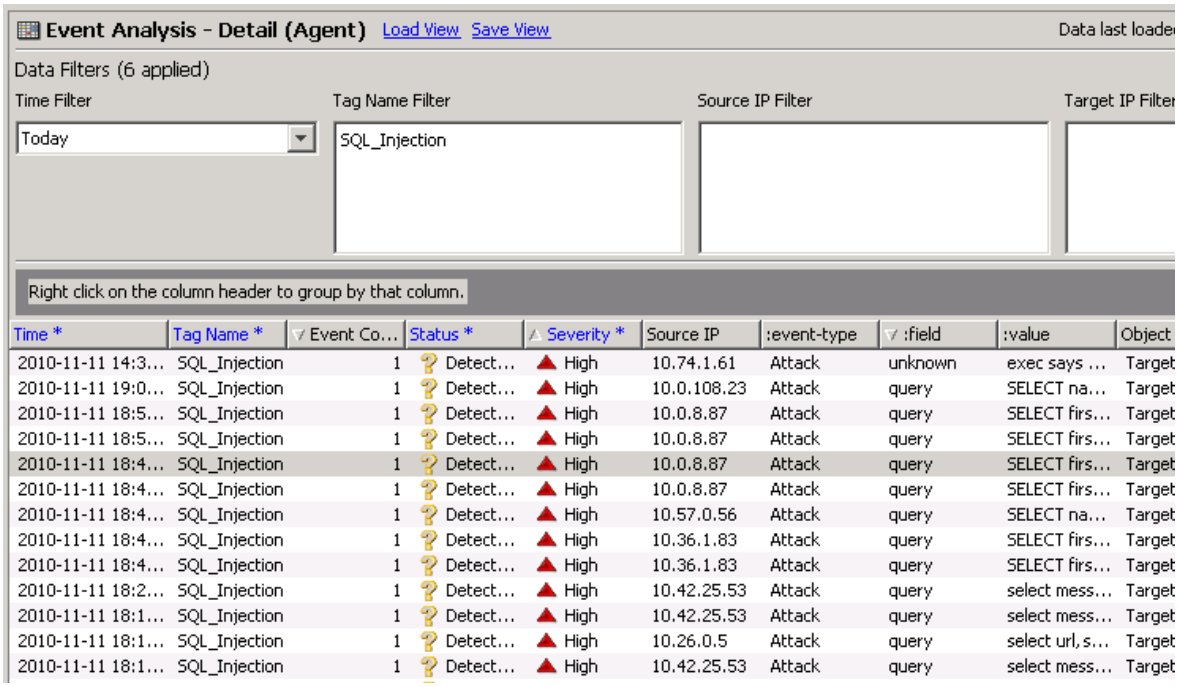
Event Analysis - Event Name (Agent) Load View Save View Data last

Data Filters (3 applied)

Time Filter: Today | Tag Name Filter | Source IP Filter | Target I

Right click on the column header to group by that column.

Tag Name	Severity	Event Count	Source Count	Target Count	Status
HTTP_Tivoli_Prov_Mgr_Malformed_Post	High	596	39	25	Detected
SQL_Injection	High	304	41	30	Detected
MSRPC_Svcctl_Remote_Control	High	29	3	3	Detected
IMAP_Tag_Overflow	High	16	1	8	Detected
Swf_RealPlayer_Frame_Overflow	High	15	10	10	Detected
HTML_DOMINO_Web_Access_Overflow	High	8	1	2	Detected
ASP_IIS_File_Change_Notification	High	6	1	1	Detected
HTTP_DotDot	High	4	2	1	Detected
HTTP_Cisco_Catalyst_Exec	High	2	1	1	Detected
Content_Compound_File_Bad_Extension	High	1	1	1	Detected
Smurf_Attack	Medium	8,477	1	1	Detected
Ping_Sweep	Medium	2,266	5	4	Detected
HTTP_URL_Name_Very_Long	Medium	2,240	200	142	Detected
TCP_Short_Header	Medium	1,721	4	3	Detected
XPATH_Injection	Medium	1,060	6	15	Detected
Stream_DoS	Medium	645	17	1	Detected
HTTP_IIS_Hex_Evasion	Medium	492	115	104	Detected
HTTP_Html_In_Ref	Medium	368	39	31	Detected



