VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

IMPLEMENTACE BEZPEČNOSTNÍCH STANDARDŮ PRO WEBHOSTINGOVOU SPOLEČNOST

IMPLEMENTING SECURITY STANDARDS FOR A WEB HOSTING COMPANY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Libor Kůřil

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Petr Sedlák

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Libor Kůřil**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2023/24
Studijní program:	Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Implementace bezpečnostních standardů pro webhostingovou společnost

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Cílem práce je zodolnit infrastrukturu webhostingové společnosti zavedením Minimálního bezpečnostního standardu.

Základní literární prameny:

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN isbn978-80-88260-39-4.

SEDLÁK, Petr a KONEČNÝ, Martin, 2023. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2023/24

V Brně dne 4.2.2024

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práce se zaměřuje na implementaci minimálních bezpečnostních standardů pro provoz webhostingové společnosti. Popisuje současný stav zabezpečení provozované infrastruktury a informačního systému. Obsahuje návrh, jak do současného stavu implementovat minimální bezpečnostní standardy, tak aby na ně bylo možné v budoucnu navázat se zavedením kybernetické bezpečnosti.

Klíčová slova

webhosting, infrastruktura, standard, bezpečnost

Abstract

The thesis focuses on the implementation of minimum security standards for the operation of a web hosting company. It describes the current state of security of the operating infrastructure and information system. It contains a proposal how to implement minimum security standards into the current state so that they can be followed up in the future with the introduction of cyber security.

Keywords

webhosting, infrastructure, standard, security

Bibliografická citace

KŮŘIL, Libor. *Implementace bezpečnostních standardů pro webhostingovou společnost* [online]. Brno, 2024 [cit. 2024-05-10]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/158738. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 10. 5. 2024

Bc. Libor Kůřil

autor

Poděkování

Rád bych poděkoval Ing. Petru Sedlákovi za odborné vedení mé diplomové práce a celkově dobré rady a připomínky po celý čas mého studia. Dále bych chtěl poděkovat mé manželce za obrovskou podporu a míru tolerance, kterou mi během celého studia věnovala. Jako poslední bych chtěl poděkovat svým rodičům, že mi celou dobu věřili.

Obsah

Úvod

V současné digitální éře se kybernetická bezpečnost stává stále důležitější nejen pro velké korporace, ale také pro malé a střední podniky. S narůstajícím počtem kybernetických útoků a hrozeb je nezbytné, aby se společnosti zaměřily na ochranu svých dat a služeb. To platí pro všechny společnosti, které jsou zodpovědné za ochranu nejen svých vlastních dat, ale také dat svých zákazníků.

Tato diplomová práce se zaměřuje na implementaci minimálních bezpečnostních standardů v kontextu webhostingové společnosti. Cílem je analyzovat a popsat, jak tyto standardy mohou být aplikovány k posílení bezpečnostního rámce společnosti.

Předmětem zkoumání standardů bude jak manažerská, tak i technická část. Společnost je tzv. startup a v současné době vedena a vyvíjena pouze jediným člověkem. V tomto kontextu je evidentní, že vedení společnosti má výrazný zájem na implementaci těchto bezpečnostních opatření, aby byla zajištěna ochrana nejen naší infrastruktury, ale i dat našich zákazníků.

V průběhu této práce bude provedena důkladná analýza jednotlivých aspektů minimálních bezpečnostních standardů s cílem identifikovat klíčové oblasti, které vyžadují zlepšení, a navrhnout specifická technická řešení. Výstup práce tak přispěje k lepšímu porozumění, jak zabezpečit nabízené služby v souladu s minimálními bezpečnostními požadavky a doporučeními, a také zformuje ucelený návod na praktickou implementaci.

1 Teoretická východiska práce

V této části budou popsány pojmy a definice, které budou použity při popisu analýzy současného stavu zabezpečení a dále při zpracování návrhové části práce.

1.1 Aktivum (Asset)

Jedná se o veškerý hmotný a nehmotný majetek organizace. Zahrnuje hardware, software, data, infrastrukturu a také lidské zdroje a intelektuální vlastnictví. Aktiva jsou klíčová pro provoz organizace. Je důležité je všechny identifikovat, klasifikovat a správně chránit. (1)

1.2 Důvěrnost (Confidentialy)

Ochrana informací před neoprávněným přístupem a zveřejněním. Cílem je zajistit, že informace jsou dostupné pouze těm osobám, které jsou k tomu oprávněny. (1)

1.3 Dostupnost (Availability)

Informace a systémy jsou přístupné pouze na požadované úrovni v požadovaný okamžik. Cílem je zajistit, že uživatelé mají přístup k potřebným datům a zdrojům v okamžiku jejich potřeby. (1)

1.4 Integrita (Integrity)

Integrita udržuje přesnost a úplnost informací. Hlavním požadavkem je zajistit, že data nejsou během ukládání, zpracování nebo přenosu nijak neoprávněně změněna, poškozena nebo zničena. (1)

1.5 CIA Triáda

Všechny výše uvedené pojmy spolu tvoří model tzv. CIA Triáda. Tento model definuje tři základní cíle, které jsou klíčové pro ochranu informací (Information security). (1)

Obrázek 1: CIA Triáda (Zdroj: Vlastní zpracování)

1.6 Traffic Light Protocol

Traffic Light Protocol (TLP) je protokol, který byl navržen za účelem usnadnění širšího sdílení potenciálně citlivých informací a zefektivnění spolupráce. Sdílení informací se odehrává od zdroje informací směrem k jednomu nebo více příjemcům. TLP je rozdělen do čtyř, potažmo pěti stupňů a barevně odlišen. (2)

- **Clear** (bílá) – Informace může být sdílená veřejně bez jakéhokoliv omezení.
- **Green** (zelená) – Informace je sdílená pouze interně v rámci organizace.
- **Amber** (oranžová): Informace sdílená interně na základě zásady *need-to-know*. Za určitých podmínek je možno předat třetí straně.
- **Amber Strict** (oranžová striktní): Informace sdílená pouze interně na základě zásady *need-to-know*.
- **Red** (Červená): Pouze pro vybrané příjemce, bez možnosti sdílet dále.

1.7 Hrozba (Treat)

Hrozba se vztahuje na potenciální nebezpečí, které může způsobit škodu nebo ztrátu informací, infrastruktury nebo technologických systémů. Tato škoda může být způsobena úmyslnými akcemi, jako jsou kybernetické útoky nebo malware, nebo neúmyslnými událostmi, jako jsou technické selhání nebo přírodní katastrofy. Identifikace a řízení hrozeb je klíčové pro ochranu organizačních aktiv a udržení kontinuity provozu. (1)

1.8 Zranitelnost (Vulnerability)

Zranitelností se označují slabiny nebo nedostatky v systémech, aplikacích nebo procesech, které mohou být využity k získání neoprávněného přístupu, způsobení škody nebo krádeže dat. Tyto zranitelnosti mohou existovat v různých formách, jako jsou softwarové chyby, nedostatečně zabezpečené sítě, slabá hesla nebo neaktualizovaný software. Identifikace, hodnocení a řešení těchto zranitelností jsou zásadní pro zajištění ochrany informací a systémů před potenciálními hrozbami a útoky. (1)

1.9 Opatření (Coutremeasure)

Opatřením se myslí akce nebo procesy, které jsou implementovány za účelem ochrany informací a systémů před hrozbami a zranitelnostmi. Tato opatření mohou zahrnovat technické nástroje, jako jsou antivirové programy a firewally, administrativní politiky, jako jsou pravidla pro správu hesel a přístupová práva, a fyzické zabezpečení, jako jsou zámky a bezpečnostní kamery. Cílem těchto opatření je snížit riziko útoků, ztráty dat nebo jiných bezpečnostních incidentů a zajistit důvěrnost, integritu a dostupnost informací. (1)

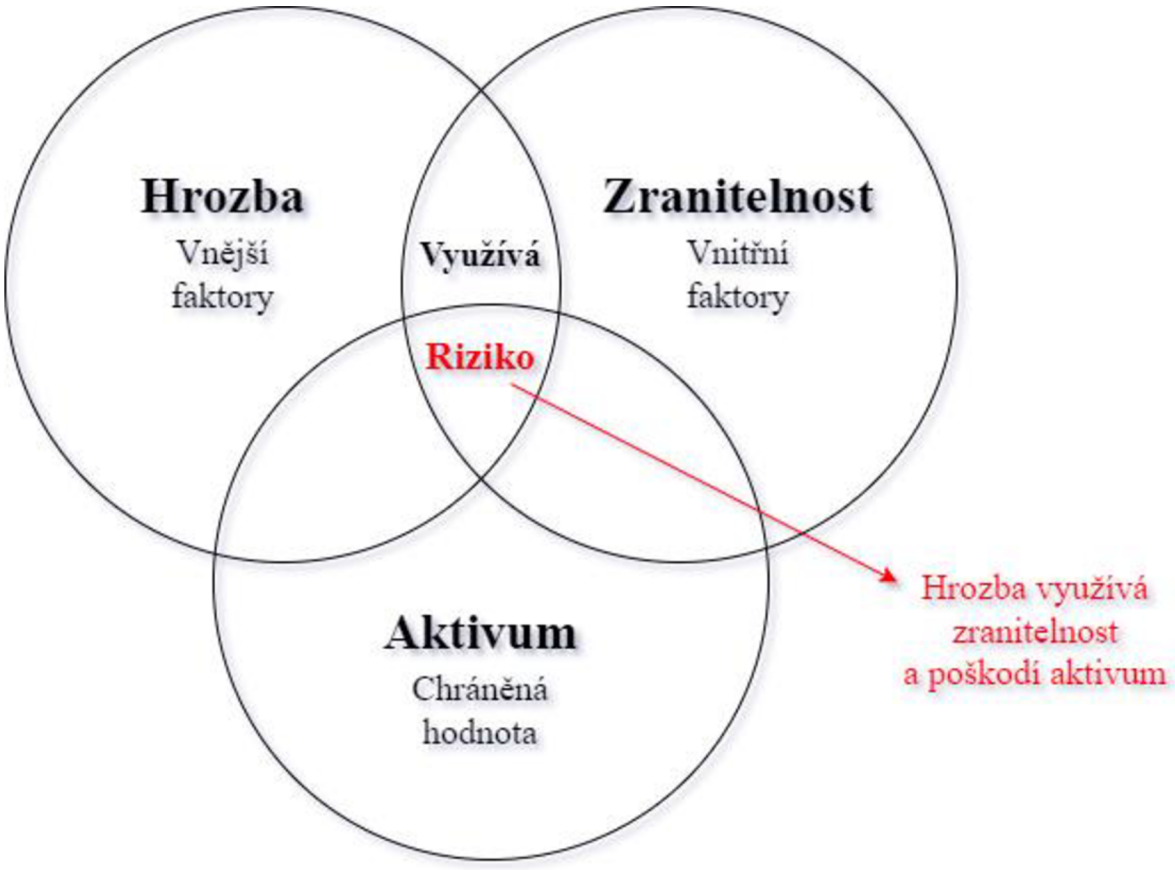
1.10 Riziko (Risk)

Rizikem se myslí možnost vzniku škody nebo ztráty, která může být způsobena využitím existujících zranitelností nebo v důsledku hrozeb. Riziko je obvykle vyjádřeno jako kombinace pravděpodobnosti vzniku škodlivého incidentu a potenciálního dopadu, který by tento incident mohl mít na organizaci. Správa rizik zahrnuje identifikaci, analýzu a hodnocení rizik, následované implementací opatření pro jejich zmírnění nebo

eliminaci. Důležitou součástí je také pravidelné monitorování a revize rizik, aby bylo možné reagovat na nově vzniklé hrozby a změny v organizačním prostředí. (1)

1.11 Dopad (Impact)

Následky, které mohou nastat v důsledku bezpečnostních incidentů, jako jsou úniky dat, narušení systémů nebo zneužití informací. Tyto následky mohou mít vážné finanční, reputační, právní nebo operativní důsledky pro organizaci. Důležité je proto nejenom identifikovat a řídit rizika, ale také plánovat a připravovat se na možné dopady, aby bylo možné efektivně reagovat a minimalizovat škody v případě bezpečnostních incidentů. (1)

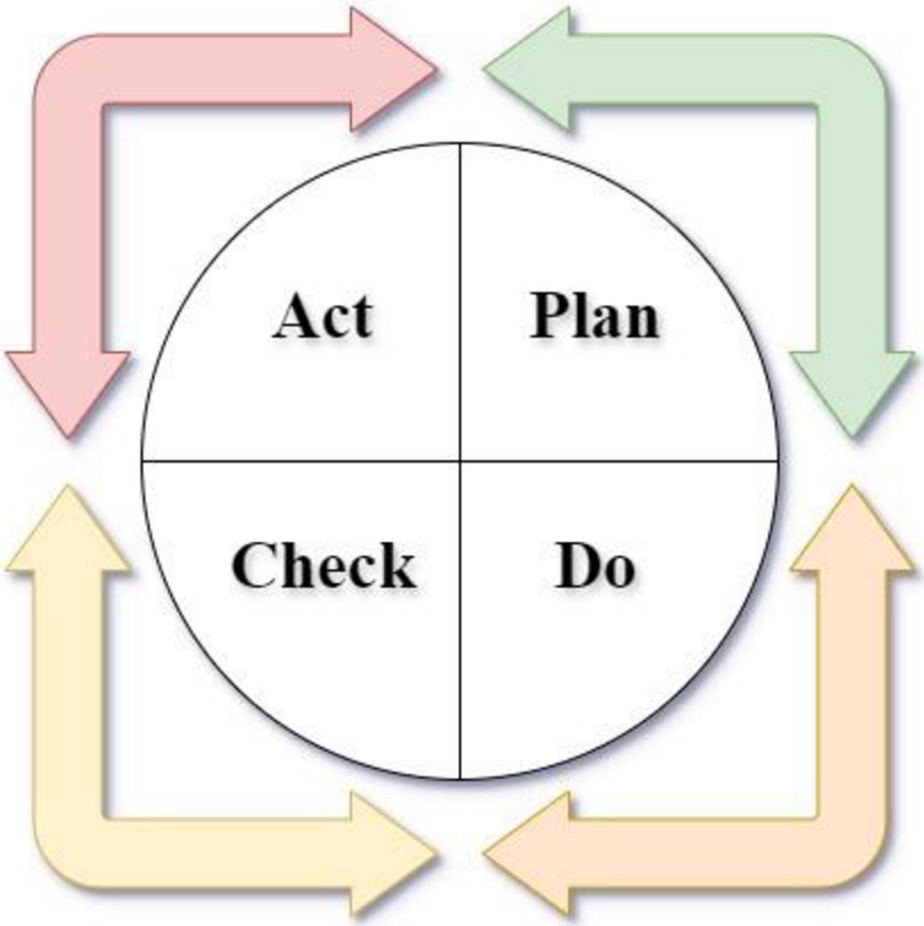


Obrázek 2: Vyjádření pojmů aktivum, zranitelnost, hrozba a riziko (Zdroj: Vlastní zpracování dle: [1], s. 16)

