

Nástroje pro podporu řízení systému informační bezpečnosti

Jan Kučera

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Jan Kučera
Osobní číslo: A22748
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Kombinovaná
Téma práce: Nástroje pro podporu řízení systému informační bezpečnosti
Téma práce anglicky: Tools for Supporting the Management of an Information Security System

Zásady pro vypracování

1. Provedte analýzu požadavků normy ISO 27001 a identifikujte klíčové oblasti, kde mohou být použity nástroje pro podporu řízení systému informační bezpečnosti.
2. Vyberte a popište volně dostupné nebo open-source nástroje, které splňují požadavky normy ISO 27001 a mohou být aplikovány v malých firmách vyvíjejících software pro SCADA systémy.
3. Navrhněte implementační plán pro zavedení vybraných nástrojů do řízení informační bezpečnosti v modelové organizaci.
4. Provedte porovnání vybraných nástrojů na základě jejich funkcí, kompatibility a nákladů na implementaci, včetně praktických výhod a nevýhod každého řešení.
5. Otestujte funkčnost a bezpečnost vybraných nástrojů v modelovém prostředí malé softwarové firmy, zaměřte se na jejich schopnost detekovat a reagovat na kybernetické hrozby.
6. Navrhněte závěrečná doporučení pro implementaci a používání vybraných nástrojů s ohledem na specifické potřeby malých organizací.

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

Seznam doporučené literatury:

1. Calder, A. ISO 27001/ISO 27002 – A Guide to Information Security Management Systems. 8th ed. IT Governance Publishing, 2023.
2. Johansen, Gerard. Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response. 3. vyd. Birmingham: Packt Publishing, 2023. ISBN 9781803248578.
3. Procházka, J. Bezpečnost informačních systémů. Brno: Vysoké učení technické v Brně, 2020.
4. Baars, H., Hintzbergen, J., & Hintzbergen, K. Foundations of Information Security based on ISO27001 and ISO27002. 4th revised ed. Zaltbommel: Van Haren Publishing, 2023. ISBN 978940180958C.
5. ISO/IEC 27001:2022. Informační bezpečnostní management – Požadavky. Ženeva: International Organization for Standardization, 2022.
6. ISO/IEC 27002:2022. Informační technologie – Bezpečnostní techniky – Praktické pokyny pro řízení informační bezpečnosti. Ženeva: International Organization for Standardization, 2022.
7. National Institute of Standards and Technology, NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: NIST, 2024. NIST CSWP 29. Dostupné z: <https://doi.org/10.6028/NIST.CSWP.29> (přístup 23. října 2024).

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **13. prosince 2024**

Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 13. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

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

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.
- při tvorbě obsahu byly v omezené míře použity nástroje AI (Claude, ChatGPT, DeepSeek, Copilot, Deepl) za účelem řešení případných problémů s konfiguracemi a nasazením některých nástrojů a k úpravám některých formulací přeložených z cizích jazyků pro lepší srozumitelnost.

Ve Zlíně, dne

.....

podpis autora

ABSTRAKT

Tato bakalářská práce se zaměřuje na analýzu a využití nástrojů pro podporu řízení systému informační bezpečnosti (ISMS) v souladu s požadavky normy ISO 27001. Cílem je identifikovat klíčové oblasti, kde mohou volně dostupné nebo open-source nástroje přispět k efektivnímu řízení ISMS, a poskytnout doporučení pro jejich implementaci v malých firmách vyvíjejících SCADA systémy. Práce zahrnuje analýzu požadavků normy ISO 27001, výběr vhodných nástrojů, jejich detailní popis a porovnání z hlediska funkcionality, kompatibility a nákladů. Součástí je také návrh implementačního plánu pro modelovou organizaci a testování vybraných nástrojů v simulovaném prostředí, se zaměřením na jejich schopnost detekovat a reagovat na kybernetické hrozby. Na závěr práce poskytuje doporučení pro jejich optimální využití v malých organizacích s ohledem na jejich specifické potřeby.

Klíčová slova: Informační bezpečnost, ISO 27001, SCADA systémy, řízení ISMS, open-source nástroje, implementace, kybernetické hrozby, bezpečnostní nástroje, řízení rizik, modelové prostředí.

ABSTRACT

This bachelor's thesis focuses on the analysis and utilization of tools supporting the management of an Information Security Management System (ISMS) in accordance with ISO 27001 requirements. The objective is to identify key areas where free or open-source tools can contribute to effective ISMS management and provide recommendations for their implementation in small companies developing SCADA systems. The thesis includes an analysis of ISO 27001 requirements, selection of suitable tools, detailed descriptions, and comparisons based on functionality, compatibility, and costs. It also proposes an implementation plan for a model organization and tests selected tools in a simulated environment, focusing on their ability to detect and respond to cyber threats. The thesis concludes with recommendations for their optimal use in small organizations, considering their specific needs.

Keywords: Information security, ISO 27001, SCADA systems, ISMS management, open-source tools, implementation, cyber threats, security tools, risk management, model environment.

Děkuji panu Ing. Lukáši Králíkovi, Ph.D., za odborné vedení, cenné připomínky a podnětnou zpětnou vazbu během tvorby této bakalářské práce.