Time *	Tag Name *	Event Co...	Status *	Severity *	Source IP	:event-type	:field	:value	Object
2010-11-11 14:3...	SQL_Injection	1	Detect...	High	10.74.1.61	Attack	unknown	exec says ...	Target
2010-11-11 19:0...	SQL_Injection	1	Detect...	High	10.0.108.23	Attack	query	SELECT na...	Target
2010-11-11 18:5...	SQL_Injection	1	Detect...	High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:5...	SQL_Injection	1	Detect...	High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	Detect...	High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	Detect...	High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	Detect...	High	10.57.0.56	Attack	query	SELECT na...	Target
2010-11-11 18:4...	SQL_Injection	1	Detect...	High	10.36.1.83	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	Detect...	High	10.36.1.83	Attack	query	SELECT firs...	Target
2010-11-11 18:2...	SQL_Injection	1	Detect...	High	10.42.25.53	Attack	query	select mess...	Target
2010-11-11 18:1...	SQL_Injection	1	Detect...	High	10.42.25.53	Attack	query	select mess...	Target
2010-11-11 18:1...	SQL_Injection	1	Detect...	High	10.26.0.5	Attack	query	select url, s...	Target
2010-11-11 18:1...	SQL_Injection	1	Detect...	High	10.42.25.53	Attack	query	select mess...	Target

Obr. 39. Analýza událostí v konzoli IBM Site Protector [26].

7.5 Systém kontroly zranitelností

Kontrola zranitelností je detekce zranitelností založená na podobné znalostní databázi, jakou používají systémy IPS nebo IDS. Výše uvedené produkty obsahují tuto funkcionalitu, u ostatních produktů je nutné řešit kontrolu samostatně. Lze též využít produkty jiných výrobců a tím zvýšit kontrolu a bezpečnost sítě. Je však nutné si uvědomit, že detekce zranitelností na jedné straně může být chápána systémem IDS nebo IPS jako pokus o narušení na straně druhé.

Kontrolu zranitelností je nutné naplánovat. Posouzení zranitelnosti je proces, ve kterém příslušný SW identifikuje a kvantifikuje bezpečnostní díry daného systému nebo sítě. Systém identifikuje hosty, jejich operační systém, kontroluje otevřené TCP a UDP porty. Získané informace porovná se znalostní databází zranitelností a vystaví certifikát ohodnocení, na základě kterého administrátor naplánuje příslušná nápravná opatření. Pokud by administrátor tato opatření neprovedl, systém IPS by následně zablokoval komunikaci využívající příslušnou zranitelnost.

ZÁVĚR

Zajištění bezpečnosti datového centra je komplexní záležitost. S tímto pojetím bylo cílem práci zpracovat, tedy poskytnout čitateli ucelený pohled na nezbytná opatření logické, fyzické, procesní a systémové bezpečnosti.

Nejprve byly zkoumány legislativní požadavky vyhlášky č. 528/2005 Sb., které mohou být dobrým startem pro stanovení jednotlivých opatření fyzické bezpečnosti, vzhledem ke kategorii prostředí, jakým datové centrum bezpochyby je. Normativní požadavky ČSN/ISO 15408:2005, podle kterých musí informační systém obsahovat nezbytné bezpečnostní funkce typu řízení přístupu, autentizace nebo audit, spadají do logické úrovně bezpečnosti a byly podkladem pro definici bezpečnostní politiky. Definování základních požadavků na fyzickou bezpečnost dále vycházelo z ČSN/ISO 17799:2005. A v neposlední řadě bylo nutné vzít v úvahu doporučení mezinárodní normy ISO 27001:2005, poskytující podporu při zavádění systému managementu bezpečnosti, jehož součástí je zpracovaná bezpečnostní politika datového centra.