1.12 Demingův model

PDCA cyklus, známý také jako Demingův model, je iterativní čtyřfázový proces pro řízení a neustálé zlepšování procesů a produktů. Jedná se o efektivní nástroj pro dosažení neustálého zlepšování v jakémkoli procesu, protože podporuje kulturu systematického hodnocení a revize. (1)

- **Plan** (plánuj): Tento krok zahrnuje analýzu současných procesů a plánování změn, které by mohly vést ke zlepšení. Důležité je stanovit zde metody pro sběr dat, která budou použita pro hodnocení změn. (1)
- **Do** (dělej): V této fázi se implementují plány. Zahrnuje to zavedení změn na menší škále nebo v experimentálním režimu, aby se omezily dopady na celkovou operaci v případě, že nové postupy nebudou fungovat, jak bylo zamýšleno. (1)
- **Check** (kotroluj): Po implementaci změn se shromažďují a analyzují data k ověření, zda došlo ke zlepšení. Tato fáze zahrnuje porovnání skutečných výsledků s očekávanými cíli, aby se zjistilo, zda byly změny úspěšné. (1)
- **Act** (jednej): Na základě výsledků získaných v kontrolní fázi se rozhodne, zda bude nový proces standardizován a používán pro všechny relevantní činnosti, nebo zda jsou potřeba další změny a úpravy. Pokud změny nevedly k očekávanému zlepšení, cyklus se opakuje s novými plány a úpravami. (1)



Obrázek 3: PDCA Cyklus (Zdroj: Vlastní zpracování dle: [1], s. 29)

1.13 Datové centrum (DC)

Datacentrum můžeme charakterizovat jako místo, kde jsou umístěny počítačové systémy a příslušenství, včetně telekomunikačních zařízení a centralizovaných úložišť, ať už fyzických nebo virtuálních. Data centrum slouží k ukládání, správě, distribuci dat a informací. Tato zařízení hrají klíčovou roli v podnikové infrastruktuře a internetových službách poskytující základ pro cloudové služby, webhosting a mnoho dalších. (1)

1.13.1 Spolehlivost (Reliability)

Spolehlivost se dá definovat jako schopnost systému nebo komponenty fungovat bez selhání po požadovanou dobu v daných podmínkách. Je klíčová pro udržení nepřetržitého provozu a minimalizaci výpadků, které by mohly negativně ovlivnit dostupnost služeb. (1)

1.13.2 Střední doba mezi poruchami (Mean Time Between Failure)

Znamená, že zařízení nebo systém je schopen fungovat dlouhodobě bez selhání, což přispívá k celkové spolehlivosti. MTBF je také důležitým faktorem při rozhodování o investicích do nového vybavení, protože vyšší MTBF obvykle naznačuje lepší kvalitu a nižší celkové náklady na vlastnictví díky méně časté potřebě oprav a údržby. (1)

1.13.3 Střední doba potřebná pro opravu (Mean Time To Repear)

Ukazatel, který vyjadřuje průměrný čas potřebný k opravě zařízení nebo systému po jeho poruše. MTTR zahrnuje celý proces od diagnostiky problému, přes samotnou opravu až po testování a znovu zprovoznění zařízení. Snížení MTTR je klíčové pro minimalizaci doby výpadku a zajištění nepřetržitého provozu v kritických aplikacích, jako jsou datová centra a IT infrastruktura. (1)

1.13.4 Redundance (Redundandcy)

Zavedení duplicitních systémových komponent, které zajišťují kontinuitu provozu i v případě selhání jedné z nich. Redundance je tedy základním stavebním kamenem pro zajištění vysoké dostupnosti a spolehlivosti IT infrastruktury, což přispívá k lepší ochraně dat a služeb před nepředvídatelnými událostmi. (1)

1.13.5 Odolnost (Resiliency)

Schopnost systému, sítě nebo organizace odolat a efektivně se zotavit z různých typů výpadků, útoků nebo katastrof. Tento koncept je klíčový pro zajištění nepřetržitého a bezpečného provozu. Odolnost tedy není jen o technických řešeních, ale také o strategickém plánování, připravenosti a průběžném vzdělávání. (1)

1.13.6 Kritické místo (SPOF)

Specifický prvek systému nebo infrastruktury, jehož selhání by mělo zásadní dopad na celkový provoz a dostupnost služeb. Identifikace a ochrana těchto kritických míst je klíčová pro zajištění kontinuity a bezpečnosti operací. Zajištění redundance a odolnosti těchto kritických míst je nezbytné pro minimalizaci rizika výpadku a zajištění nepřetržitého provozu. To zahrnuje implementaci záložních systémů, pravidelné testování a údržbu, stejně jako strategické plánování pro rychlou obnovu v případě selhání. (1)

1.13.7 Kategorizace DC

Tabulka 1: Kategorizace datových center (Zdroj: Vlastní zpracování dle: [1], s. 269)

Třída	Tier I	Tier II	Tier III	Tier IV
	Basic	**Redundant components**	**Concurently maintable**	**Fault tolerant**
Počet přívodů do DR	Pouze 1	Pouze 1	1 Aktivní 1 Pasivní	2 Aktivní
Redundance prvků	N	N+1	N+1	min. N+1
Podporovaná plocha	20 %	30 %	80–90 %	100 %
Průměrná hustota zátěže	1,9 – 2,8 kW/m	3,7 – 4,7 kW/m	9,3 – 13,9 kW/m	>13,9 kW/m
Max. roční výpadek	**28,8 hod**	**22 hod**	**1,6 hod**	**15 min**
Dostupnost	**99,671 %**	**99,749 %**	**99,982 %**	**99,995 %**

1.13.8 Studie proveditelnosti

Mezinárodní telekomunikační asociace BISCI vydala podpůrný dokument s podrobným popisem jednotlivých problematik, dokument se nazývá:

ANSI/NECA/BISCI 002-2019 Data Center Design and Implementation Best Practices. (1)

Doporučená osnova studie proveditelnosti:

- Obecné požadavky,
- Analýzy,
- Návrhy,
- Definice požadavků,
- Specifikace,
- Rámcový rozpočet,
- Závěr (Ano-Ne) (1)

Studie proveditelnosti by měla být provedena odborníky z různých oblastí, včetně IT specialistů, inženýrů, právníků a finančních analytiků, aby bylo zajištěno, že všechny aspekty projektu jsou důkladně prozkoumány a hodnoceny. Je nutné brát na zřetel, že studie proveditelnosti je hlavním rozhodovacím dokumentem pro investora. (1)

Požadavky je možné shrnout do následujících bodů:

1. Teoretická východiska.
2. Požadavky na projekt DC.
3. Požadavky ze zákona (Kybernetický zákon).
4. Relevantní normy DC.
5. Požární normy.
6. Normy pro zemnění a pospojování.
7. Interní předpisy investora. (1)

V případě analýzy výběru lokality je nutné dodržet doporučené vzdálenosti od uměle vytvořených elementů, viz. *Tabulka 2*:

Tabulka 2: Kategorizace datových center (Zdroj: Vlastní zpracování dle: [1], s. 261)

Element	Doporučená minimální vzdálenost
Letiště	8 km
Vzletové a přistávací dráhy	1,6 km
Vodní trasy	3,2 km
Přístav	3,2 km
Jezera a přehrady	3,2 km
Vodojemy (Věžové)	1,6 km
Chemické továrny a sklady	8 km
Elektrárny (na uhlí nebo plyn)	8 km
Slévárny a těžký průmysl	8 km
Plynové stanice a distribuce	1,6 km
Železnice	1,6 km
Vedení VVN	1,6 km

Jaderné elektrárny	80 km
Skládky a spalovny	3,2 km
Vojenské objekty a sklady munice	13 km
Obecní voda a kanalizace odpadních vod	3,2 km
Vysílací stanice R/TV	5 km
Lomy	3,2 km
Výzkumné laboratoře	5 km
Vlastní skladovací prostory	1,6 km
Lakovna, prodej barev	1,6 km
Hospodářská stavení (výkrmny, jatka)	3,2 km

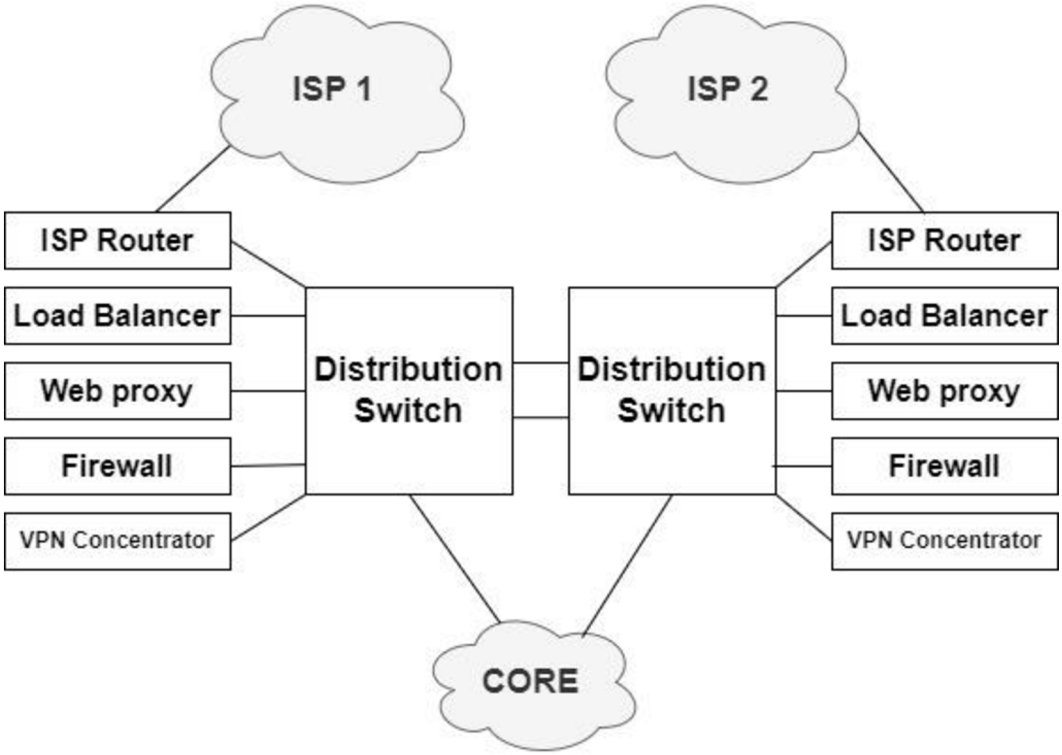
1.13.9 Provoz datového centra

Mezinárodní telekomunikační asociace BISCI vydala také dokument, který popisuje rutinní provoz datového centra: **ANSI/NECA/BISCI 009**-2019 Data Center Operations and Maintenance Best Practice, který popisuje následující činnosti:

- Governance.
- Standard operating procedures.
- Security
    - Security Plan.
    - Physical, cyber and IT security.
    - Material control and loss prevention.
    - Computer room and cricial facility areas special considerations.
    - Event response.
- Maintenance.
- Emergency operating procedures.
- Management.

V kontextu provozu datových center je klíčovým faktorem zajištění vysoké dostupnosti a spolehlivosti služeb. To vyžaduje implementaci redundantních řešení, která minimalizují riziko výpadku a zajišťují nepřetržitý chod systémů. Jedním z

příkladů takového řešení je redundantní konektivita datového centra k internetu. Tato strategie zahrnuje použití více nezávislých internetových připojení, což zajišťuje, že v případě selhání jedné linky mohou ostatní připojení převzít její funkci a udržet tak datové centrum online. Redundantní konektivita je tedy zásadní pro udržení operativní kontinuity a ochranu před potenciálními výpadky, které by mohly způsobit značné ekonomické nebo reputační škody. (1)



Obrázek 4: Redundantní konektivita DC k internetu (Zdroj: Vlastní zpracování dle: [1], s. 267)

Stejně důležité je také redundantní napojení na poskytovatele energií. Toto opatření zajišťuje, že v případě výpadku jednoho zdroje energie může druhý zdroj okamžitě převzít zásobování energií, čímž se eliminuje riziko přerušení provozu způsobeného nedostatkem elektrické energie. Redundantní napojení na poskytovatele energií je tedy klíčové pro zajištění nepřetržitého provozu datového centra a ochranu před následky energetických výpadků. (1)

1.13.10 Certifikace DC

Důvodů, proč mít certifikované datacentrum, je hned několik. Mezi ty hlavní patří dostupnost a důvěryhodnost pro zákazníky. Certifikace je postavena na dvou modelech:

1. TIA-924 – certifikace vycházející z normy ANSI-TIA/EIA 942
2. Uptime Institute – certifikace je dána metodikou společnosti Uptime Institute.

Uptime Institute je nezávislá organizace zaměřená na zlepšování výkonnosti, efektivity a spolehlivosti. Institut poskytuje certifikaci ve třech úrovních:

- Projektové (Desing),
- Konstrukční (Facility),
- Provozní (Operation).