Děkuji též své rodině za trpělivost, podporu a povzbuzení, které mi umožnily práci dokončit.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	15
1 POJETÍ INFORMAČNÍ BEZPEČNOSTI V KONTEXTU MODERNÍCH ORGANIZACÍ.....	16
2 NORMA ISO 27001.....	18
2.1 CÍL NORMY ISO 27001 A JEJÍ VÝZNAM V ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI.....	18
2.2 PŘEHLED NORMY ISO 27001.....	19
2.3 MODEL PLAN-DO-CHECK-ACT A PRINCIP KONTINUÁLNÍHO ZLEPŠOVÁNÍ V ISO 27001.....	20
Vedení (ISO 27001 - Kapitola 5)	22
Plánování (ISO 27001 - Kapitola 6).....	22
Podpora (ISO 27001 - Kapitola 7)	22
Provoz (ISO 27001 - Kapitola 8)	22
Hodnocení výkonnosti (ISO 27001 - Kapitola 9)	22
Zlepšování (ISO 27001 - Kapitola 10).....	23
3 NÁSTROJE PRO PODPORU SYSTÉMŮ ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI.....	24
3.1 KLÍČOVÉ OBLASTI ISMS VHODNÉ PRO PODPORU OPEN-SOURCE NÁSTROJI.....	24
3.1.1 Identifikace rizik a zranitelností.....	25
3.1.2 Správa aktiv.....	26
3.1.3 Řízení přístupu a identit	27
3.1.4 Monitorování a detekce hrozeb	28
3.1.5 Reakce na incidenty	30
3.1.6 Automatizace bezpečnostních procesů	31
4 CHARAKTERISTIKA A VÝBĚR OPEN-SOURCE NÁSTROJŮ PRO ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI	33
4.1 VÝHODY A LIMITY OPEN-SOURCE ŘEŠENÍ V OBLASTI BEZPEČNOSTI.....	33
4.2 VHODNOST POUŽITÍ V MALÝCH A STŘEDNÍCH SOFTWAREVÝCH FIRMÁCH	34
5 ZÁVĚR TEORETICKÉ ČÁSTI.....	36
II PRAKTICKÁ ČÁST.....	37
6 KRITÉRIA PRO VÝBĚR NÁSTROJŮ V SOULADU S ISO/IEC 27001	38
6.1 METODICKÝ PŘÍSTUP TÉTO PRÁCE K VÝBĚRU NÁSTROJŮ	39
7 MODELOVÁ ORGANIZACE A VÝCHOZÍ STAV BEZPEČNOSTI	41
8 VÝBĚR A POROVNÁNÍ NÁSTROJŮ PRO PODPORU SYSTÉMŮ ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI	42
8.1 IDENTIFIKACE RIZIK A ZRANITELNOSTÍ.....	42
8.2 SPRÁVA AKTIV	44
8.3 ŘÍZENÍ PŘÍSTUPU A IDENTIT	46

8.4	MONITOROVÁNÍ A DETEKCE HROZEB.....	48
8.5	REAKCE NA INCIDENTY	50
8.6	AUTOMATIZACE BEZPEČNOSTNÍCH PROCESŮ.....	52
8.7	SHRNUTÍ: VÝBĚR OPEN-SOURCE NÁSTROJŮ PRO PODPORU ISMS	54
9	IMPLEMENTACE.....	56
9.1	POSTUP NASAZENÍ A INTEGRACE NÁSTROJŮ	56
	Fáze II – Monitoring a detekce hrozeb	57
9.2	OVĚŘENÍ TECHNICKÝCH A ORGANIZAČNÍCH PŘEDPOKLADŮ.....	57
9.2.1	Technické předpoklady	58
9.2.2	Organizační předpoklady	58
9.3	HARMONOGRAM IMPLEMENTACE	59
9.4	RIZIKA BĚHEM IMPLEMENTACE A NÁVRHY JEJICH MITIGACE	61
9.4.1	Nejasné rozdělení odpovědností.....	61
9.4.2	Nedostatek času.....	62
9.4.3	Slabá motivace týmu	62
9.4.4	Podcenění a absence dokumentace.....	62
9.4.5	Nedostatečná podpora vedení.....	62
9.4.6	Omezené zdroje a kapacity.....	63
9.4.7	Integrace s existujícími procesy	63
9.4.8	Udržitelnost a kontinuální zlepšování	63
9.5	INSTALACE A ZÁKLADNÍ KONFIGURACE NÁSTROJŮ.....	63
9.5.1	Nasazení a konfigurace Snipe-IT	64
	Postup instalace:	64
9.5.2	Nasazení a konfigurace Keycloak	65
9.5.3	Nasazení Wazuh a základní konfigurace detekce hrozeb	67
9.5.4	Instalace a konfigurace TheHive	70
9.5.5	Instalace a konfigurace systému pro automatizaci bezpečnostních procesů (Shuffle)	72
10	TESTOVÁNÍ FUNKČNOSTI NASAZENÝCH NÁSTROJŮ V PRODUKČNÍM PROSTŘEDÍ	75
10.1	CÍL A PŘÍSTUP K TESTOVÁNÍ	75
10.2	TESTOVACÍ SCÉNÁŘE A PRŮBĚH	75
10.2.1	Scénář 1: Neoprávněný pokus o přihlášení (test detekce Wazuh)	76
10.2.2	Scénář 2: Založení incidentu v TheHive na základě alertu	76
10.2.3	Scénář 3: Automatizované workflow mezi nástroji (Shuffle).....	77
10.2.4	Scénář 4: Falešně pozitivní alert a jeho uzavření	78
10.3	VYHODNOCENÍ VÝSLEDKŮ TESTOVÁNÍ.....	78
10.4	PŘÍNOS PRO ISMS	79
11	ZÁVĚREČNÁ DOPORUČENÍ	80
11.1	STANOVENÍ ODPOVĚDNOSTI A UDRŽITELNOSTI ISMS V PROSTŘEDÍ MALÉ ORGANIZACE	80