Fyzická bezpečnost je nezbytná vzhledem k existenci řady rizikových jevů. Provedená analýza identifikovala vnější a vnitřní hrozby, úmyslné či náhodné. Ohodnocení aktiv a jejich zranitelností vycházelo z expertního posouzení. Stalo se základem návrhu patřičných protiopatření. Jednalo se o režimová opatření společně s fyzickou ostrahou, o technické a mechanické prostředky. Návrh zónového uspořádání datového centra společně s použitými prostředky vytvořily kompaktní základ bezpečného datového centra. Ten doplnil fyzický návrh bezpečné redundantní počítačové sítě.

V další úrovni byla zkoumána bezpečnost z pohledu jednotlivých systémů. Byla navržena doporučená konfigurace bezpečné počítačové sítě. Serverové prostředí má svůj útočný povrch a ten bylo nutné minimalizovat. Zónové uspořádání počítačové sítě bylo součástí logického designu.

Závěrečná část práce nastínila současné hrozby pocházející z hackerských útoků. Systém kontroly bezpečnosti vycházel z návrhu prostředků aktivní bezpečnosti. Byly popsány systémy detekce a prevence narušení, dostupná zařízení a kritéria jejich výběru. Návrh topologie vycházel z teoretické přípravy, jejíž aktuálnost se ukázala jako problém, vzhledem k rychle se vyvíjející oblasti. Tyto systémy jsou natolik rozsáhlé, že lze na práci navázat důkladnou analýzou dalších konkurenčních produktů a jejich porovnáním.

SEZNAM POUŽITÉ LITERATURY

[1]ENDORF, Carl. Detekce a prevence počítačového útoku. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.

[2] BERKA, Milan. Bezpečná počítačová síť. Praha: Dashofer, 2004, 1600 s.

ISSN 1801-8033.

[3] SELECKÝ, Matúš. Penetrační testy a exploitace. Brno: Computer Press, 2012, 304 s.

ISBN 978-80-251-3752-9.

[4] VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: UTB, 2012, 152 s.

ISBN 978-80-7454-230-5.

[5] COLE, Eric. Network security bible. 2nd ed. Indianapolis: Wiley Publishing, 2009,

891 p. ISBN 978-0-470-50249-5.

[6] SOSINSKY, Barrie. Mistrovství-počítačové sítě. 1. vyd. Brno: Computer Press, 2010,

840 s. ISBN 978-80-251-3363-7.

[7] ŠEBESTA, V.; ŠTVERKA, V.; STEINER, F.; ŠEBESTOVÁ, M. Systémy řízení bezpečnosti informací, Část 3: Směrnice pro management rizik bezpečnosti informací podle BS 7799-3:2005 s komentářem k managementu rizik v ISMS. Praha: Český normalizační institut, 2007, ISBN 978-80-7043-535-9.

[8] STEINER, F.; TUPA, J. Management rizik v systémech řízení bezpečnosti informací. In MOPP 2007. V Plzni : Západočeská univerzita, 2007. s. 177-183. ISBN 978-80-7043-535-9.

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

[10] FRYE, Douglas W. Network security policies and procedures. New York: Springer, 2007, 240 p. ISBN 03-874-7955-4.

[11] SINGH, Abhishek. Vulnerability analysis and defense for the Internet. New York: Springer, 2008, 254 p. ISBN 03-877-4390-1.

[12] WU, Chwan-Hwa. Introduction to computer networks and cybersecurity. Boca Raton: CRC Press, 2013, 1336 p. ISBN 978-1-4665-7213-3.

[13] TIA-942. Telecommunications Infrastructure Standard for Data Centers. Arlington, VA: TELECOMMUNICATIONS INDUSTRY ASSOCIATION, 2005. *E-Bookspdf.org* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.e-bookspdf.org/download/ansi-tia-942-a.html

[14] MOLÍK, V.; VÁCHA, H.; NOVÁK, R. Datová centra realisticky. *SystemOnLine* [online]. © 2010 [cit. 2014-04-29]. Dostupné z: http://www.systemonline.cz/sprava-it/datova-centra-realisticky.htm

[15] SHZ plynové. *PBZ s.r.o.* [online]. © 2010 [cit. 2014-04-29]. Dostupné z: http://www.pzb.cz/cs/shz-plynove

[16] IRISAccess 7000. *IrisID* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.irisid.com/irisaccess7000