Certifikace zaměstnanců datových center podle odborných kritérií nabízí mnoho možností. Jako příklad lze uvést strukturovaný program certifikace pro pracovníky datových center od společnosti EXIN:

- CDSC – Certified Data Centre Specialist,
- CDCP – Certified Data Center Professional,
- CDRP – Certified Data Center Risk Professional,
- CDMS – Certified Data Center Expert,
- CTIA – Certified TIA-942 Internal Auditor,
- CTDC – Certified TIA-942 Design Consultant,
- CDFC – Certified Data Founder Certificate (1)

Obrázek 5: Certifikační známky organizace Uptime Institute (Zdroj: [3])

1.14 SLA (Service-level agreement)

SLA neboli smlouva o úrovni služeb, představuje formální dohodu mezi poskytovatelem služby a jeho zákazníkem. Tato dohoda explicitně definuje a stanovuje očekávanou úroveň služeb, které mají být poskytovány. Smlouva detailně specifikuje povahu služeb, kvalitativní standardy, které musí být dodrženy, odpovědnosti jak poskytovatele, tak zákazníka, a metriky, které jsou používány k měření výkonu poskytovaných služeb. Dále SLA často zahrnuje ustanovení o sankcích pro případ, že nedojde k dodržení stanovených kritérií, včetně možných kompenzací pro zákazníka. Tato smlouva je klíčová pro zajištění transparentnosti, předvídatelnosti a spolehlivosti ve vztahu mezi poskytovatelem služby a zákazníkem, a také hraje zásadní roli v managementu očekávání a zajištění kvality poskytovaných služeb. (1)

V rámci Smlouvy o úrovni služeb (SLA) jsou definovány metriky, které slouží k měření kvality a výkonu poskytovaných služeb. Mezi tyto metriky patří například rychlost reakce, dostupnost služeb, kvalita realizace a počet zpracovaných požadavků. Tyto indikátory umožňují oběma stranám efektivně sledovat a hodnotit kvalitu poskytovaných služeb. (1)

Dále SLA obsahuje ustanovení o postupech, které budou aplikovány v případě nesplnění stanovených standardů. Tyto postupy mohou zahrnovat různé sankce nebo

kompenzace pro zákazníka, což zajišťuje, že obě strany mají jasné očekávání a jsou chráněny v případě vzniklých problémů. (1)

1.14.1 Specifikace služeb v SLA

1. Incident Management
2. Problem Management
3. Change Management
4. Release Management
5. Configuration Management
6. Capacity Management
7. IT Service Continuity Management and Availability Management
8. Information Security Management (1)

1.15 NDA (Non-disclosure agreement)

NDA neboli dohoda o mlčenlivosti, je právní dokument, kde se strany zavazují nezveřejňovat určité informace považované za důvěrné. Tyto informace jsou v rámci dohody jasně specifikovány, stejně jako podmínky jejich ochrany a doba, po kterou musí být důvěrnost zachována. Dohoda je často využívána v obchodních vztazích, například při fúzích, akvizicích nebo společných technologických projektech, aby se zabránilo úniku citlivých dat konkurenci nebo do veřejného prostoru. (4)

1.15.1 Obsah NDA

1. **Identifikace smluvních stran**: Dohoda o mlčenlivosti přesně specifikuje, které strany jsou součástí smlouvy a kdo má povinnost zachovávat mlčenlivost a na koho se tato povinnost vztahuje.
2. **Vymezení důvěrných informací**: NDA určuje, které údaje jsou klasifikovány jako citlivé a musí být chráněny dohodou o mlčenlivosti.
3. **Vyloučení aplikace**: NDA definuje situace, ve kterých určité informace nejsou považovány za důvěrné a nejsou chráněny mlčenlivostí, což může zahrnovat veřejně dostupné údaje nebo informace, které jsou již stranám známé.
4. **Právní podmínky plnění mlčenlivosti**: NDA stanovuje konkrétní pravidla pro zacházení s důvěrnými informacemi, včetně metod jejich zabezpečení,

doby, po kterou musí zůstat tajné, a dalších aspektů týkajících se jejich ochrany.

5. **Skončení NDA**: Smlouva o mlčenlivosti může být rozvázána různými způsoby, včetně písemného oznámení nebo vzájemné dohody smluvních stran.
6. **Povinnosti při ukončení**: Dohoda o mlčenlivosti stanoví, jaké kroky musí strany podniknout po jejím skončení, včetně vrácení všech důvěrných informací, zničení jejich kopií a zachování mlčenlivosti po určitou dobu i po ukončení platnosti smlouvy.
7. **Sankce při porušení mlčenlivosti**: Dohoda o mlčenlivosti může zahrnovat klauzule o trestech pro případ porušení dohodnutých podmínek mlčenlivosti. Tyto sankce mohou obsahovat finanční pokuty, požadavky na náhradu škody nebo jiné právní kroky. (4)

1.16 CAB (Change Advisory Board)

CAB, což je zkratka pro Change Advisory Board, představuje skupinu osob odpovědných za posuzování změn v IT prostředí organizace. Tato rada se skládá z technických pracovníků a klíčových rozhodovatelů, přičemž její složení není pevně dané. Role manažera změn spočívá v tom, že zajistí přítomnost správných lidí s potřebnými informacemi a odbornostmi, kteří jsou schopni efektivně posoudit každou navrhovanou změnu. (5)

Je běžné, že pro specifické typy změn jsou do procesu přizváni specializovaní experti, aby poskytli své znalosti a poradenství. Důležité je zdůraznit, že CAB a Change Management nejsou totožné pojmy. Zatímco CAB se primárně soustředí na revizi a poradenství ohledně změnových požadavků z pohledu potenciálních rizik a nechtěných důsledků, Change Management zahrnuje širší spektrum aktivit spojených s plánováním, hodnocením, schvalováním a monitoringem všech změn. (5)

Pracovníci, kteří se standardně účastní CAB:

- Senior Network Engineer
- Senior Application Development engineer
- All Operations Managers
- Service Desk
- Infrastructure engineer

- Senior Security Engineer
- Information Security Officer
- Business Relationship Manager
- Service Owners
- Business users (5)

1.17 MFA (Multi-factor Authentication)

Vícefaktorové ověřování (MFA) je způsob ověření identity uživatele, který vyžaduje více než jeden důkaz totožnosti. Na rozdíl od tradičního přístupu, kdy se používá pouze uživatelské jméno a heslo, MFA kombinuje dva nebo více ověřovacích faktorů. Tato metoda zvyšuje bezpečnost tím, že komplikuje neoprávněný přístup k aplikacím a citlivým informacím a je účinným nástrojem pro ochranu proti krádeži identity, kybernetickým útokům a porušení dat. (6)

1.18 IDM (Identity Management)

Správa identit představuje soubor postupů a technologií, které se zaměřují na řízení a ochranu digitálních identit v rámci organizace. Tento systém umožňuje řízení uživatelských účtů, procesů autentizace a autorizace, a nabízí služby zajišťující, že oprávnění uživatelé získávají přístup k potřebným informačním zdrojům v odpovídající dobu a podmínkách. IDM systémy obvykle zahrnují funkce jako je správa uživatelských rolí, nastavení přístupových politik, provádění auditů a vytváření reportů. (7)

1.19 MDM (Mobile Device Management)

Správa mobilních zařízení (MDM) představuje klíčový nástroj pro zabezpečení a efektivní správu mobilních zařízení v rámci organizace. Tento typ softwaru umožňuje organizacím nejen zabezpečit a monitorovat mobilní zařízení zaměstnanců, ale také spravovat a prosazovat firemní zásady na těchto zařízeních. (8)

Hlavním cílem MDM je ochrana podnikové sítě prostřednictvím zabezpečení a optimalizace mobilních zařízení, jako jsou notebooky, chytré telefony a tablety, které se připojují k podnikovým sítím. (8)

V kontextu ovládání PC se MDM také označuje jako unified endpoint management (UEM), což umožňuje organizacím spravovat všechna jejich podniková

zařízení z jednoho místa. Tento integrovaný přístup nejen zvyšuje bezpečnost podnikových sítí, ale také umožňuje zaměstnancům používat svá vlastní zařízení (BYOD), což může vést k vyšší efektivitě práce a produktivitě. (8)

1.20 Kryptologie

Kryptologie je věda zabývající se studiem metod šifrování, tj. způsobů, jakými lze informace ochránit před neoprávněným přístupem nebo dešifrováním. Zahrnuje jak kryptografii, což je umění vytváření šifer a kódů, tak kryptoanalýzu, která se snaží tyto šifry a kódy rozluštit. Cílem kryptologie je zajistit bezpečnost a důvěrnost informací v digitálním světě. (1)

1.20.1 Kryptografie

Kryptografie je disciplína kryptologie, která se zabývá návrhem a vytvářením šifrovacích systémů a metod pro zabezpečení informací. Tato věda hraje klíčovou roli v ochraně dat před neoprávněným přístupem a zajišťuje, že informace jsou přenášeny a ukládány v bezpečné formě. Kryptografie využívá matematické teorie a algoritmy k šifrování a dešifrování dat, což umožňuje udržet důvěrnost, integritu a autentičnost informací v digitálním prostředí. (1)

Kryptologické systémy:

1. **DES** – Data Encryption Standard: Vznik v roce 1975. Založen na blokovém symetrickém šifrování privátním klíčem, blok má délku 64 bitů.
2. **IDEA** – Inernational Data Encryption Algorithm: Vznik v roce 1990. Založen na algoritmu s délkou klíče 128 bitů se symetrickým šifrováním, blok má délku 64 bitů.
3. **RSA** – Rivest, Shamir a Adleman algoritmus: Vznik v roce 1977. Založen na asymetrickém šifrování.
4. **AES** – Advanced Encrzption Standard: Vznik v roce 1997. Délka vstupně-výstupního bloku AES 128 bitů a délkou klíče 128, 192, až 256 bitů. (1)

1.21 MBS (Minimální bezpečnostní standard)

Jedná se o dokument vydaný NÚKIB a poskytuje základní principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro organizace, které nepodléhají regulaci zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Je vhodný zejména pro ty, kteří teprve začínají s implementací bezpečnostních opatření, a přistupuje k tématu formou návodných doporučení. Dokument je rozdělen do dvou částí pro snadnější orientaci. První část se věnuje manažerským aspektům a typicky zahrnuje popisy procesů, které je třeba v organizaci zavést a udržovat. Druhá část je technicky zaměřená a je určena především pro IT specialisty, poskytuje konkrétní pokyny pro zajištění minimální úrovně zabezpečení. (9)

2 Analýza současného stavu

2.1 Představení společnosti

Webhostingová společnost se zabývá poskytováním hostingových služeb pro soukromé osoby a malé podniky.

Společnost v současné době disponuje jedním fyzickým serverem umístěným v Brněnském datacentru společnosti *nej.cz s.r.o.* a jedním mikropočítačem Raspberry PI, který je geo-lokačně oddělen a je provozován v datacentru společnosti *BEST-HOSTING s.r.o.* se sídlem v Hradci Králové. Protože firma nedisponuje vlastním datovým centrem, odpadá starost se zajištění internetové konektivity, přidělování rozsahu IP adres a dodávkami elektrické energie. Výše uvedené je zajištěno prostřednictvím smlouvy s dodavatelem a předem dohodnutých SLA.

2.2 Činnosti

Mezi její rozsah nabízených služeb patří komplexní hostingové služby, jako jsou:

- Správa internetových domén,
- Správa DNS záznamů pro vlastní doménu,
- Mail hostingové řešení pro provoz e-mailů pod vlastní doménou,
- Webový hosting pro skriptovací jazyk PHP,
- Webový hosting pro vysokoúrovňový programovací jazyk Python v oddělených kontejnerech,
- Provoz relačních databází typu MySQL a PostgreSQL,
- Správa CRON úloh,
- aj.

2.3 Organizační struktura

Společnost aktuálně nemá členění do organizačních struktur, protože je řízena a vedena jediným člověkem, který má na starosti veškerou agendu. Je majitelem, manažerem, vývojářem, systémovým administrátorem a operátorem helpdesku.

2.4 Fyzická bezpečnost datacentra

Společnost nevlastní své datové centrum, ale využívá pronajaté prostory třetí strany. Současné datové centrum, které firma využívá, je konstruováno podle kategorie TIER III, což zahrnuje možnost servisu za provozu, duální zdroje napájení pro IT komponenty, redundanci N+1, více distribučních cest a dieselové generátory s neomezenou dobou provozu. Nicméně hlavní trasy vodního chlazení nejsou redundantní, protože datové centrum bylo integrováno do již stávající budovy. (10)

2.4.1 Napájení datacentra

Datové centrum TH Brno je napojeno na elektrickou síť skrze rozvodnu 110/22 kV Líšeň pomocí dvou vysokonapěťových přípojek, které jsou propojeny smyčkově přes vlastní vysokonapěťovou rozvodnu centra s dvěma transformátory o výkonu 1 MW. Tato rozvodna přebírá energii z hlavní přenosové soustavy z rozvoden Čebín a Sokolnice, což zajišťuje redundanci napájení datového centra na úrovni primární přenosové soustavy.

Datové centrum je vybaveno čtyřmi dieselovými generátory Volvo Penta s výkonem 630 kVA, které jsou zajištěny redundancí N+1 a mají zásobu paliva na 24 až 48 hodin. Systém řízení umožňuje generátorům automatické připojení zpět k distribuční síti bez přerušení, což minimalizuje riziko výpadku během testování UPS jednotek a stejnosměrných zdrojů.

Pro zabezpečení proti krátkým výpadkům a poruchám v distribuční síti jsou v datovém centru instalovány centrální jednotky UPS s kapacitou 960 kVA na každou větev, které poskytují záložní energii na dobu 15 minut, a také baterie pro stejnosměrné zdroje, které napájí zařízení stejnosměrným proudem. (10)

2.4.2 Chlazení

Systém chlazení je dvouokruhový (glykol-voda) s centrálními kompresorovými chladícími jednotkami (chillery). Suché chladiče se nachází na střeše budovy datacentra, na sálech jsou pak umístěny klimatizační jednotky o výkonu 50 kW a zvlhčovače vzduchu. Všechny aktivní kritické prvky chladicího systému mají redundanci N+1.

Pro zvýšení chladícího výkonu a spolehlivosti je systém chlazení postupně doplňován jednotkami na bázi přímého výparu. V datových sálech je udržována teplota v rozsahu 20-27 °C a relativní vlhkost v rozmezí 30-70 %.

Pro chlazení stojanů, resp. v nich umístěných zařízení, je využíván systém uzavřených studených uliček (novější sály), systému teplých a studených uliček (starší sály) či průchodu vzduchu dnem stojanů. Studený vzduch od klimatizačních jednotek je ke stojanům distribuován skrz prostor dvojité technologické podlahy MERO. Systém chlazení je dimenzován tak, aby zvládl až 10 kW tepelného výkonu na stojan. (10)

2.4.3 Konektivita

Datacentrum TH Brno je do NIX.cz připojeno kapacitou 2× 200 Gbps přes vlastní páteřní síť dvěma linkami v kruhové topologii (dvě nezávislé trasy).

Se Slovenskem je datacentrum připojeno 10Gbps linkou do SIX.sk a 10Gbps linkou do NIX.sk.

Do zahraničí je TH Brno připojenou 200Gbps linkou zakončenou v Praze a 120Gbps linkou zakončenou v Brně.