11.2	ÚDRŽBA, AKTUALIZACE A SPRÁVA BEZPEČNOSTNÍ INFRASTRUKTURY	81
11.3	INTEGRACE NÁSTROJŮ DO KAŽDODENNÍHO PROVOZU ORGANIZACE	81
11.4	ŠKOLENÍ ZAMĚSTNANCŮ A ROZVOJ BEZPEČNOSTNÍHO POVĚDOMÍ (SECURITY AWARENESS).....	82
11.5	PROVOZNÍ NÁKLADY, ROZŠÍŘITELNOST A DALŠÍ ROZVOJ SYSTÉMU	83
12	ZÁVĚR.....	84
	SEZNAM POUŽITÉ LITERATURY.....	85
	SEZNAM OBRÁZKŮ	87
	SEZNAM TABULEK.....	88
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	89

ÚVOD

Oblast informačních technologií prodělala v posledních dvou desetiletích zásadní změny, které vyústily v exponenciální růst hrozeb vůči informačním systémům organizací. Klasická rizika, jako jsou viry či jednoduché phishingové útoky, byla nahrazena sofistikovanými útoky typu Advanced Persistent Threat (APT), ransomwarem, útoky na hardwarové a softwarové dodavatelské řetězce či zneužitím umělé inteligence. Podle údajů společnosti Check Point Software Technologies čelily české společnosti ve druhém čtvrtletí 2024 v průměru 2 094 kybernetickým útokům týdně, což představuje meziroční nárůst o 34 %. Tento počet je o více než pětinu vyšší než světový průměr. [1]

Mezi hlavní trendy v oblasti bezpečnosti a řízení rizik patří konsolidace bezpečnostních dodavatelů, kdy organizace upřednostňují integrovaná řešení od menšího počtu poskytovatelů, aby snížily složitost a zlepšily efektivitu bezpečnostních opatření. Pozornost se soustředí na modely Zero Trust, které vycházejí z předpokladu nulové důvěry a kladou důraz na průběžné ověřování identity uživatelů i zařízení. [2]

Specifickou výzvou jsou kybernetické útoky na SCADA systémy, jež řídí kritickou infrastrukturu. Tyto systémy byly původně navrženy pro provoz v izolovaném prostředí, ale jejich propojení s širší IT infrastrukturou a přístupem do internetu zvyšuje riziko útoků. Příkladem může být incident z roku 2003 v jaderné elektrárně Davis-Besse v Ohiu, kde se do systémů přes nedostatečně zabezpečenou síť dodavatele dostal počítačový malware, což vedlo k pětihodinovému výpadku monitorovacího systému. [3]

Vzhledem k těmto hrozbám se organizace stále více soustředí na zavádění robustních ISMS v souladu s požadavky normy ISO 27001. Tato norma představuje komplexní rámec pro systematické řízení bezpečnostních rizik a ochranu citlivých informací. Nasazení volně dostupných či open-source nástrojů pro podporu řízení ISMS je přitom obzvláště výhodné pro menší společnosti, jelikož jim umožňuje dosahovat vysoké úrovně ochrany i při omezených zdrojích a reagovat na aktuální trendy v oblasti informační bezpečnosti s důrazem na proaktivní přístup, kontinuální vzdělávání a schopnost pružně reagovat na nové technologie a hrozby.

V teoretické části práce se zaměříme na hlubší analýzu normy ISO 27001 s cílem identifikovat klíčové požadavky a oblasti, kde může implementace nástrojů výrazně zlepšit řízení ISMS. Tato část také obsáhne základní principy fungování ISMS a jeho úlohu v celkovém bezpečnostním rámci organizace.

Praktická část práce se soustředí na výběr, implementaci a testování konkrétních nástrojů v modelovém prostředí malé společnosti vyvíjející software pro SCADA systémy. Součástí praktické části bude přehled, analýza a výběr vhodných volně dostupných open-source nástrojů a jejich vztah k požadavkům normy ISO 27001, se zvláštním zaměřením na jejich aplikovatelnost v malých organizacích.