[17] Perimeter Security. *Optex Group* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.optex-europe.com/applications/#perimeter

[18] Network Foundation Design. *Cisco.com* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Education/SchoolsSRA_DG/SchoolsSRA-DG/SchoolsSRA_chap3.html

[19] Cisco ASA 5500-X Series Next-Generation Firewalls. *Cisco.com* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-c

[20] SKALICKÝ, Marek. Řízení zranitelností ICT. *Rar.cz* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/QualysGuard/$FILE/DSM-3-2007_Uvod_do%20rizeni_zranitelnosti_ICT.pdf

[21] Bezpečnost informačních systémů. *NBÚ* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/

[22] Use of RFC 1918 "Private Addresses" on the UC Berkeley Campus Network. *Berkeley* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.net.berkeley.edu/netinfo/ip/rfc1918.shtml

[23] BUECKER, A.; BULHOES, D.; DOBBS, Matthew. Stopping Internet Threats Before They Affect Your Business by Using the IBM Security Network Intrusion Prevention Systém. *IBM Redbooks* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.redbooks.ibm.com/redpapers/pdfs/redp4683.pdf

[24] VMWare Virtual Networking Concepts. *VMware.com* [online]. © 2007 [cit. 2014-04-29]. Dostupné z: https://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

[25] Altron Data Centre Solution. *Altron.com* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.altronds.net/solutions/

[26] BUECKER, Alex. Network Intrusion Prevention Design Guide. *IBM Redbooks* [online]. © 2014 [cit. 2014-04-29]. Dostupné z: http://www.redbooks.ibm.com/redbooks/pdfs/sg247979.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AC	Alternate Current
ACS	Access Control System
AR	Analýza rizik
ARP	Address Resolution Protocol
BP	Bezpečnostní politika
BP	Bridge Protocol
BPDU	Bridge Protocol Data Unit
BW	Business Warehouse
CBPDU	Configuration Bridge Protocol Data Unit
CC	Common Criteria
CCTV	Circuit Closed Television
CEM	Common Evaluation Methodology
CIDR	Classless Inter-Domain Routing
CRAMM	CCTA Risk Analysis and Management Method
CRM	Customer Relationship Management
ČSN	Česká státní norma
CVVS	Common Vulnerability Scoring System
DMZ	Demilitarizovaná zóna
DPI	Deep Packet Inspection
DoS	Denial of Service
DDoS	Distributed Denial of Service
DW	Data Warehouse
EAL	Evaluation Assurance Level
EBIT	Earnings before Interest and Taxes

EPS	Elektrická požární signalizace
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
GbE	Gigabit Ethernet
HIDS	Host based IDS
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technologies
IDS	Intrusion detection system
IOS	Integrated Operating System
IP	Internet Protocol
IPS	Intrusion prevention system
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
MBSA	Microsoft Baseline Security Analyzer
MTBF	Mean Time between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MZS	Mechanické zábranné systémy
NB	Network-based
HB	Host-based
NAP	Network Access Protection
NIDS	Network based IDS

NVD	National Vulnerability Database
PDCA	Plan-Do-Check-Act
PP	Protection Profile
PZS	Poplachový zabezpečovací systém
SAS	Security Alarm System
SCM	Supply Chain Management
SHZ	Samočinné hasící zařízení
SLA	Service Level Agreement
SLM	Service Level Management
SNMP	Simple Network Monitoring Protocol
SPI	State full Packet Inspection
ST	Security Target
STP	Spanning tree protocol
TCA	Topology Change Accept
TCN	Topology Change Notification
TCP	Transmission Control Protocol
TCSEC	Computer System Evaluation Criteria
TOE	Target of Evaluation
UDP	Undirected Data Protocol
UPS	Uninterruptable Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: MATICE HROZEB