S peeringovými centry je propojení zajištěno s kapacitou 2× 200 Gbps do peering.cz a 1× 10 Gbps do google.com. Další linky zajišťují propojení s vybranými partnery. (10)

2.4.4 Přístup

Autorizované osoby z řad zákazníků mají možnost přístupu do dohledového centra (NOC) nepřetržitě 24 hodin denně, 7 dní v týdnu, po celý rok. Zákazníci získají na své jméno čipové karty, které jim umožní nezávislý vstup do budovy a do datových sálů. Klíče k rackům jsou uloženy v elektronicky zabezpečených trezorech pro klíče, kde je přístup řízen a monitorován. (10)

2.4.5 Zabezpečení

Veškeré vstupy do budovy datacentra jsou monitorovány kamerovým systémem CCTV se záznamovým zařízením, které uchovává záznam 14 dní zpětně. Vnitřní kamerový systém je instalován v celém objektu. Výstupy všech kamer jsou vyvedeny na centrální pult dohledového centra. Budova je zabezpečena elektronickým

zabezpečovacím systémem (EZS) s lokálními poplachovými výstupy (sirénami) a s výstupy vyvedenými na centrální pult dohledového centra.

Vchody do budovy, do jednotlivých kanceláří či technologických prostor jsou vybaveny elektronickými zámky a čtečkami čipových karet pro ověření přístupových oprávnění. Všechny vstupy jsou logovány.

U vstupu do technologických sálů datového centra sídlí Dohledové centrum se stálou službou v režimu 24/7/365, jehož pracovníci zajišťují fyzické ověření přístupových oprávnění vstupujících osob.

Pro případ násilného vniknutí a jiných závažných bezpečnostních incidentů je sjednána bezpečnostní služba v režimu 24/7/365 s dojezdem do 15 minut. (10)

2.4.6 Protipožární systém

Datacentrum TH Brno je vybaveno systémem pro detekci a hašení požáru, včetně elektrického systému požární signalizace (EPS) s protipožárními čidly a evakuačními sirénami. Čidla jsou umístěna nejen v datových sálech, ale i pod dvojitou technologickou podlahou. Signály z EPS jsou přivedeny na centrální pult dohledového centra, které obsahuje nadřazený řídící systém s vizualizací budovy, umožňující rychlé určení lokality požáru.

Technologické sály jsou vybaveny automatickým hasicím systémem (SHZ). Pro hašení požárů v těchto prostorách se používají chemická hasiva FM-200 a Novec-1230, která nezpůsobují škody na instalovaných zařízeních. (10)

2.5 Řízení přístupů

Řízení přístupů je v našem případě nutné rozdělovat na dva pohledy. Přístupy pro správce systému, administrátory a pro uživatele, kteří mají část systému vyhrazenou pro provoz vlastních aplikací (klientská část). Každý uživatel má přidělený jedinečný identifikátor, podle kterého je možné jej dohledat.

Protože ve společnosti pracuje jediný člověk, ztrácí pojem BYOD v současné situaci význam. Nástroj MDM chybí úplně. Co se týká uživatelů jakožto zákazníků, kteří používají systém pro běh aplikací, není chtěné ani možné, aby byli kontrolovány jejich zařízení, pomocí kterých se připojují k systému.

Administrátoři systému mají také vlastní uživatelské účty, které nemají takový stupeň oprávnění jako je tomu v případě správců systému. Některé technické a uživatelské účty nejsou vytvářeny centrálně, ale přímo na serveru jako linux účty s POSIX oprávněním. Aktuálně neexistuje žádný ucelený dokument, který by nařizoval, jak vytvářet technické účty a kde je možné jim upravit nebo změnit heslo.

2.5.1 Registrace, autentizace a identifikace uživatelů

Pokud je uživatel vytvářen centrálně, tak je použit systém adresářové struktury OpenLDAP na protokolu LDAP. Pravidla a procesy pro vytváření nejsou definovány.

2.5.2 Politika hesel pro uživatelské a privilegované účty

Současná politika hesel je tristní, viz. výčet hodnot níže:

- minimální délka hesla je 8 znaků,
- heslo musí obsahovat minimálně jedno velké písmeno a číslici,
- maximální doba platnosti je neomezená,
- je možné používat stejné heslo,
- minimální platnost hesla není omezena,
- účet se při neplatných pokusech o heslo neuzamyká,
- jednorázové prvotní heslo není nastaveno

2.6 Požadavky v oblasti ochrany před škodlivým kódem

V rámci našeho systému není aktuálně implementován žádný aktivní systém pro detekci nebo odhalení škodlivého kódu. Ty časti systému, u kterých je to opodstatněné, jsou provozovány ve vyhraném síťovém prostředí.

2.7 Kybernetické bezpečnostní události a incidenty

V současné době není stanoven žádný proces, eskalační proces a pravidla, která by reagovala na vzniklou kybernetickou bezpečnostní události. Hlavní důvod je dán počtem lidí v organizaci. Pokud by ovšem taková situace nastala, bude řešena s takovou prioritou, jak bude uznáno za vhodné pro běh informačního systému.

Pro případnou analýzu těchto událostí jsou využívány provozní záznamy, které můžeme rozdělit do několika kategorií.

2.7.1 Skupina SEC

Do této kategorie spadají bezpečnostní nástroje, firewall, routery aj. Tato kategorie logů není ve značné míře v naší správě, a to právě z důvodu provozování vlastní infrastruktury v datacentru třetí strany. Pokud by tedy došlo k tak závažnému incidentu, bylo by nutné kontaktovat datacentrum s požadavkem o součinnost při řešení incidentu.

2.7.2 Skupina APP a OS

Tato kategorie zahrnuje servery, pracovní stanice a aplikace, které jsou kompletně pod naší správou. Pokud by tedy bylo nutné prověřit systémové logy (selhání služby, chyby, zapnutí, vypnutí), auditní události (pokusy o přihlášení, přístupy k souborům, změna nastavení) nebo komunikaci na úrovni aplikace (klientské požadavky na server, informace o přihlášení, počty transakcí) máme logy z jednotlivých stanic a serverů k dispozici.

Současný stav uchovávání provozních logů v tabulce 1 viz. níže:

Tabulka 3: Počet dnů uchování logů (Zdroj: Vlastní zpracování)

SEC				
Počet dní	Datacentrum			
OS	**Systém**	**Audit**		
Počet dní	30	30		
APP	**C<>S**	**Využití účtů**	**Aktivita**	**Akce**
Počet dní	14	14	14	14

2.7.3 Centrální log management

Všechny logy z informačního sytému musí být integrovány do centrálního řešení. V našem případě tomu tak ovšem není. Není implementovaný žádný nástroj na kolekci logů a jejich bezpečnostní vyhodnocování. Všechny logy jsou tedy dostupné pouze na serveru, kde běží operační systém nebo aplikace. Je tedy nutné přímé přihlášení do systému a vyčtení potřebných informací z logu přímo tam.

2.8 Požadavky v oblasti aplikační bezpečnosti

Pro vývoj a integraci interních systémů je používáno výhradně testovací prostředí. Testovací prostředí je fyzicky odděleno a aktuálně provozováno lokálně v místě bydliště majitele společnosti. Pro vývoj není nutné využívat produkční data. Testovací data jsou fiktivně vymyšlené údaje, a to pouze s výjimkou testování domén, kdy je nutné používat již existující zaregistrovanou doménu dle podmínek příslušného registrátora.

2.9 Ukládání hesel

Pro ukládání hesel je v současné době používáno několik nástrojů a metod. Hesla, která jsou vytvářena automatizací, jsou uloženy v textové podobě na souborovém systému. Na venek jsou ve skrytém adresáři a dostupné pouze na automatizačním serveru. Některá systémová hesla jsou uložena v aplikaci *Keepass* na lokálním počítači v zaheslovaném souboru. Hesla pro emailové účty používají hashovací algoritmus SHA512. Heslo pro přístup do webové administrace klientského účtu pro ovládání hostingových služeb je uloženo pomocí šifrovací algoritmus Bcrypt. Posledním používaným úložištěm hesel je program *Gopass*. Uložená hesla jsou v souboru na souborovém systému a jsou šifrována pomocí GPG klíčů. Program GPG používá hashovací algoritmy SHA1, SHA256, SHA384, SHA512, SHA224 a RIPEMD160. Používání "salt(u)" není nikde implementováno.

2.10 Požadavky v oblasti zajišťování úrovně dostupnosti informací

Aktuální architektura celého serverové řešení je postavena na jednom fyzickém hostu, na kterém jsou dále provozovány virtuální servery. To znamená že v případě výpadku nějaké komponenty na fyzickém hostovi, která není redundantní (např. RAID řadič), nebo výpadek celého fyzického hosta, bude mít za následek výpadek kompletně celé infrastruktury. Jak je z popisu patrné, celé infastruktura je provozována jako "SPOF". Výpadek se tedy může vyšplhat řádově až na několik dnů.

2.10.1 Zálohování

Všechny zálohy jsou ukládány na serveru. Pro zálohování jsou použity samostatné pevné disky, které jsou vyhrazeny pouze pro zálohy. Jak a co se zálohuje:

Tabulka 4: Současný stav záloh (Zdroj: Vlastní zpracování)

Server	Co zálohujeme	Interval	Kolik dní zálohy uchováváme	Jak často provádíme rozdílové zálohy	Kdy probíhá zálohování	Předpokládaná doba obnovy
Server-x	Celý server – fyzický	Nikdy	-	-	-	-
Server-x	Celý server – virtuální	1x denně	5	Denně	5:00 – 6:00	20 minut
Server–x	Databáze	1x denně	7	Denně	2:00 – 3:00	5 minut
Server-x	Databáze transakční logy	Nikdy	-	-	-	-
Server-x	Filesystem (klientská data, interní data)	1x denně	7	Denně	4:00 – 5:00	10 minut

2.11 Požadavky v oblasti cloudových služeb

Protože společnost v současné době nevyužívá žádné cloudové služby třetích stran, nebude dále řešeno.

2.12 Závěr analýzy

Z celkové analýzy současného stavu infrastruktury vyplývá, že není absolutně připravena na bezvýpadkový provoz jako takový a už vůbec ne na to usilovat v současném stavu o implementaci bezpečnostních standardů. Pokud bude společnost chtít implementovat bezpečnostní standardy, bude nutné vynaložit další finanční prostředky na posílení serverové infrastruktury a také přijmout další zaměstnance.

2.13 Současný stav politik

Tabulka 5: Současný stav implementovaných politik (Zdroj: Vlastní zpracování)

Politiky	**Současný stav**
Manažerská část	
Klasifikace o ochrana informací	Neimplementováno
Řízení dodavatelů	Neimplementováno
Řízení lidských zdrojů	Neimplementováno
Řízení změn	Neimplementováno
Řízení kontinuitní činnosti	Neimplementováno
Audit kybernetické bezpečnosti	Neimplementováno
Technická část	
Fyzická bezpečnost	Implementováno
Řízení přístupů	Implementováno částečně
Požadavky v oblasti ochrany před škodlivým kódem	Implementováno částečně
Kybernetické bezpečnostní události a incidenty	Neimplementováno
Požadavky v oblasti aplikační bezpečnost	Implementováno částečně
Kryptografické prostředky	Implementováno částečně
Požadavky v oblasti zajišťování úrovně dostupnosti informací	Neimplementováno

3 Návrh řešení

Pro efektivní implementaci kybernetické bezpečnosti je nutné, aby byla zajištěna podpora a angažovanost nejvyššího vedení společnosti. To zahrnuje poskytnutí potřebných finančních, personálních a technických zdrojů, ale také vytvoření konkrétních bezpečnostních rolí a funkcí, vytváření bezpečnostních politik a dokumentace. Pro účinnou správu kybernetické bezpečnosti je nezbytné určit zodpovědnou osobu či role, které budou mít na starosti nejenom řízení a rozvoj bezpečnostních opatření, ale také pravidelné hodnocení stavu kybernetické bezpečnosti, zajištění plnění bezpečnostních plánů a komunikaci týkající se kybernetické bezpečnosti s vrcholovým managementem.

3.1 Klasifikace a ochrana informací

Pro klasifikaci informací bude používán Traffic Light Protocol (TLP) dle doporučení NÚKIB. Podle této metodiky budou hodnoceny informace z pohledu důvěrnosti, integrity a dostupnosti. Hodnocení informace vždy musí provézt garant informace.

3.1.1 Označení informací

- TLP: CLEAR – U takto označené informace není nutné dávat žádný štítek nebo značku. V případě označení bude v patičce uvedeno: *This item´s classification is Public.*

- TLP: GREEN – Interní informace z označení v patičce dokumentu: *This item´s classification is Internal. Do not distribute outside of the organization.*

- TLP: AMBER – Informace šířená v rámci organizace a partnerům třetí strany interními kanály. Označení: *This item´s classification is Restricted. Do not distribute to the third parites without owners approval.*

- TLP: AMBER + STRICT – Informace šířená pouze v rámci organizace: *This item´s classification is Restricted. Do not distribute outside of the organization.*

- TLP: RED – Většinou se jedná o verbální informace, které není možno nijak uložit. Pokud se jedná o dokumenty jsou označeny: *This item´s classification is Confidental. Do not distribute to the third parites without owners approval.* Při předávání informace tohoto charakteru je vždy nutný souhlas původce informace.

Tabulka 6: Klasifikace důvěrnosti (Zdroj: Vlastní zpracování)

Důvěrnost				
Úroveň	**Popis**	**Požadavky na ochranu**	**Likvidace/Změny**	**Zálohování**
Nízká	Veřejně přístupné informace. Nerušení důvěryhodnosti neohrožuje.	Nejsou kladeny žádné požadavky na manipulaci, nebo likvidaci.	Likvidace je možná. Změna bude verzovaná.	Dle vlastního uvážení.
Střední	Neveřejné informace bez právní ochrany.	Pouze pro interní potřebu, je možné dle domluvy postoupit třetí straně	Přepis média. Nutné verzování.	Pravidelné zálohování.
Vysoká	Neveřejné informace s právní ochranou.	Pouze pro interní potřebu, na základě smlouvy o NDA je možné postoupit třetí straně.	Fyzická likvidace média. Nutné verzovat.	Pravidelné zálohování.
Kritická	Neveřejné informace určené pouze pro vedení společnosti.	Vyžadováno šifrování. Nutnost schválení při předávání.	Skartace přenosového média, takovým způsobem, aby byly změny nevratné.	Pravidelné zálohování, dle individuální potřeby.

Tabulka 7: Klasifikace Integrity (Zdroj: Vlastní zpracování)

Integrita				
Úroveň	**Popis**	**Požadavky na ochranu**	**Likvidace/Změny**	**Zálohování**
Nízká	Narušení neohrožuje zájmy organizace.	Nejsou vyžadovány.	Bez omezení.	Nevyžadováno.
Střední	Narušení může způsobit poškození oprávněných zájmů organizace.	Nastavení přístupových oprávnění.	Omezení práv na změnu. Likvidace možná smazáním.	Nutno pravidelně zálohovat.
Vysoká	Narušení způsobí vážná poškození zájmů organizace.	Nutná implementace kryptografických prostředků na ochranu.	Omezení práv na změnu. Likvidace možná pouze zničením média.	Nutno zálohovat a kontrolovat.
Kritická	Narušení způsobí velmi vážná poškození zájmů organizace.	Nutné implementace MFA pro ověření oprávnění k přístupu.	Právo na změnu má pouze vedení společnosti. Likvidace možná pouze nevratným zničením média.	Zálohovat dle individuální potřeby.