Nejprve bude proveden výběr nástrojů na základě jejich funkcionality, kompatibility s normou ISO 27001 a nákladů na implementaci. Následně bude navržen podrobný implementační plán, který zahrne technické i organizační kroky potřebné pro úspěšné nasazení vybraných nástrojů. Důležitou součástí bude testování nástrojů, kde budou zkoumány jejich schopnosti detekce a reakce na kybernetické hrozby, stejně jako jejich vliv na zlepšení procesů řízení informační bezpečnosti.

I TEORETICKÁ ČÁST

1 POJETÍ INFORMAČNÍ BEZPEČNOSTI V KONTEXTU MODERNÍCH ORGANIZACÍ

Informační bezpečnost představuje komplexní disciplínu zaměřenou na ochranu informačních aktiv před širokým spektrem rizik a hrozeb, které mohou zásadně ovlivnit fungování a konkurenceschopnost firemních systémů.

V nejširším pojetí ji lze chápat jako systematický přístup k ochraně informací a informačních systémů před neoprávněným přístupem, zneužitím, úpravou, zničením či jiným nežádoucím zásahem. Zahrnuje soubor technických, organizačních a personálních opatření, která dohromady tvoří ucelenou strategii kybernetické ochrany. Klíčové aspekty informační bezpečnosti spočívají ve třech základních principech známých jako CIA triáda:

- **Confidentiality** (Důvěrnost) představuje zajištění toho, aby k citlivým informacím měly přístup pouze oprávněné osoby. Jejím cílem je chránit data před neoprávněným přístupem, který by mohl vést ke zneužití konkurencí, vydírání, k vážnému poškození organizace, nebo například ke zneužití údajů o uživatelích. [4]
- **Integrity** (Integrita) zajišťuje, že informace zůstávají po celou dobu ukládání, přenosu a zpracování úplné, přesné a neporušené. Jakákoli neoprávněná změna dat musí být včas odhalena a napravena, aby byla zachována jejich věrohodnost a správnost. [4]
- **Availability** (Dostupnost) zajišťuje, aby oprávnění uživatelé měli včasný a spolehlivý přístup k požadovaným informacím a systémům vždy, kdy je to potřeba. Jejím cílem je minimalizovat výpadky a zajistit nepřetržitou funkčnost klíčových služeb. Nedostupnost klíčových dat či služeb může vést k narušení provozu a vážným dopadům na činnost organizace. [4]

Pro společnosti zaměřené na vývoj software a informačních systémů má informační bezpečnost mimořádný význam. Tyto organizace často pracují s vysoce citlivými průmyslovými daty a technologiemi, které jsou potenciálním terčem kybernetických útoků. Jakékoli selhání v oblasti informační bezpečnosti může mít dalekosáhlé důsledky nejen pro samotnou firmu, ale i pro koncové uživatele jejich systémů.

V důsledku narůstající sofistikovanosti kybernetických hrozeb a dostupnosti nástrojů pro jejich provádění bez hlubších znalostí technologií jsou tradiční reaktivní přístupy

nahrazovány proaktivními strategiemi, které kombinují pokročilé technologie, umělou inteligenci a strojovým učením tak, aby byla potenciální rizika včas identifikována a eliminována. [5]

Mezi hlavní výzvy patří především rychle se měnící bezpečnostní prostředí, nástup cloudových technologií a SaaS řešení, nárůst práce z domova a využití vzdáleného připojení a s tím spojená nutnost zabezpečení decentralizovaných firemních zdrojů. Organizace jsou nuceny neustále aktualizovat své bezpečnostní strategie a procesy a investovat do školení zaměstnanců, kteří jsou často nejslabším článkem bezpečnostního řetězce. [6]

Dokumenty jako ISO 27001, které poskytují ucelený rámec pro systematické řízení informační bezpečnosti, tak nejen z pohledu legislativy a mezinárodních standardů hrají klíčovou roli. Tyto standardy nepředstavují jen technická doporučení, ale také komplexní metodiku, která zahrnuje analýzu rizik, návrh bezpečnostních opatření a kontinuální zlepšování.

2 NORMA ISO 27001

Norma ISO/IEC 27001 je mezinárodní standard, který byl vyvinut Mezinárodní organizací pro normalizaci (ISO) ve spolupráci s Mezinárodní elektrotechnickou komisí (IEC). Tento standard definuje požadavky na ISMS a poskytuje organizacím systematický rámec pro ochranu citlivých informací před širokým spektrem hrozeb.

Standard popisuje nejen požadavky na zavedení a provoz ISMS, ale také zdůrazňuje význam pravidelného monitorování, auditování a neustálého zlepšování. Významnou součástí je také tzv. cyklus Plan-Do-Check-Act (PDCA), který podporuje systematický přístup k optimalizaci bezpečnostního řízení v čase a který je podrobněji popsán v kapitole “2.3 Model PDCA a princip kontinuálního zlepšování v ISO 27001”.