Hrozby	Zranitelnost	Pravd.	Data	Aplikace	Server fyzický 1 aplikace (SF)	Server virtuální 1 aplikace (SV)	Server HOSTITEL pro více aplikací (H)	LAN infrastruktura (směrovač, firewall, přepínač)	WAN infrastruktura (směrovač, okruhy)	Datová uložiště (DS)	Zálohovací knihovny, zařízení (ZK)	Kabeláž LAN, WAN (K)	Bezpečnostní zařízení CCTV, ACS (BZ)	Poplachové zařízení PZS, EPS (PZ)	Hasící zařízení (SHZ)	Komunikační systémy (KS)	Přenosová zařízení poplachových systémů (KP)	Systémy primárního napájení (AC)	Systémy záložního napájení (UPS)	Systémy záložního napájení (DA)	Klimatizace (KL)	Přístup k datům a aplikacím (P)
Externí náhodné			5	4	4	3	4	4	3	5	5	3	5	5	3	3	5	5	5	5	5	3
Přírodní hrozba (povodeň, bouřka apod.)	Fyzické poškození zařízení vodou	2	3	3	3	3	3	3	1	3	3	2	3	3		3	1	1	1	1	1	3
Blackout / výpadek napájení (primární i záložní	Nedostupnost systémů v DC	2																	3	3		
Selhání komunikace, technická závada u operátora	Nedostupnost DC přes WAN	2	1	1					3							2						3
Požár v okolí	Fyzické poškození zařízení ohněm	1	3	3	1	1	1	1	3	1	1	1	2	1		3	1	3	1	1	1	3
Výbuch v okolí	Fyzické poškození zařízení destrukcí	1	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2	1	3	3	3	3
Externí úmyslné																						
Požár úmyslně založený	Fyzické poškození zařízení ohněm	2	3	3	1	1	1	1	3	1	1	1	2	1		3	1	3	1	1	1	3
Výbuch úmyslně založený	Fyzické poškození zařízení destrukcí	2	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2	1	3	3	3	3
Teroristický útok, sabotáž	Fyzické poškození zařízení, budovy	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1	1	3
Infiltrace komunikace (narušení, zachycení,	Nedostupnost DC přes WAN	3	3	3					3							2						3
Logická infiltrace (hacking, viry, falšování	Vnější hackerské útoky (zneužití dat, nedostupnost	5	3	3																		3
Interní náhodné																						
Závady zařízení	Nedostupnost služby, dat, aplikace, sítě,	4			2		3	1		3	1		3	3		1	1			1	3	
Lidské chyby (uživatelů, administrátorů,	Nedostupnost služby, dat, aplikace, sítě	4	2	2	1	1		1		1												2
Poškození vodou	Fyzické poškození zařízení vodou	2	3	3	3	3	3	3	1	3	3	2	3	3		3	1	1	1	1	1	3
Požár	Fyzické poškození zařízení ohněm	2	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2	1	3	3	3	3
Interní úmyslné																						
Logická infiltrace (hacking, viry, falšování	Vnitřní hackerské útoky, zneužití dat, nedostupnost	3	3	3						3	3											3
Infiltrace komunikace (narušení, zachycení,	Nedostupnost DC přes WAN	3	3	3					3							2						3
Závady zařízení	Nedostupnost služby, dat, aplikace, sítě,	2			3		3	3		3	3		3	3		3	3			3	3	
Lidské chyby (uživatelů, administrátorů,	Nedostupnost služby, dat, aplikace, sítě	2	3	3	3	3		3		3												3
Poškození vodou	Fyzické poškození zařízení vodou	1	3	3	3	3	3	3	1	3	3	2	3	3		3	1	1	1	1	1	3
Požár	Fyzické poškození zařízení ohněm	1	3	3	3	3	3	3	1	3	3	2	3	3	1	3	1	1	1	1	1	3