Tabulka 8: Klasifikace Dostupnosti (Zdroj: Vlastní zpracování)

Dostupnost		
Úroveň	**Popis**	**Požadavky na ochranu**
Nízká	Výpadek v řádu několika dnů není s významný.	Pravidelné zálohování. Stačí 1x týdně.
Střední	Výpadek v řádu několika hodin.	Pravidelné zálohování. Stačí provézt 1x denně.
Vysoká	Výpadek v řádu několika minut.	Pravidelné zálohování. Testování obnovy na testovacím prostředí. Zálohování prováděno minimálně 2x za den.
Kritická	Výpadek v řádu několika minut.	Pravidelné zálohování na úrovní dat, ale také vytvářením snapshotů systému.

3.2 Řízení dodavatelů

Pro řízení dodavatelů bude jako podpůrný materiál využit dokument *Požadavky na smlouvy s dodavateli* vydaný NÚKIB ve verzi 1.4 platný kde dni 22.12.2022.(11)

3.2.1 Ustanovení o bezpečnosti informací

Ve smlouvě s dodavatelem bude uvedeno, jaké informace zpracovává a jejich popis z hlediska zajištění důvěrnosti, dostupnosti a integrity. Součástí všech smluv bude také ujednání o povinnosti seznámit se s interními směrnicemi a politikami společnosti upravující pravidla ochrany a manipulaci informací a likvidací dat. Dále budou popsána pravidla pro zajištění NDA, SLA a integrity informací, bude-li to nutné. (9)

3.2.2 Ustanovení o oprávnění užívat data

Smlouva o právech k datům. Bude stanoveno, komu data náleží, kdo má k datům užívací právo, jakým způsobem má dodavatel nakládat s daty a jak se k nim řídí přístup. Jako poslední bod bude uvedeno, jak s daty naložit po ukončení spolupráce. (9)

3.2.3 Ustanovení o autorství kódu

Ve smlouvě o autorství kódu bude stanoveno na základě, jaké licence je program dodáván a jaké jsou její podmínky. Dále bude uvedeno, zda je program dodáván s komponentou třetí strany, která spadá pod nějakou licenci. (9)

Také bude uvedeno, kdo je autorem zdrojového kódu, kdo má právo provádět změny v kódu a jak je možné s kódem dále nakládat. Mimo to bude také dodána kompletní dokumentace a ustanovení upravující, jak je možné s ní nakládat. (9)

3.2.4 Ustanovení o kontrole a auditu dodavatele

Smlouva o možnosti provést zákaznický audit. Obsahem bude, jak často, jakým způsobem, za jakých podmínek je možné audit provést. Také bude stanoveno, kam budou mít auditoři přístup. (9)

3.2.5 Ustanovení upravující řetězení dodavatelů

Pokud bude dodavatel určitou část služby, kterou nám bude dodávat, outsourcovat u subdodavatele, je nutné nám tuhle skutečnost neprodleně oznámit. Subdodavatel je povinen dodržovat stejná smluvní ujednání jako dodavatel, za tohle

chování odpovídá přímo dodavatel. V naší kompetenci je možné výběr subdodavatele zcela řídit a ovlivňovat. (9)

3.2.6 Ustanovení o povinnosti dodavatele dodržovat politiky

Povinnost dodavatele dodržovat bezpečnostní politiky společnosti. Pokud nebude uvedeno jinak, postupuje se podle toho, co je obsaženo ve všeobecných obchodních podmínkách. (9)

3.2.7 Ustanovení o řízení změn

Řízení změn probíhá na základě definované Standard Change nebo Normal Change. Standard Change je předem definovaný schválený proces, který probíhá pravidelně. Tzn. má popsanou změnu, den v týdnu a čas, kdy probíhá. Typicky jde o nasazování nové verze aplikace, která je vyvíjena za pomocí Agile přístupu.

V případě Normal Change, která není definována pravidelně, je nutné svolat CAB pro přezkoumání možných dopadů změny na produkční prostředí. Je nutné doložit možné riziko vyplývající z nasazení nové verze a doložit výsledek provozu z testovacího prostředí a jakým způsobem bude provedeno vrácení na původní verzi aplikace.

3.2.8 Ustanovení o souladu smluv s obecně závaznými předpisy

Obecně je vždy nutné dodržovat všechny zákony, vyhlášky, nařízení, evropské předpisy, obecně závazné vyhlášky apod. Pokud je ve smlouvě uvedena specifikace s konkrétním předpisem, je nutné se jím řídit. (9)

3.2.9 Povinnosti dodavatele informovat o incidentech

V případě bezpečnostního incidentu je nutné neprodleně kontaktovat povinný subjekt, který je incidentem zasažen. (9)

3.2.10 Povinnosti dodavatele informovat o způsobu řízení rizik

Povinností dodavatele je podrobně popsat a rozvést, jakým způsobem nebo metodou budou řízeny rizika a také jaké jsou zbytková rizika související s plněním smlouvy. Pokud to bude možné, bude s dodavatelem sjednána možnost kontroly způsobu řízení rizik v rozsahu, který se dotýká plnění smlouvy. (9)

3.2.11 Povinnosti dodavatele informovat změně vlastnictví

Pokud dojde k vlastnické změně dodavatele, je nutné nás o této skutečnosti neprodleně informovat. (9)

3.2.12 Ustanovení o právu jednostranně odstoupit od smlouvy

Jako bylo popsáno výše, pokud dojde ke změně vlastnictví dodavatele, je nutné mít možnost odstoupení od smlouvy, případně pokud dojde k významné změně kontroly nad dodavatelem. Důležité je se vyvarovat plné závislosti na dodavateli tzv. vendor lock-in. (9)

3.2.13 Specifikace podmínek při ukončení smlouvy

Při ukončení spolupráce s dodavatelem bude stanovena délka přechodného období pro pravidla migrace dat, poskytování součinnosti budoucímu dodavateli a poskytování know-how novému dodavateli. Dále bude definováno, jakým způsobem bude předána provozní dokumentace. Jak bylo uvedeno v předešlém odstavci, je nutné dávat velký pozor na vendor lock-in. (9)

3.2.14 Specifikace podmínek pro řízení kontinuity činností

Stanovení podmínek dodavatele pro řízení kontinuitní činnosti a součinnost při zapojení v případě havarijních plánů. (9)

3.2.15 Specifikace podmínek pro formát předání dat

Bude definováno, jakým způsobem a v jakém formátu budou předány data v rámci tzv. **exit strategie**. Formát a způsob se bude lišit v závislosti na tom, o jaká data se bude jednat. V případě, že se bude jednat o provozní data, která bude nutné likvidovat, bude definováno, jakým způsobem a bude vyžadováno prohlášení o tom, že data byla skutečně zlikvidována. (9)

3.2.16 Pravidla pro likvidaci dat

Způsob likvidace dat bude vždy popsán na základě toho, o jak citlivá a důležitá data se jedná. Na základě tohoto popisu bude určen způsob jejich likvidace. Nejčastěji se bude jednat o smazání nebo zničení dat z fyzického nosiče, na kterém jsou zapsána. (9)

3.2.17 Ustanovení o sankcích za porušení povinností

Stanovení sankcí za porušení pravidel bude vždy adekvátní k ceně poskytované služby dodavatelem tak, aby bylo dosaženo odstranění nedostatků nebo plnění všech stanovených povinností. (9)

3.3 Řízení lidských zdrojů

Všem interním a externím zaměstnancům je 1x ročně stanoveno školení na základy kybernetické bezpečnosti, a to formou online testu, který musí absolvovat na 100 %. Pro administrátory, správce systému je pořádáno školení navíc v případě, že se objeví nové vyhlášky nebo jejich úprava.

3.3.1 Řízení zaměstnanců

Všichni zaměstnanci jsou pravidelně testováni na bezpečnosti pomocí phishingových mailů, které mají za účel otestovat jejich teoretické znalosti uvedené do praxe. Pokud zaměstnanec zaregistruje podezřelý mail nebo si není jistý jeho důvěryhodností, měl by jej přeposlat na adresu abuse@****ting.cz, kde bude mail přezkoumán příslušným oddělením. Zaměstnanec bude dále instruován, jak se má zachovat.

3.3.2 Řízení zákazníků

Pro zákazníky je na oficiálních stránkách společnosti vystaven blog, který je pravidelně aktualizován. Obsahuje nejenom novinky o společnosti, ale z větší míry je zaměřen na bezpečnost, a to tak, aby reflektoval námi nabízené a provozované služby. V případě, že zákazník zaznamená neobvyklé chování systému nebo bude mít podezření, že něco není v pořádku, může neprodleně kontaktovat zákaznickou podporu a požádat o součinnost s prověřením nastalé situace.

3.4 Řízení změn

V případě prováděných změn informačního nebo komunikačního systému, je nutné celou změnu zapsat a zdokumentovat její jednotlivé kroky, včetně plánu vrácení do předchozího stavu a také důkladného otestování změny. Změna bude probíhat následujícím způsobem:

1. Svolání CAB, kde bude přednesen požadavek na změnu, včetně popisu, o jakou změnu se jedná, čeho se změna týká, uvedení všech komponent, kterých se změna dotýká, zda bylo možné změnu otestovat na testovacím prostředí, časový odhad prováděné změny, jakým způsobem bude probíhat testování, které dokumenty bude nutné upravit a jak bude v případě neúspěchu probíhat rollback plán.
2. Pokud bude změna předschválena, bude vytvořen ticket, ve kterém budou všechny výše zmíněné změny zaznamenány.
3. Bude vytvořen a zaznamenán plán jednotlivých kroků změny, a to v nástoji k tomu určeném (např. MS Excel, LibreOffice Calc, RTP tool,…), včetně časových odhadů a rollback plánu.
4. Následně může být ticket poslán na schválení. Musí tak být učiněno nejpozději 24 hodin před plánovanou změnou, aby bylo možné včas informovat všechny subjekty, kterých se bude změna týkat.

3.5 Řízení kontinuitní činnosti

Pro řízení plánu obnovy a kontinuitní činnosti bude vypracován samostatný dokument, který popisuje jednotlivé situace a jak se v těch situacích zachovat. Oba dokumenty musí být popsány tak, aby v případě havárie bylo možné zajistit správnou funkci informačního a komunikačního systému. Problémy spojeny s obnovou po havárii jsou úzce spjaty s nepřetržitým chodem organizace. Tento plán obnovy provozu organizace se týká jejího informačního systému, dat nebo infrastruktury po vzniku havárie.

3.5.1 BCP – Business Continuity Plan

Jako první bod je nutné definovat osoby, které se podílejí na chodu organizace a přiřadit jim jejich zodpovědnosti v případě nastalé mimořádné události.

Tabulka 9: Role a zodpovědnosti při BCP (Zdroj: Vlastní zpracování)

Role	Zodpovědnost
Vedení (CTO, CEO)	Je zodpovědný za kompletní správu IT infrastruktury a koordinaci činností technického týmu.

CISO	Monitoruje bezpečnostní hrozby a zajišťuje, že všechny bezpečnostní protokoly jsou aktualizovány a dodržovány.
Administrátoři	Provádějí technické úkony potřebné k obnově operací, jako je obnova dat a spuštění záložních systémů.
Zákaznická podpora	Informuje klienty o stavu a předpokládaném čase obnovy služeb, zajišťuje komunikaci s klienty a veřejností.

Druhým klíčovým krokem v procesu vyhodnocení a posouzení rizik ohrožujících kontinuitu činností je sestavení možných scénářů, které mohou v organizaci nastat. Tento krok zahrnuje identifikaci a analýzu různých událostí, které by mohly vést k přerušení běžného provozu, viz. *Tabulka 10*.

Tabulka 10: Scénáře ohrožující kontinuitní činnost (Zdroj: Vlastní zpracování)

Scénář	Důvěrnost dat	Dostupnost dat	Integrita dat
Výpadek serveru	Při obnově může dojít k porušení bezpečnosti, což může vézt k neoprávněnému přístupu.	Přímo ovlivněna.	Možné poškození dat, nebo jejich ztráta.
Kybernetický útok	Možnost získání neoprávněného přístupu k citlivým informacím.	DDoS útok zapříčiní nedostupnost online služeb (webových stránek, mailových služeb).	Škodlivé kódy zašifrují data nebo zablokují přístup k nim.
Lidská chyba	Veřejné publikování citlivých interních informací.	Nesprávná konfigurace serveru, která způsobí jeho přetížení.	Nesprávná konfigurace databáze, která způsobí nekonzistenci dat.

Třetí klíčovou oblastí je stanovení minimální úrovně infrastruktury, která je stále schopna zachovat základní služby systému v chodu. Tento parametr je zásadní pro plánování kontinuity provozu a obnovy po haváriích, neboť specifikuje, jaké zdroje a kapacity musí být minimálně k dispozici, aby systém mohl nadále poskytovat klíčové služby i v omezených podmínkách. Jedná se o následující:

- 1x fyzický sever
- 3x virtuální servery – Mail server, webový server a IDM server
- 1x LXC kontejner – Webové rozhraní klientské aplikace

Při zachování výše uvedené funkčnosti je možné značnou kapacitu přesunout na práci k obnovení chodu nebo dat infrastruktury.

3.5.1.1 RTO

Doba obnovení chodu (Recovery Time Objective – RTO) infrastruktury po havárii je stanovena na **60 minut**. Po této době již může dojít k negativním dopadům na podnikání. Tedy jako odliv klientů ke konkurenčním společnostem a poškození jména vedení. V případě překročení uvedené doby bude zákazníkům jako kompenzace nabídnuta výrazná sleva na předplatné služeb.

3.5.1.2 RPO

Bod obnovení dat (Recovery Point Objective – RPO). V tabulce níže jsou definována časová období, za která musí dojít k obnově dat po havárii systému. Uvedené časy vycházejí z provedení obnovení na testovacím prostředí, kde byly obnovy testovány.