První verze normy ISO/IEC 27001 byla zveřejněna v roce 2005 jako přímý nástupce britského standardu BS 7799. Aktualizace z let 2013 a 2022 přinesly významné změny, zvláště v oblasti harmonizace s ostatními normami systémů managementu a v rozšíření souboru bezpečnostních opatření (Annex A) podle nové verze ISO/IEC 27002:2022. Verze z roku 2022 klade zvýšený důraz na rizikově orientovaný přístup a na přizpůsobení novým technologickým výzvám, jako jsou cloudová prostředí, práce na dálku a pokročilých kybernetických útoků. [7]

V této kapitole se nejprve podrobně zaměříme na cíle a strukturu normy ISO/IEC 27001, její význam pro malé softwarové organizace a popíšeme klíčové požadavky, které je třeba splnit v rámci implementace ISMS.

2.1 Cíl normy ISO 27001 a její význam v řízení informační bezpečnosti

Norma ISO/IEC 27001 byla vytvořena s cílem nabídnout organizacím jasně definovaný postup, jak efektivně řídit informační bezpečnost. Hlavním účelem je poskytnout strukturovaný rámec pro identifikaci, hodnocení a snižování rizik spojených s ochranou informací. Zároveň zavádí procesy, které pomáhají bezpečnostním incidentům předcházet, zmírňovat jejich dopady a zajišťovat kontinuitu provozu.

ISO 27001 umožňuje organizacím přistupovat k informační bezpečnosti systémově a strategicky. Místo reaktivního řešení problémů podporuje proaktivní řízení rizik, kdy organizace identifikují slabá místa, zavádějí opatření a kontinuálně zlepšují svou bezpečnostní politiku. Standard je navržen tak, aby byl škálovatelný a použitelný jak pro

malé společnosti, tak pro velké korporace, přičemž umožňuje přizpůsobení konkrétním potřebám dané organizace.

Hlavním přínosem normy ISO 27001 je ochrana důvěrnosti, integrity a dostupnosti informací – tedy základních pilířů efektivního řízení informační bezpečnosti. Zavedení této normy organizacím umožňuje lépe zvládat bezpečnostní hrozby, plnit legislativní požadavky a zároveň posilovat důvěru zákazníků i obchodních partnerů.

2.2 Přehled normy ISO 27001

Struktura normy je rozdělena do několika hlavních částí, které dohromady tvoří základní rámec pro zavedení a správu ISMS. Její členění vychází z tzv. harmonizované (někdy též “jednotné”) struktury Annex SL, která sjednocuje formát všech moderních norem systémů řízení a usnadňuje jejich vzájemnou integraci, například s normami ISO 9001 (Systémy managementu kvality) nebo ISO 14001 (Systémy environmentálního managementu). [8]

Vlastní požadavky na systém řízení jsou obsaženy v kapitolách 4 až 10, kterými se budeme podrobněji zabývat ve vztahu ke klíčovým požadavkům normy v části “2.4 - Klíčové požadavky normy ISO 27001 a jejich aplikace”. Každá z těchto kapitol se zaměřuje na klíčovou oblast implementace ISMS:

- Kapitola 4 – Kontext organizace
- Kapitola 5 – Vedení
- Kapitola 6 – Plánování
- Kapitola 7 – Podpora
- Kapitola 8 – Provoz
- Kapitola 9 – Hodnocení výkonnosti
- Kapitola 10 – Zlepšování

Důležitou součástí normy je také příloha A, která obsahuje seznam 93 bezpečnostních opatření rozdělených do čtyř kategorií: organizační, personální, fyzické a technologické. Tyto opatření vycházejí z dokumentu ISO/IEC 27002:2022 a slouží jako základ pro tzv. “Prohlášení o aplikovatelnosti” (Statement of Applicability), v němž organizace určuje, které opatření bude zavádět a proč. [8]

Struktura normy je navržena tak, aby bylo možné systém řízení informační bezpečnosti přizpůsobit konkrétním potřebám a možnostem většiny organizací. Klade důraz na jasné nastavení procesů, vhodnou volbu bezpečnostních opatření a pravidelné vyhodnocování jejich účinnosti. Díky tomu není rámec ISO27001 závislý na konkrétních technologiích, ale staví na principech odpovědnosti, plánování a kontinuálního zlepšování. Text podkapitoly.