PŘÍLOHA P II: MATICE RIZIK

Hrozby	Zranitelnost	Pravd.	Data	Aplikace	Server fyzický 1 aplikace (SF)	Server virtuální 1 aplikace (SV)	Server HOSTITEL pro více aplikací (H)	LAN infrastruktura (směrovač, firewall, přepínač)	WAN infrastruktura (směrovač, okruhy)	Datová uložiště (DS)	Zálohovací knihovny, zařízení (ZK)	Kabeláž LAN, WAN (K)	Bezpečnostní zařízení CCTV, ACS (BZ)	Poplachové zařízení PZS, EPS (PZ)	Hasící zařízení (SHZ)	Komunikační systémy (KS)	Přenosová zařízení poplachových systémů (KP)	Systémy primárního napájení (AC)	Systémy záložního napájení (UPS)	Systémy záložního napájení (DA)	Klimatizace (KL)	Přístup k datům a aplikacím (P)
Externí náhodné			5	4	4	3	4	4	3	5	5	3	5	5	3	3	5	5	5	5	5	3
Přírodní hrozba (povodeň, bouřka apod.)	Fyzické poškození zařízení vodou	2	30	24	24	18	24	24	6	30	30	12	30	30	0	18	10	10	10	10	10	18
Blackout / výpadek napájení (primární i záložní	Nedostupnost systémů v DC	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	30	30	0	0
Selhání komunikace, technická závada u operátora	Nedostupnost DC přes WAN	2	10	8	0	0	0	0	18	0	0	0	0	0	0	12	0	0	0	0	0	18
Požár v okolí	Fyzické poškození zařízení ohněm	1	15	12	4	3	4	4	9	5	5	3	10	5	0	9	5	15	5	5	5	9
Výbuch v okolí	Fyzické poškození zařízení destrukcí	1	15	12	12	9	12	12	9	15	15	9	15	15	6	9	10	5	15	15	15	9
Externí úmyslné																						
Požár úmyslně založený	Fyzické poškození zařízení ohněm	2	30	24	8	6	8	8	18	10	10	6	20	10	0	18	10	30	10	10	10	18
Výbuch úmyslně založený	Fyzické poškození zařízení destrukcí	2	30	24	24	18	24	24	18	30	30	18	30	30	12	18	20	10	30	30	30	18
Teroristický útok, sabotáž	Fyzické poškození zařízení, budovy	1	15	12	12	9	12	12	9	15	15	9	15	15	9	9	15	15	15	5	5	9
Infiltrace komunikace (narušení, zachycení,	Nedostupnost DC přes WAN	3	45	36	0	0	0	0	27	0	0	0	0	0	0	18	0	0	0	0	0	27
Logická infiltrace (hacking, viry, falšování identity)	Vnější hackerské útoky (zneužití dat, nedostupnost služby)	5	75	60	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	45
Interní náhodné																						
Závady zařízení	Nedostupnost služby, dat, aplikace, sítě,	4	0	0	32	0	48	16	0	60	20	0	60	60	0	12	20	0	0	20	60	0
Lidské chyby (uživatelů, administrátorů,	Nedostupnost služby, dat, aplikace, sítě	4	40	32	16	12	0	16	0	20	0	0	0	0	0	0	0	0	0	0	0	24
Poškození vodou	Fyzické poškození zařízení vodou	2	30	24	24	18	24	24	6	30	30	12	30	30	0	18	10	10	10	10	10	18
Požár	Fyzické poškození zařízení ohněm	2	30	24	24	18	24	24	18	30	30	18	30	30	12	18	20	10	30	30	30	18
Interní úmyslné																						
Logická infiltrace (hacking, viry, falšování	Vnitřní hackerské útoky, zneužití dat, nedostupnost	3	45	36	0	0	0	0	0	45	45	0	0	0	0	0	0	0	0	0	0	27
Infiltrace komunikace (narušení, zachycení,	Nedostupnost DC přes WAN	3	45	36	0	0	0	0	27	0	0	0	0	0	0	18	0	0	0	0	0	27
Závady zařízení	Nedostupnost služby, dat, aplikace, sítě,	2	0	0	24	0	24	24	0	30	30	0	30	30	0	18	30	0	0	30	30	0
Lidské chyby (uživatelů, administrátorů,	Nedostupnost služby, dat, aplikace, sítě	2	30	24	24	18	0	24	0	30	0	0	0	0	0	0	0	0	0	0	0	18
Poškození vodou	Fyzické poškození zařízení vodou	1	15	12	12	9	12	12	3	15	15	6	15	15	0	9	5	5	5	5	5	9
Požár	Fyzické poškození zařízení ohněm	1	15	12	12	9	12	12	3	15	15	6	15	15	3	9	5	5	5	5	5	9