Tabulka 11: Čas obnovy dat (Zdroj: Vlastní zpracování)

Data	Požadovaný čas obnovy
Hostingová data	15 minut
Mailové zprávy	25 minut
Databáze	45 minut
Virtuální server	60 minut
LXC Kontejner	25 minut

3.6 Audit kybernetické bezpečnosti

Provádění auditu kybernetické bezpečnosti můžeme rozdělit na dvě kategorie, a to audit interní a audit prováděn externí společností. Vedení společnosti má zájem a podporuje provádění auditu v obou uvedených případech. S výsledky auditu bude možné dále pracovat jako se zdrojem informací, který je možno použít pro další plánování a zlepšování bezpečnosti. Hlavní soubor domén, které budou přezkoumávány jsou:

- bezpečnostní dokumentace a bezpečnostní politiky organizace,
- právní předpisy,
- smluvní závazky, které se vztahují k informačnímu nebo komunikačnímu systému

3.6.1 Interní audit

Interní audit bude prováděn interním zaměstnancem společnosti, který je zodpovědný za provoz. Audit bude prováděn pravidelně 1x ročně a při mimořádných bezpečnostních událostech, bude vyžadováno provedení interního auditu do 1 měsíce od uskutečnění události nebo incidentu.

3.6.2 Externí audit

Pro externí audit bude využíváno společností třetích stran, která jsou pro to vyškolena. Dále je nutné, aby se jednalo o společnosti, které nejsou s naší organizací spjaty dalšími smlouvami a nedodávají žádné jiné služby. Na činnost organizace provádějící audit bude dohlížet zaměstnanec, který má na starosti provádění interního auditu. Bude stanoveno, že externí audit je nutné provádět minimálně jednou za 2 roky.

3.7 Fyzická bezpečnost

Současně využívané datové centrum třetí strany je z pohledu základního zajištění fyzické bezpečnosti dostačující. Vzhledem k tomu, že bude nutné celou stávající fyzickou (serverovou) infrastrukturu vybudovat od začátku, bylo vybráno nové datacentrum, kam bude postupně celá infrastruktura migrována. Výběr nového DC byl zcela logickým krokem, který reflektuje kvalitnější, a dokonce i nižší cenu za poskytované služby, než máme v současné době. Další a celkem zásadní důvod

přechodu je ten, že společnost provozující DC se věnuje komplexnímu řešení Kybernetické bezpečnosti a je certifikovaným partnerem **Národního úřadu pro kybernetickou a informační bezpečnost** (NÚKIB).

Nově vybrané DC dokonce splňuje bezpečnostní a technologické standardy TIER IV, kde jsou kladeny i nároky na udržitelnost, to znamená že splňují požadavky na energetickou nenáročnost a minimální ekologickou zátěž provozu.

3.7.1 Napájení DC

DC je zásobováno elektrickou energií ze dvou transformačních stanic. Jedna trafostanice je ve vlastnictví společnosti a je umístěna na jejich vlastním pozemku. Pro zajištění nepřerušovaného provozu v případě výpadku elektrického napájení jsou k dispozici dva dieselové generátory, které byly testovány na schopnost udržet nepřetržitý chod po dobu tří dnů. Každá z napájecích větví je navržena tak, aby zvládla plnou zátěž a je vybavena samostatným UPS systémem pro ochranu před krátkodobými výpadky.

3.7.2 Chlazení

Systém chlazení datacentra je strukturován do dvou nezávislých obvodů, přičemž každý z nich disponuje chladicí kapacitou přesahující plánované potřeby datacentra a skládá se z více samostatných jednotek.

3.7.3 Konektivita

Samotné datové centrum je propojeno prostřednictvím tří geograficky oddělených optických cest. Redundance spojení je zajištěna pomocí protokolů BGP a TRILL. K dosažení úplné síťové neutrality je možné využít služby dalších telekomunikačních operátorů.

3.8 Řízení přístupů

Pro naše řízení přístupů ve společnosti je nutné vytvořit úplně nové definice, politiky a pravidla. Dále je nutné rozlišovat přidělování přístupů zákaznickým účtům a zaměstnancům společnosti.

3.8.1 Definice rolí a zodpovědnosti

V první řadě je nutné vydefinovat jednotlivé role a zodpovědnosti a přiřadit specifické úrovně přístupových práv na základě jejich potřeb.

3.8.1.1 Interní (externí) zaměstnanci

Vzhledem k současné velikosti společnosti by rozdělení a definování jednotlivých rolí mohlo vypadat následovně:

Tabulka 12: Role zaměstnanci (Zdroj: Vlastní zpracování)

	Vedení společnosti	Správci systému	Zákaznická podpora	Zaměstnanci
CTO	●			
CEO	●			
CISO	●			
SysAdmin		●		
DevOps		●		
Support			●	
Accountant				●
BackOffice				●
Sales Manager				●

3.8.2 Zákazníci

V případě role zákazníka se vždy bude jednat o jedno ze dvou v současné době nabízených hostingových řešení. Samozřejmě je možné, aby měl zákazník na jednom účtu zřízeny obě možnosti služeb.

Tabulka 13: Role zákazníci (Zdroj: Vlastní zpracování)

	Zákazník	Významný zákazník
Sdílený hosting	●	●
LXC hosting	●	●

3.8.3 Politika přístupů

Politika přístupů je zásadní prvek v rámci řízení informační bezpečnosti v organizacích. Její základní úlohou je zajištění, že pouze autorizované osoby mají přístup k citlivým datům a systémovým zdrojům, a to v souladu s jejich pracovními pozicemi a potřebami. Tato politika je nezbytná pro zabezpečení informací a systémů proti neautorizovanému přístupu a potenciálním bezpečnostním rizikům.

3.8.3.1 Zaměstnanci

Tabulka 14: Politika přístupů zaměstnanci (Zdroj: Vlastní zpracování)

	Vedení společnosti	Správci systému	Zákaznická podpora	Zaměstnanci
Správa serverů	●	●	●	
Fyzická přístup do serverovny	●	●		
Administrátorský přístup na server	●	●		
Uživatelský přístup na server	●	●	●	
Monitoring	●	●	●	
Správa projektů	●	●		
Git repositář	●	●		
IDM	●	●		
Administrace DNS záznamů	●	●	●	
Hosting znalostní báze	●	●	●	
Obecná znalostní báze	●	●	●	●
Klientská	●	●	●	

znalostní báze				
Metriky systému	●	●	●	
Software pro sdílení souborů	●	●	●	●
CRM systém	●			●
Účetní software	●			●

3.8.3.2 Zákazníci

Tabulka 15: Politika přístupů zákazníci (Zdroj: Vlastní zpracování)

	Zákazník	**Významný zákazník**
Uživatelský přístup na server	●	●
Git repositář		●
Administrace DNS záznamů	●	●
Klientská znalostní báze	●	●
Metriky systému		●
Software pro sdílení souborů		●

3.8.4 Implementace systému pro správu identit (IDM)

Jako hlavní nástroj pro správu identit a politik přístupu byl zvolen open-source systém **FreeIPA.** Jedná se o bezplatný otevřený systém, který byl vyvinut společností *Red Hat*. Poskytuje hlavně centralizovanou správu autentizace a autorizace účtů. Hlavními důvody, proč byl nástroj vybrán jsou:

- **Centralizovaná správa uživatelů a skupin** – jednotné řešení pro správu uživatelů, skupin a hostů (virtuální a fyzické servery). To znamená usnadnění přidávání, odstraňování nebo úpravu účtů.
- **Autentizace a autorizace** – široká škála autentizačních metod jako je použití hesel, Kerberos ticketů, nebo certifikátů.
- **Správa přístupových politik** – definování oprávnění a přístupů založené na rolích (RBAC)

- **Integrace** – Protože potřebujeme jednotné přihlášení jak do operačního systému, tak i do aplikace máme vše na jednom místě.
- **Zabezpečení a šifrování** – podporuje funkce pro ochranu dat a komunikace. Je možno využití SSL/TLS pro šifrování síťových přenosů.
- **Webové rozhraní a CLI** – nástroj samotný je možno ovládat přes webové rozhraní nebo je možné použít příkazovou řádku.
- **Audit a sledování** – Obrovská přidaná hodnota spočívá v tom, že nástroj umožňuje sledování aktivit uživatelů a administrátorů, což umožňuje detekci a reakci na způsobené bezpečnostní incidenty.

3.8.5 Vícefaktorová autentizace MFA

3.8.5.1 Zaměstnanci

Pro přihlašování do všech informačních systémů je nutné používat dvoufaktorovu autentizaci. Všichni interní, potažmo externí zaměstnanci, musí mít nastavené dvoufaktorové ověřování pomocí mobilního telefonu, na které je zaslán ověřovací kód pro přihlášení.

Byl zvolen nástroj **2FAS (Two Factor Authentication System),** a to z důvodu jeho snadného použití a také proto, že je multiplatformní. Je možné jej provozovat na na iOS i Android zařízení, ale také jako rozšíření ve webové prohlížeči. Dalším důvodem je, že aplikace samotná pro získání ověřovacího tokenu vyžaduje pro přístup ověření, a to buď biometrický (otisk prstu, naskenování obličeje) nebo pomocí zvoleného pin kódu.

3.8.5.2 Zákazníci

Pro zákazníky není vyžadována dvoufaktorová autentizace, je však výslovně doporučena. Je také doporučeno používat stejnou aplikaci jako je tomu v případě zaměstnanců.

3.8.6 Školení a osvěta

3.8.6.1 Zaměstnanci

Pro zaměstnance jsou pořádány pravidelná školení a workshopová cvičení o bezpečnosti, které zahrnují nejen dvoufaktorovou autentizaci, ale i další důležité aspekty kybernetické bezpečnosti. Tato školení jsou navržena tak, aby poskytla zaměstnancům nezbytné znalosti a dovednosti pro ochranu firemních dat a systémů.

3.8.6.2 Zákazníci

Pro zákazníky, kteří chtějí zlepšit svou bezpečnost při přihlašování, je důležité, aby se seznámili s principy a praktikami dvoufaktorové autentizace (2FA). Na našem blogu na oficiálních stránkách společnosti pravidelně publikujeme články, které se věnují bezpečnostním rizikům spojenými se službami, které provozujeme. Tyto články jsou zaměřené na osvětu a poskytování praktických rad, jak se chránit před kybernetickými hrozbami.

3.8.7 Politika hesel

Politika hesel je stanovena stejně pro všechny typy účtů. Tedy pro privilegované a uživatelské účty.

- Minimální délka hesla je 18 znaků.
- Heslo musí obsahovat velká písmena, malá písmena, číslice a speciální znaky.
- Maximální doba platnosti hesla je 3 měsíce.
- Zákaz používaní stejného hesla.
- Zamčení účtu po 5 neplatných přihlášení.
- Jednorázové prvotní heslo musí být změněno do 24 hodin.

3.9 Požadavky v oblasti ochrany před škodlivým kódem

Hlavním důvodem ochrany před škodlivým kódem je snížení dopadů a pravděpodobnosti, že k napadení vůbec dojde. Způsoby ochrany by měli být následující.

3.9.1 Segmentace sítě

Tabulka 16: Segmentace sítě (Zdroj: Vlastní zpracování)

Kde je použito	Popis	Rozsahy
Fyzické a virtuální servery	Veřejné IPv4 a IPv6 adresy přiděleny datacentrem	109.105.xx.xx/xx 2001:4ba8:xx.xx.xx/xx
Interní LXC kontejnery	Interní IPv4 podsíť	10.0.xx.xx/xx
Zákaznické LXC kontejnery	Interní IPv4 podsíť	172.16.xx.xx/xx

3.9.1.1 Fyzické a virtuální servery

Fyzické a virtuální servery jsou stavěny na veřejně dostupných IP adresách přidělených datacentrem. Každý nově postavený server má automaticky zapnutý firewall, kde je standardně všechna komunikace směrem z internetu zakázána. Povolování firewallu a jednotlivých portů se děje až následně podle toho, jaké služby na serveru běží a podle toho, zda mají být dostupné přímo z internetu nebo jenom interně.

3.9.1.2 Interní LXC kontejnery

Interní kontejnery postaveny na technologii LXC (LinuxX Containers) jsou používány pro provoz interní nástrojů jako je např. ticketovací systém a nástroj pro správu uživatelů. Hlavní důvod je mít oddělené administrativní nástroje od produkčních systémů.

3.9.1.3 Zákaznické LXC kontejnery

Zákaznické kontejnery využívají stejnou technologii jako interní s tím rozdílem, že se jedná o neprivilegované prostředí. Zákazník tedy dostane před připravené prostředí na provoz aplikace. Nemá přístup k administrátorskému účtu (root) a nemá možnost instalace jakýchkoliv dalších balíčků. Má tedy možnost nahrát pouze vlastní aplikaci a editovat vybrané konfigurační soubory související s provozem aplikace.

3.9.2 SW pro detekci a odstranění škodlivého kódu

Všechny naše používané aplikace běží na operačních systémech linux nebo UNIX, jako je například BSD, není až tak nutné používat antivirové řešení pro kontrolu operačního systému. Není možné říct, že viry pro tento druh systému neexistují, ale vzhledem k tomu, jak je navržena koncepce řízení uživatelských oprávnění, nedochází k fatálnímu ovládnutí systému, které by mělo za výsledek výpadek služeb. Může ovšem dojít k narušení Integrity a důvěrnosti informací.

3.9.2.1 ClamAV

Hlavním používaným nástrojem pro detekci škodlivého kódu je **Clam AntiVirus** (ClamAV). Jedná se multiplatformní antivirové řešení. V našem případě tedy není problém instalovat toto antivirové řešení na OS linux nebo UNIX. Instalace a konfigurace uvedeného nástroje je jednoduchá a dá se provádět automatizovaně. Je tedy možné zvolit jinou konfiguraci per server. Aplikace běží jako systémový démon. Aktualizace databáze probíhá automaticky několikrát za den, ale je možné ji též vyvolat ručně. V konfiguraci je možné nastavit, které složky nebo soubory se mají skenovat, co se v případě odhalení škodlivého kódu má stát, tudíž je možné nastavit, aby program vykonal akci smazání určitého souboru nebo poslal jenom notifikace o jeho odhalení.

Protože na naší infrastruktuře také provozujeme mailové služby, je uvedený program logickou volbou, protože jeho hlavní způsob použití je právě pro detekci virů v e-mailech na straně poštovních serverů. Je možné kontrolovat také mnoho formátů souborů, které jsou posílány jako přílohy mailové komunikace. Např. Zip, RAR, Tar, Gzip, RTF, PDF.

3.9.2.2 Aktualizace OS

Mezi významné zdroje, které přispívají k bezpečnosti systému, patří sledování CVE, tedy veřejně dostupných zranitelností v oblasti kybernetické bezpečnosti. Ať už se jedná o verzi firmware fyzického serveru, operační systém nebo samostatných programů na něm provozovaných. Protože většina programového vybavení je instalováno ze standardních systémových balíčků operačního systému, dochází při aktualizaci OS, také k aktualizaci instalovaných programů. Pokud je to možné, dochází k otestování aktualizace na testovacím prostředí, a to hlavně z důvodů změny, nebo

způsobu konfigurace některých programů. Výše uvedené může v případě produkčního systému zapříčinit zbytečnou nedostupnost služeb.