2.3 Model Plan-Do-Check-Act a princip kontinuálního zlepšování v ISO 27001

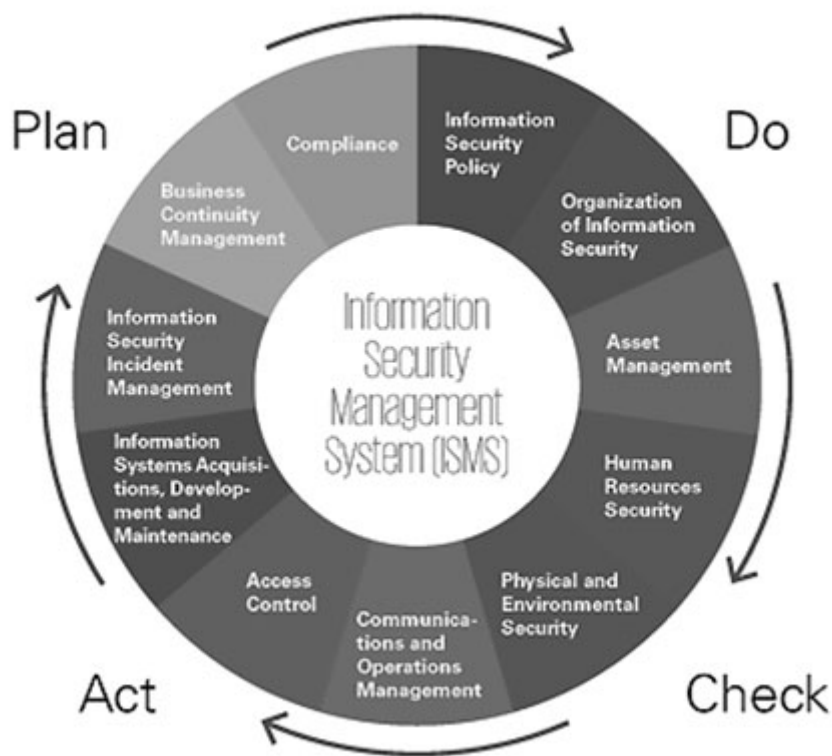
Proces řízení informační bezpečnosti nekončí zavedením opatření – součástí normy je i požadavek na kontinuální zlepšování. Organizace musí aktivně řešit nedostatky, reagovat na nové hrozby a přizpůsobovat bezpečnostní mechanismy tak, aby odpovídaly aktuálním rizikům a potřebám.

Model Plan-Do-Check-Act (PDCA) je v normě ISO/IEC 27001:2022 použit jako základní princip pro řízení a neustálé zlepšování systému informační bezpečnosti. Požadavky normy jsou uspořádány tak, aby odpovídaly jednotlivým fázím tohoto cyklu. Model PDCA je rozdělen do čtyř fází, které spolu tvoří cyklus průběžného zlepšování:

- **Plan (plánuj):** V této fázi organizace stanoví cíle informační bezpečnosti, identifikuje rizika a definuje potřebné procesy a zdroje potřebné k jejich řízení. Součástí je i vymezení kontextu organizace, požadavků zainteresovaných stran a stanovení politiky ISMS. [9]
- **Do (dělej):** Následuje realizace plánovaných opatření. Organizace implementuje bezpečnostní opatření, provozuje ISMS a zajišťuje provozní činnosti podle stanovených plánů a vnitřních předpisů. [9]
- **Check (kontroluj):** Tato fáze zahrnuje monitorování, měření, analýzu a vyhodnocování výkonnosti ISMS. Organizace provádí interní audity a přezkoumání systému vedením s cílem ověřit, zda jsou cíle a opatření plněny. [9]
- **Act (jednej):** Na základě zjištěných výsledků organizace přijímá nápravná opatření a upravuje ISMS tak, aby došlo k odstranění zjištěných nedostatků a k dalšímu zlepšení systému. [9]

Jedna z největších předností modelu PDCA je jeho schopnost přizpůsobení se specifickým potřebám různých typů organizací a efektivně reagovat na měnící se podmínky,

nové hrozby a technologický vývoj tím, že podporuje cyklický přístup namísto statického řešení bezpečnosti.



Obrázek 1 Schéma modelu PDCA [10]

2.4 Klíčové požadavky normy ISO 27001 a jejich aplikace

Požadavky normy ISO/IEC 27001:2022 jsou rozděleny do kapitol 4 až 10, které tvoří základ pro zavedení a fungování ISMS. Jejich struktura odpovídá jednotlivým fázím cyklu PDCA. V každé kapitole nalezneme konkrétní požadavky, které musí organizace splňovat, aby byla v souladu s normou. V následující části jsou kapitoly stručně popsány z hlediska obsahu společně s jejich zaměřením na praktickou aplikaci.

Kontext organizace (ISO 27001 - Kapitola 4)

Tato část vyžaduje, aby organizace určila faktory, které mají vliv na řízení informační bezpečnosti, včetně požadavků zainteresovaných stran a rozsahu systému řízení. To může znamenat například identifikaci požadavků od klientů na regulaci, závislost na cloudových službách nebo specifika spojená s vývojem konkrétních aplikací. Je důležité přesně vymezit, na jaké oblasti se ISMS vztahuje – zda pokrývá pouze vývojové činnosti, nebo i správu interní infrastruktury. [10]

Vedení (ISO 27001 - Kapitola 5)

Vedení společnosti musí aktivně podporovat proces řízení informační bezpečnosti, schválit vnitrofiremní bezpečnostní politiku a určit odpovědnosti za klíčové oblasti. V malých firmách často vedení plní současně výkonné i bezpečnostní role, a proto je důležité formálně určit, kdo zodpovídá za ISMS a zda je například jmenována osoba odpovědná za řízení rizik. [11]

Plánování (ISO 27001 - Kapitola 6)

V rámci plánování musí organizace stanovit cíle v oblasti informační bezpečnosti a nastavit postupy pro řízení rizik. V praxi to znamená vytvořit metodiku pro identifikaci, analýzu a vyhodnocení rizik a následně určit vhodná opatření k jejich snížení. [11] U softwarové společnosti to může zahrnovat například řízení rizik spojených s vývojovým prostředím, přístupem k repozitářům, práci s testovacími daty nebo prací na dálku.

Podpora (ISO 27001 - Kapitola 7)

Podpora zahrnuje zajištění potřebných zdrojů, školení, komunikace a řízení dokumentace. V menší organizaci je vhodné využít nástroje pro správu znalostí, jako jsou interní wiki, školení ohledně bezpečnostních zásad, nebo jednoduché šablony pro dokumentaci bezpečnostních procesů. Důležitá je také evidence pravidelného proškolení zaměstnanců a ověřování jejich kompetencí. [11]

Provoz (ISO 27001 - Kapitola 8)

Zaměřením této kapitoly je provozní řízení a realizace plánovaných bezpečnostních opatření, jako např. správa přístupových práv, bezpečnostní monitoring, logování aktivit, ochrana vývojového a produkčního prostředí nebo proces řízení změn. [11] K podpoře těchto činností lze využít nástroje, jako jsou systémy pro správu identit a přístupů (IAM), nástroje pro bezpečnostní monitoring a detekci událostí (SIEM) či ochranu koncových zařízení (EDR).

Hodnocení výkonnosti (ISO 27001 - Kapitola 9)

Organizace musí pravidelně vyhodnocovat účinnost ISMS prostřednictvím interního auditu a revize vedením společnosti. V malém podniku lze audit provádět s využitím checklistů a vzájemného hodnocení mezi odpovědnými osobami. Vedení by mělo provádět revizi alespoň ročně a mělo by obashovat posouzení toho, zda byly nastavené cíle dosaženy a také návrh případných zlepšení nebo nápravných opatření. [11]

Zlepšování (ISO 27001 - Kapitola 10)

Závěrečná část normy ISO/IEC 27001:2022 se zaměřuje na nápravná opatření a proces průběžného zlepšování ISMS. Organizace musí být schopna identifikovat oblasti, které nejsou ve shodě s normou, bezpečnostní incidenty a nedostatky v systémech a reagovat na ně tak, aby zabránila opakování stejných problémů. Součástí tohoto procesu je vedení záznamů o incidentech, přijatých opatřeních a výsledcích provedených náprav. Dokumentace systému řízení musí být pravidelně aktualizována podle zjištěných skutečností. Každý krok v rámci zlepšování musí být doložen, vyhodnocen a v případě potřeby přizpůsoben reálným podmínkám organizace. Důležité je nastavit procesy tak, aby byly dostatečně efektivní a přitom nenáročné na administrativu, což norma umožňuje díky své flexibilní struktuře. [11]

3 NÁSTROJE PRO PODPORU SYSTÉMŮ ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI

Efektivní řízení informační bezpečnosti dnes vyžaduje více než jen dobře nastavené procesy a pravidla. Vzhledem k narůstající složitosti IT prostředí a požadavkům na snadnou auditovatelnost, se moderní ISMS neobejdou bez technické podpory v podobě specializovaných nástrojů. Pomocí těchto nástrojů mohou organizace nejen rizika identifikovat a reagovat na bezpečnostní incidenty, ale zároveň i zajišťovat dohled, řízení přístupů, evidenci aktiv nebo automatizaci opakujících se činností.

Pro malé a střední podniky, které často nemají k dispozici rozsáhlé IT týmy nebo vysoké rozpočty, představují open-source řešení cenově dostupnou, a přitom plně funkční alternativu ke komerčním produktům. Výhodou těchto nástrojů je nejen jejich dostupnost, ale také široká uživatelská a vývojářská komunita, která přispívá k jejich neustálému rozvoji a zvyšování jejich možností a schopností.

V této kapitole se zaměříme na charakteristiku open-source nástrojů, které mohou efektivně podporovat plnění klíčových požadavků normy ISO/IEC 27001. Zvláštní důraz bude kladen na jejich praktické uplatnění v podmínkách, kde je potřeba dosáhnout vysoké úrovně bezpečnosti i s omezenými prostředky.

3.1 Klíčové oblasti ISMS vhodné pro podporu open-source nástroji

Norma ISO/IEC 27001 zahrnuje širokou škálu požadavků, které se zabývají jak strategickým řízením, tak praktickými bezpečnostními opatřeními v každodenním provozu organizace. Ne všechny oblasti normy však vyžadují implementaci technických řešení. Tato kapitola se proto zaměřuje na výběr těch bezpečnostních domén, u nichž je možné, nebo žádoucí využít open-source nástroje pro podporu a automatizaci plnění požadavků.

Cílem je identifikovat konkrétní části systému řízení informační bezpečnosti, kde mohou open-source řešení přinést významnou přidanou hodnotu z hlediska efektivity, dostupnosti a funkčnosti. Výběr oblastí vychází z analýzy normy ISO/IEC 27001:2022 a ze specifických potřeb menší softwarové společnosti, pro kterou je práce koncipována.

Pro každou z následujících oblastí bude v praktické části práce identifikován vhodný open-source nástroj nebo jejich kombinace, přičemž důraz bude kladen na jejich soulad s příslušnými požadavky ISO 27001 a praktickou použitelnost v prostředí malé organizace.