Tabulka 17: Intervaly aktualizací (Zdroj: Vlastní řešení)

Co	Typ aktualizace	Interval	Čas
OS (fyzický server, virtuální server)	Periodická	1x měsíčně	20:00 – 2:00
	Kritická	Dle potřeby	Po pracovní době
Firmware (fyzický server)	Periodická	1x ročně	Nutná úplná odstávka
	Kritická	Dle potřeby	Nutná úplná odstávka
Interní LXC kontejnery	Periodický	1x měsíčně	18:00 – 20:00
	Kritický	Dle potřeby	Možno i během pracovní doby
Zákaznické LXC kontejnery	-	-	-

Zákaznické kontejnery není možné pravidelně aktualizovat. S největší pravděpodobností by došlo k výpadku zákaznické aplikace. Zákazník je informován o možných bezpečnostních zranitelnostech v jeho prostředí. K vyřešení nastalé situace je možné použití dvou způsobů:

1. Zákazník si naplánuje odstávku jeho systému a v administraci systému si vytvoří nové prostředí s aktualizovaným OS. Velkou nevýhodou tohoto řešení je, že bude muset svou aplikaci znovu nasadit a nakonfigurovat.
2. Zákazník v administraci provede aktualizaci svého prostředí s tím, že akceptuje možný výpadek aplikace. V tomto případě se nejedná o tak veliký zásah. V tom lepším případě nebude potřeba dělat s nasazenou aplikací vůbec nic, v tom horším bude například nutná úprava konfigurace a tom nehroším přepsání části aplikace.

V obou případech je však možné využít rollback a tím provedené změny vrátit zpět do původního funkčního stavu před aktualizací prostředí.

3.10 Kybernetické bezpečnostní události a incidenty

Před samotným stanovením postupu, jak reagovat na bezpečnostní události a incidenty, je nejprve nutné interně stanovit, co za událost nebo incident považujeme. Viz. vypracované tabulky níže s postupy, jak při odhalení incidentu reagovat. Je nezbytně nutné o vzniklé události informovat vedení společnosti, které případně stanový další postup.

3.10.1 Phishing

Tabulka 18: Událost phishing (Zdroj: Vlastní zpracování)

Aktivita	Jak reagovat?
Obdržení e-mailové zprávy, která se snaží vylákat citlivé informace.	Neklikat na odkazy. Ověřit identitu odesílatele. Přeposlat email na adresu abuse@****hosting.cz.

3.10.2 Malware

Tabulka 19: Událost malware (Zdroj: Vlastní zpracování)

Aktivita	Jak reagovat?
Škodlivý software na počítači nebo serveru	Identifikovat a analyzovat typ malware. Pokud je to možné, obnovit data ze zálohy. Aktualizovat OS.

3.10.3 DDoS útok

Tabulka 20: Událost DDoS útok (Zdroj: Vlastní zpracování)

Aktivita	Jak reagovat?
Přetížení webových služeb	Dočasná změna TTL u DNS záznamů. Přesměrování DNS záznamů. Žádost o pomoc na úrovni DC.

3.10.4 Zero-day útok

Tabulka 21: Událost Zero-day útok (Zdroj: Vlastní zpracování)

Aktivita	Jak reagovat?
Útok na ještě neznámé zranitelnosti software nebo hardware	Úplná izolace aplikace od běžného provozu. Neprodlené kontaktování vývojáře software.

3.10.5 Úniky dat

Tabulka 22: Událost únik dat (Zdroj: Vlastní zpracování)

Aktivita	Jak reagovat?
Neúmyslné zveřejnění citlivých informací.	Odpojení serverů od sítě nebo jejich úplné vypnutí. Analyzovat logy všech zdrojů. Oznámení všem zainteresovaným stranám (pokud se jich to týká).

Je nezbytné zaznamenat a analyzovat každou z uvedených událostí, což umožní vylepšení bezpečnostních protokolů a preventivních opatření. Pečlivá dokumentace a reportování jsou zásadní pro rozpoznání příčin úniků dat a zajištění efektivnějšího zvládání podobných situací v budoucnu.

Datacentrum, kde jsou umístěny naše servery, disponuje vlastním bezpečnostním týmem CSIRT. V případě zjištění incidentu s potenciálně širokým dopadem lze incident oznámit přímo zde.

3.10.6 Zdroje logů

Jednotlivé logy jsou kategorizovány do několika skupin. V této části budou jednotlivé skupiny popsány a budou jim přiřazeny zařízení a události, které obsahují.

3.10.6.1 Skupina SEC

V našem případě sem patří autentizační servery Kerberos a RADIUS, které komunikují s IDM nástrojem FreeIPA. Zde jsou uchovávány logy s obsahem, kdo a

jakým způsobem přistupoval na server a který učet se hlásil do informačního nebo komunikačního systému.

3.10.6.2 Skupina OS

Zahrnuje záznamy systémových událostí, jako jsou spuštění a ukončení služby nebo její selhání. Tyto logy pocházejí převážně ze serveru.

3.10.6.3 Skupina APP

Zde jsou logy, které dokumentují provoz aplikací. Především:

- Komunikace klient – server (C<>S)
- Informace o přihlášení
- Aktivita uživatelů (Aktivita)
- Pády aplikace, ukončení aplikace (Akce)

Všechny výše uvedené logy, je nutné uchovávat po určitou dobu, viz. *Tabulka 23*.

Tabulka 23: Minimální počet dnů uchování logů (Zdroj: vlastní zpracování dle: [9])

SEC				
Počet dní	60			
OS	**Systém**	**Audit**		
Počet dní	30			
APP	**C<>S**	**Využití účtů**	**Aktivita**	**Akce**
Počet dní	7	7	1	30

3.10.7 Centrální log management

Jako centrální řešení pro kolektování logů ze všech systému byla vybrána technologie ELK Stack. Jedná se o spojení nástrojů Elasticsearch, Logstash a Kibana. Všechny uvedené nástroje jsou open-source a umožňují efektivní manipulaci, prohledávání a zobrazování rozsáhlých objemů dat v reálném čase.

3.11 Požadavky v oblasti aplikační bezpečnosti

Pro implementaci bezpečnostních standardů bude nutná migrace celého serverového řešení do nové datacentra. Z tohoto důvodu se jeví ponechání serveru v současném datacentru jako vhodný nástroj pro provoz testovacího prostředí.

Jako primární cíl testovacího prostředí je v našem případě interně vyvíjená webová aplikace pro administrace hostingových služeb, která je navázána na spoustu interních, ale také externích integrací. Samotná aplikace je postavena na webovém frameworku **Django** a vyvíjena v jazyce **Python**. Mezi hlavní interní integrace patří mailové služby (vytváření e-mailových schránek a aliasů), správa DNS záznamů, limity služeb, Cron úlohy aj. Před produkčním nasazením je nutné všechny komponenty otestovat, a to jak z pohledu funkčního, ale také z pohledu zabezpečení.

Při vývoji a testování není nutné používat produkční data s výjimkou domén. Protože společnost má několik vlastních testovacích domén ve správě, není nutné žádným způsobem data anonymizovat nebo maskovat.

3.11.1 Interní testování zabezpečení webové aplikace

Zabezpečení aplikace je možné otestovat z naší strany, a to za pomoci dostupných operačních systémů a open-source nástrojů k tomu určených. Jako nejvhodnější se jeví použití OS Kali linux nebo Parrot OS. Jedná se o linuxové distribuce základem vycházející z distribuce Debian, která patří do rodiny OS GNU/Linux s předinstalovanými programy k provádění penetračního testování, hledání zranitelností a forenzní analýzy.

Testování může probíhat v několika úrovních. Podle způsobu provedení na automatizované nebo manuální testy. Testy můžeme dále rozdělit podle použité techniky na pasivní nebo aktivní, nebo podle úrovně znalostí systému. K provádění testů bude nutné přijmout nebo vyčlenit alespoň jednoho zaměstnance na pozici **Tester.**

3.11.2 Testování externí společností

Pro nezávislou bezpečnostní analýzu aplikace je možné poptat externí společnost, která provede otestování webové aplikace. Společnost by s námi neměla mít uzavřenou žádnou další smlouvu na poskytování nebo dodávání služeb. Před

provedením analýzy bude nutné definovat jednotlivé kroky a komponenty, kterých se má testování týkat.

3.12 Kryptografické prostředky

3.12.1 Šifrování pevných disků

Všechny pevné disky používané ve fyzických serverech jsou používány v RAIDu, nebo chcete-li jako diskové pole. Nejčastěji je používán RAID 1, pro který je nutné použít minimálně dva disky a data jsou zrcadlena na všechny disky v poli. Disková pole jsou rozdělena na systémové a datové disky. Systémové disky jsou šifrovány na úrovni operačního systému pomocí algoritmu AES a šifrovacím módem XTS s délkou klíče 256 bitů. V případě použití datových disků, na kterých jsou stavěny virtuální servery jsou disky šifrovány pomocí stejného algoritmu a také na úrovni OS.

3.12.2 Šifrování dat

Zákaznická data a některá data společnosti jsou šifrována na úrovni souborového systému. Hlavním důvodem je, že šifrování zabraňuje neoprávněným osobám v přístupu k citlivým datům, což pro nás jakákoliv zákaznická data jsou. Šifrovací algoritmus je používán stejný, jako je tomu v případě šifrování pevných disků. Je použit algoritmus AES se šifrovacím módem XTS a délkou klíče nejméně 256 bitů.

3.12.3 Externí zařízení

Připojování USB disků nebo vkládání SD karet do fyzické serveru je mimo základní instalaci operačního systému zakázáno. Mezi hlavní prvky ochrany patří použití tzv. Bezel. Jedná se o přední uzamykatelný rámeček umístěný na fyzickém serveru, který zabraňuje nechtěnému vypnutí nebo restartování serveru, vytažení pevných disku a mimo jiné omezuje přístup k USB portům pro připojení zařízení.

Obrázek 6: Pohled na přední stranu serveru bez Bezel (Zdroj: https://www.router-switch.com)

Obrázek 7: Pohled na přední stranu serveru s umístěným Bezel (Zdroj: https://www.router-switch.com)

Zadní USB konektory jsou dostupné ze zadní části rackového stojanu. Zde není možné umístit žádný rámeček, proto jsou USB konektory zakázány na úrovni BIOSu.

Obrázek 8: Pohled na zadní stranu serveru (Zdroj: https://www.router-switch.com)

3.12.4 Ukládání hesel

Všichni zaměstnanci – Pro ukládání hesel je možné používat osobní klíčenku v podobě aplikace Keepass a jejích derivátů. Je zakázáno ukládat hesla do internetových prohlížečů.

Správci systému a administrátoři – Pro sdílení systémových hesel je používána klíčenka Gopass šifrovaná pomocí GPG klíče a verzována v systému Git. Tato klíčenka bude také napojena na automatizaci, která instaluje infrastrukturu. Protože vytváření systémových hesel probíhá automatizovaně, je nutné hesla shromažďovat a udržovat přístupná pro administrátory.

Webová klientská aplikace – Pro přístup do aplikace pro správu hostingových služeb je používá interně vyvíjená klientská aplikace. Při první registraci uživatele je mu automaticky vygenerováno a zasláno heslo na e-mailovou adresu s upozorněním, ať

si heslo co nejdříve změní. Heslo je uloženo v hashované podobě přímo v databázi aplikace. Jako hashovací algoritmus je používán **Bcrypt**.

3.13 Požadavky v oblasti zajišťování úrovně dostupnosti informací

Je zcela zásadní zajistit vysokou dostupnost naší infrastruktury, protože jakýkoliv výpadek má bezprostředně negativní vliv a dopad na celé naše podnikání a také reputaci společnosti. Je tedy nezbytné implementovat robustní řešení, které minimalizuje riziko výpadků a zajistí co největší dostupnost.

3.13.1 Řešení vysoké dostupnosti

Nový návrh řešení zahrnuje implementaci tři nodového systému. Tento přístup vyžaduje tři identické servery s totožnou konfigurací procesorů, operační paměti a pevných disků. Tyto servery budou integrovány do jednoho clusteru, což také zaručuje efektivní distribuci zátěže. Hlavním důvodem vybudování clusterového řešení je, že v případě výpadku jednoho fyzického serveru se všechny na něm běžící virtuální servery řádově během vteřin zmigrují na jeden ze dvou stále běžících serverů.

3.13.2 SPOF

Realizací vysoké dostupnosti (High Availability, HA) podle navrhovaného tří nodového systému dojde k úplnému odstranění SPOF (Single Point of Failure). Toto řešení zajistí, že infrastruktura bude robustnější a schopná udržet nepřetržitý provoz i v případě výpadku jednoho ze serverů, což výrazně zvyšuje spolehlivost a dostupnost služeb. Vzhledem k migraci infrastruktury do datového centra kategorie Tier IV je výskyt SPOF nemožný.

3.13.3 Zálohování

Tabulka 24: Zálohování infrastruktury (Zdroj: Vlastní zpracování)

Server	Co zálohujeme	Interval	Kolik dní zálohy uchováváme	Jak často provádíme rozdílové zálohy	Kdy probíhá zálohování	Předpokládaná doba obnovy
Server-x	Celý server – fyzický	1x denně	14	Denně	1:00 – 2:00	60 minut
Server-x	Celý server – virtuální	1x denně	30	Denně	3:00 – 4:00	40 minut
Server–x	Databáze	2x denně	30		6:00 – 6:30 20:00 – 20:30	10 minut
Server-x	Databáze transakční logy		730	Každou transakci	Dle transakcí	10 minut
Server-x	Filesystem (klientská data, interní data)	1x denně	20	Denně	4:00 – 5:00	15 minut

3.14 Požadavky v oblasti cloudových služeb

Do budoucna se nepočítá s využíváním cloudových služeb pro provoz některé z části našeho informačního systému. Pokud se ovšem objeví opodstatněný důvod, proč implementovat nějakou cloudovou službu, bude vyžadováno dodržování podmínek dle dokumentu NÚKIB – minimální bezpečnostní standard.

3.15 Přehled stavu navržených politik

Tabulka 25: Srovnání stavu politik (Zdroj: Vlastní zpracování)

Politiky	Stav před zavedením MBS	Stav po zavedení MBS
Manažerská část		
Klasifikace o ochrana informací	Neimplementováno	Implementováno
Řízení dodavatelů	Neimplementováno	Implementováno
Řízení lidských zdrojů	Neimplementováno	Implementováno
Řízení změn	Neimplementováno	Implementováno
Řízení kontinuitní činnosti	Neimplementováno	Implementováno
Audit kybernetické bezpečnosti	Neimplementováno	Implementováno
Technická část		
Fyzická bezpečnost	Implementováno	Implementováno
Řízení přístupů	Implementováno částečně	Implementováno
Požadavky v oblasti ochrany před škodlivým kódem	Implementováno částečně	Implementováno
Kybernetické bezpečnostní události a incidenty	Neimplementováno	Implementováno
Požadavky v oblasti aplikační bezpečnost	Implementováno částečně	Implementováno
Kryptografické prostředky	Implementováno částečně	Implementováno
Požadavky v oblasti zajišťování úrovně dostupnosti informací	Neimplementováno	Implementováno
Požadavky v oblasti cloudových služeb	Neimplementováno	Neimplementováno

3.16 Ekonomické aspekty implementace

Pro implementaci minimálních bezpečnostních standardů bude nezbytné vynaložit značné investice. Vzhledem k tomu, že se jedná o start-up s jedním zaměstnancem, bude nutné najmout nové pracovníky na klíčové pozice, jako jsou CISO, softwarový vývojář a systémový administrátor s přesahem do DevOps. Kromě toho bude potřeba posílit serverovou infrastrukturu, což si vyžádá další finanční prostředky.

Všechny finanční prostředky, které bude nutné vynaložit, jsou shrnuty a porovnány se stavem před implementací v tabulkách uvedených níže.

Tabulka 26: Měsíční náklady na zaměstnance (Zdroj: Vlastní zpracování)

	Před implementací		**Po implementaci**	
Pozice	**Zaměstnanci**	**Náklady**	**Zaměstnanci**	**Náklady**
CTO, CEO	1x	Vlastní čas	1x	Vlastní čas
CISO	0	0,-	1x	80 000,-
Software vývojář	0	0,-	2x	80 000,-
SysAdmin s přesahem do DevOps	0	0,-	1x	60 000,-

Tabulka 27: Náklady na pořízení HW před implantací (Zdroj: Vlastní zpracování)

Zařízení	**Počet**	**Technologie**	**Náklady na pořízení HW**
Server Dell R610	1x	Virtualizace LXC kontejnery Zálohování	9500,-
Mikro počítač Raspberry Pi 4	1x	Sekundární DNS sever Geo-lokačně odděleno Sekundární Zálohování	2000,-

Tabulka 28: Náklady na pořízení HW po implementaci (Zdroj: Vlastní zpracování)

Zařízení	Počet	Technologie	Náklady na pořízení HW
Sever Dell R630	3x	Virtualizace LXC kontejnery High Availability	260 082,-
Server Dell R430	2x	Primární zálohování High Availability	186 786,-
Server Dell R330	1x	Sekundární DNS server Geo-lokačně odděleno Sekundární zálohování	34 112,-

Tabulka 29: Měsíční náklady na provoz infrastruktury (Zdroj: Vlastní zpracování)

	Měsíční náklady na provoz HW	
Zařízení	**Před implementací**	**Po implementaci**
1x Server Dell R610	2 499,-	-
1x Raspberry PI 4	159,-	-
3x Server Dell R630	-	5 463,-
2x Server Dell R430	-	1 972,-
1x Sever Dell R330	-	899,-

Tabulka 30: Přehled nákladů na pořízení a provoz (Zdroj: Vlastní zpracování)

	Před implementací	**Po implementaci**
Náklady na pořízení HW celkem	11 500,-	480 978,-
Náklady měsíční celkem (zaměstnanci + provoz)	2 658,-	228 307,-
Náklady roční celkem (zaměstnanci + provoz)	31 896,-	2 739 684,-

Z vypracovaných tabulek je zřejmé, že i když jsou počáteční investice do implementace bezpečnostních standardů vysoké, mohou tyto opatření v dlouhodobém horizontu přinést finanční úspory. Zlepšení bezpečnosti může výrazně snížit riziko incidentů, které by mohly vést k finančním ztrátám způsobeným výpadky služeb a únikem dat. Efektivní bezpečnostní strategie také přispěje k lepšímu výkonu systémů a snížení nákladů na jejich údržbu. Jak je vidět, měsíční náklady na zaměstnance a provoz se podstatně zvýšily. To je daň za provozování bezpečných a dostupných služeb.

3.16.1 Výpočet návratnosti investice do zabezpečení

Výpočet návratnosti investice do zabezpečení budeme používat ukazatel ROSI (Return on Security Investment), což můžeme přeložit jako „Návratnost investice do bezpečnosti“. Investici zvažujeme následujícím způsobem:

- Protože jsou webhostingové služby pro útočníky zajímavé, musí společnost čelit asi 40 kybernetickým útokům ročně
- Odhaduje se, že každý útok stojí společnost přibližně 100 000,-
- Očekává se, že implantace standardů zabrání asi 90 % útoků
- Roční náklady na provoz jsou 2 739 684,-

Výpočet ROSI:

$$ROSI = \frac{(40 * 100\,000) * 0.9 - 2\,739\,684}{2\,739\,684} = 31\%$$

Dle provedeného výpočtu je zřejmé, že investování do rozšíření infrastruktury společnosti a nábor nových pracovníků je z pohledu návratnosti investice finančně výhodný. Tento výsledek znamená, že za každý investovaný 1 000 000,- Kč do bezpečnosti získáváme zpět 310 000,- Kč ve formě snížení rizik a ztrát způsobených bezpečnostními událostmi a incidenty. Tato hodnota je obzvlášť důležitá pro vedení společnosti, protože poskytují jasný důkaz o tom, že investice do bezpečnosti nejsou pouze nákladem, ale skutečně přinášejí měřitelný finanční přínos.

3.17 Případová studie: Zero-day útok

Tato případová studie se zabývá útokem *Zero-day* útokem na webovou aplikaci společnosti. Jedná se o klientskou aplikaci pro administraci hostingových služeb.

Uvedená aplikace je vyvíjena interně týmem softwarových vývojářů ve společné kooperaci s DevOps týmem, který má na starosti její nasazovaní na testovací a produkční prostředí. Celá aplikace je psaná v jazyce **Python** a postavena na webovém frameworku **Django.** Jedná se o open-source webový aplikační framework, který je napsaný právě v jazyce Python a je vyvíjenou početnou komunitou lidí z celého světa. Komunita pravidelně vydává aktualizace jak *Major,* tak i *Minor* verze uvedeného frameworku. S tím je také spojena nutnost aktualizace samotného programovacího jazyka **Python**.

Aplikace je nasazena v privilegovaném LXC kontejneru, který je umístěn ve vlastním síťovém prostředí. Kontejner, potažmo aplikace, tedy nemá povolený přístup k fyzickým nebo virtuálním serverům a také nemá přístup k ostatním klientským LXC kontejnerům. Aplikace samotná potřebuje pro svůj běh databázi, kde jsou ukládána data a nastavení všech zákaznických účtů. V našem případě se jedná o MySQL databázi.

Všechno ovládání klientského nastavení je prováděno pomocí API požadavků, které jsou zabezpečeny heslem nebo autentizačními tokeny a navázány na automatizační nástroje.

3.17.1 Možný scénář napadení

- Útočník objeví neošetřenou chybu aplikace nebo frameworku a je schopen vložit škodlivý kód
- Útočník objeví chybu ve webovém serveru
- Útočník získá přístup k datům zákazníků, která jsou uložena v databázi.

3.17.2 Důsledky napadení

- Dojde k úniku citlivých dat zákazníků – narušení Důvěrnosti dat
- Ztráta důvěry zákazníků v naše nabízené služby – narušení Dostupnost dat

3.17.3 Reakce na útok

Tabulka 31: Reakce na útok (Zdroj: Vlastní zpracování)

Před implementací	Po implementaci
CEO se snaží vyřešit vzniklou situaci podle nejlepšího vědomí a svědomí.	Kontaktování vedení společnosti (CTO, CEO, CISO).
Neexistuje žádný postup, jak na danou situaci reagovat.	Izolace aplikace od běžného provozu – úplné vypnutí LXC kontejneru.
	Svolání týmu DevOps a software vývojářů.

3.17.4 Opatření

Tabulka 32: Opatření (Zdroj: Vlastní zpracování)

Před implementací	Po implementaci
Nebyly provedeny žádné kroky.	Provoz aplikace ve vyhrazeném síťovém prostředí.
	Pravidelné aktualizace OS.
	Pravidelné aktualizace webového frameworku.
	Pravidelné aktualizace programovacího jazyka Python.

Jak lze pozorovat, rozdíly v reakcích a opatřeních na vznik incidentu spojeného se zranitelností typu *zero-day* jsou značné. Implementace bezpečnostních standardů významně přispěla k ochraně aktiva a k minimalizaci doby výpadku systému, což je klíčové pro udržení kontinuity provozu a zajištění bezpečnosti informací. Implementace standardů umožňuje rychleji a efektivněji reagovat na bezpečnostní hrozby, což je zásadní pro minimalizaci potenciálních škod způsobených útoky. Tímto způsobem lze výrazně snížit rizika spojená se *zero-day* zranitelnostmi a zvýšit odolnost systému proti kybernetickým útokům.

Závěr

V diplomové práci jsem se zabýval implementací minimálních bezpečnostních standardů ve vztahu k provozování webhostingové společnosti. Cílem bylo analyzovat stávající bezpečnostní opatření a na základě identifikovaných slabých míst navrhnout a zavést politiky, které by zvýšily ochranu dat a poskytovaných služeb.

Během vypracovávání této práce byla provedena důkladná analýza současného stavu zabezpečení, kde byly odhaleny nedostatky nejenom v samotném zabezpečení provozované infrastruktury, ale také v infastruktuře jako takové. Tyto nedostatky zahrnovaly hlavně politiky na úrovni vrcholového vedení pro činnosti řízení a auditování společnosti. V technické části politik se jednalo primárně o reakci na vzniklé bezpečnostní události a zajišťování úrovně dostupnosti informací. Analýza také ukázala, že stávající infrastruktura funguje jako jediný bod selhání (SPOF), což by v případě poruchy fyzického serveru znamenalo několika denní výpadek služeb.

V procesu návrhu implementace byly postupně probrány všechny důležité body. Manažerská část byla důkladně rozpracována a technické aspekty byly upraveny tak, aby splňovaly podmínky implementace bezpečnostních standardů, což zajišťuje, že celá infrastruktura bude nejen funkční z pohledu vysoké dostupnosti, ale také bezpečnější pro všechny uživatele systému. Ať už se bude jednat o zaměstnance nebo o klienty společnosti.

Z ekonomického pohledu půjde o velkou investici nejen do hardwarové infrastruktury, ale i do oblasti náboru nových zaměstnanců, bez nichž by realizace změny nebyla možná. Zmíněný lidský faktor je klíčovým prvkem celého prováděného procesu. To podtrhuje fakt, že investice do lidí je stejně důležitá jako investice do technického vybavení. Tento lidský element je nezbytný pro úspěšné zavedení změn a zajištění, že nové systémy budou efektivně fungovat a splňovat očekávané standardy. Ovšem při pohledu návratnosti investice do zabezpečení se jedná o zcela logický krok, který reflektuje požadavky na bezpečnost služeb.

Pokud budou popsané standardy zavedeny podle doporučených postupů, jsem přesvědčen, že společnost získá významnou konkurenční výhodu a posílí svou pozici nejen na domácím trhu, ale také v rámci Evropské unie.

Seznam použité literatury

[1] **Petr SEDLÁK, Martin KONEČNÝ**. *Problematika ISMS v manažerské informatice*. Brno: CERM, Akademické nakladatelství, 2023. ISBN isbn978-80-7623-110-8.

[2] **TRAFFIC LIGHT PROTOCOL**. *first.org* [online], 2024. [cit. 2024-05-01]. Dostupné z: https://www.first.org/tlp/docs/v2/tlp-v2-cz.pdf

[3] **Uptime Institute**. *uptimeinstitute.com* [online], 2024. [cit. 2024-04-30]. Dostupné z: https://uptimeinstitute.com/publicity-kit

[4] **Co znamená zkratka NDA?** *aksmarda.cz* [online], 2023. [cit. 2024-04-30]. Dostupné z: https://www.aksmarda.cz/rady-a-tipy/co-znamena-zkratka-nda/

[5] **What´s an ITSM CAB? A Simple Explanation**. *itsmtransition.com* [online], 2014. [cit. 2024-05-03]. Dostupné z: https://itsmtransition.com/2013/06/whats-an-itsm-cab-a-simple-explanation/

[6] **What is Multi-Factor Authentication (MFA)?** *cyberark.com* [online], 2024. [cit. 2024-05-05]. Dostupné z: https://www.cyberark.com/what-is/mfa/

[7] **Identity and Access Management (IAM).** *oracle.com* [online], 2021. [cit. 2024-05-06]. Dostupné z: https://www.oracle.com/security/identity-management/

[8] **What is Mobile Device Management (MDM)?** *forinet.com* [online], 2023. [cit. 2024-05-08]. Dostupné z: https://www.fortinet.com/tw/resources/cyberglossary/mobile-device-management

[9] **Minimální bezpečnostní standard**. *nukib.cz* [online], 2023. [cit. 2024-03-21]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[10] **Datacentrum Brno**. *nej.cz* [online], 2022. [cit. 2024-03-28]. Dostupné z: https://business.nej.cz/housing/datacentrum-brno/

[11] **Požadavky na smlouvy s dodavateli**. *nukib.cz* [online], 2022. [cit. 2024-05-03]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/pozadavky_na_smlouvy_s_dodavateli_v1.4.pdf

Seznam obrázků

Seznam tabulek

Seznam zkratek

TLP	Traffic Light Protocol
DC	Data centrum
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restore
SPOF	Single Point of Failure
SLA	Service-level agreement
NDA	Non-disclosure agreement
CAB	Change-advisory board
MFA	Multi-factor authentication
IDM	Identity Management
MDM	Mobile device management
PC	Personal computer
BYOD	Bring Your Own Device
MBS	Minimální bezpečnostní stadard
PHP	Skriptovací jazyk
LXC	Linux Containers
RAID	Redundant Array of Inexpensive Disks
RTO	Recovery Time Objective
RPO	Recovery Point Objective
POSIX	Portable Operating Systém Interface
LDAP	Lightweight Directory Access Protocol
RBAC	Roled-based access control
CLI	Command Line
SSL	Secure Sockets Layer
TLS	Transport Layer Security
CVE	Common Vulnerabilities and Exposures
PDF	Portable Document Format

RTF	Rich Text Format
Tar	Tape archiver
Gzip	GNU zip
RAR	Roshal Archive
OS	Opearting systém
DNS	Domain Name System
GPG	GNU Privacy Guard