3.1.1 Identifikace rizik a zranitelností

Jedním ze základních prvků systému řízení informační bezpečnosti je systematická identifikace, vyhodnocování a řízení bezpečnostních rizik. Norma ISO/IEC 27001:2022 klade na tento proces zásadní důraz a věnuje mu samostatné požadavky v kapitole 6.1 „Opatření k řešení rizik a příležitostí“. Řízení rizik je také úzce propojeno s vybranými opatřeními uvedenými v příloze A, například A.5.9 (Inventář aktiv), A.5.12 (Klasifikace informací), A.8.8 (Řízení technických zranitelností) a A.5.24 až A.5.27 (Řízení bezpečnostních incidentů). [11]

Cílem řízení rizik je nejen incidentům předcházet, ale také prokázat, že organizace chápe jaké má zranitelnosti, zná potenciální hrozby a je schopna přijmout přiměřená opatření k jejich ošetření. Výhodou takového přístupu je, že podporuje transparentnost a umožňuje efektivně rozhodovat o tom na jaké oblasti bezpečnosti se zaměřit co se týká přidelení zdrojů, ať už lidských nebo finančních. Proces řízení rizik obvykle zahrnuje následující kroky:

- identifikaci informačních aktiv a jejich vlastníků,
- identifikaci hrozeb a zranitelností vztahujících se k těmto aktivům,
- odhad a vyhodnocení dopadů a pravděpodobnosti,
- výběr a implementaci opatření ke snížení rizika na přijatelnou úroveň.

Z pohledu ISO 27001 je důležité, aby byl tento proces dokumentovaný, opakovatelný a přizpůsobený kontextu organizace. Neexistuje jediná univerzální metodika – norma ponechává volnost ve způsobu hodnocení i v tom, jak jsou rizika kategorizována, ale vyžaduje, aby byl zvolený přístup konzistentní a aby bylo možné ho doložit.

V praxi se malé organizace často potýkají s tím, že proces identifikace rizik není formalizovaný, nebo probíhá pouze intuitivně. To může vést k přehlížení zásadních oblastí, jako jsou zranitelnosti v síťové infrastruktuře, vývojovém prostředí nebo přístupových mechanismech. V souvislosti s rychlým vývojem technologií a kybernetických útoků je přitom nezbytné, aby byla rizika pravidelně přehodnocována a aktualizována.

Mezi hlavní výzvy v oblasti řízení bezpečnostních rizik v současnosti patří zejména vysoká dynamika zranitelností v cloudových a hybridních prostředích, kde se infrastruktura často mění a tradiční ochranná opatření ztrácejí účinnost. Dalším problémem je nedostatek kvalifikovaných odborníků schopných provádět manuální analýzu bezpečnostních hrozeb a

zranitelností, což snižuje schopnost organizací efektivně zareagovat na nové hrozby. Problematickou oblastí může být také omezená dostupnost aktuálních a kvalitních dat o vznikajících zranitelnostech a incidentech, která jsou nezbytná pro správné vyhodnocení rizik.

Vzhledem k těmto výzvám je v mnoha organizacích nutné posílit nejen samotný proces hodnocení rizik, ale i schopnost efektivně detekovat a vyhodnocovat technické zranitelnosti v reálném čase.

3.1.2 Správa aktiv

Správa informačních aktiv tvoří jeden ze základních předpokladů efektivního řízení informační bezpečnosti. Aktiva představují veškeré hodnotné prvky informačního systému – od fyzických zařízení, přes data, software, až po znalosti a procesy. Bez systematické evidence a klasifikace těchto aktiv nelze účinně implementovat bezpečnostní opatření, přidělovat odpovědnosti ani reagovat na vznikající rizika.

Oblasti ve kterých norma ISO/IEC 27001:2022 klade důraz na správu aktiv jsou body v příloze A – A.5.9 (Inventář aktiv), A.5.10 (Odpovědnosti za aktiva) a A.5.12 (Klasifikace informací). [11] Tyto požadavky určují, že organizace musí:

- vést aktuální a úplný inventář všech aktiv relevantních pro informační bezpečnost,
- přiřadit odpovědnosti za správu těchto aktiv konkrétním osobám,
- stanovit hodnotu a kritičnost informací pomocí klasifikace dle důvěrnosti, integrity a dostupnosti.

Z hlediska implementace ISMS je právě správa aktiv výchozím bodem pro další oblasti, jako je řízení přístupů, řízení rizik či reakce na incidenty. Bez přehledu o tom, jaká aktiva organizace vlastní, kdo je používá, kde se nachází nebo jak jsou chráněna, vzniká významné bezpečnostní riziko.

V prostředí menších firem, které často fungují v dynamických podmínkách bez formálních procesů, bývá správa aktiv podceňována. Častým problémem je například neexistující evidence výpočetní techniky, neformální sdílení přístupových údajů, nebo špatné řízení přístupu k databázím obsahujícím citlivá zákaznická data. Taková situace může vést ke ztrátám dat, neoprávněným přístupům nebo neúmyslnému zveřejnění informací.

Mezi aktuální výzvy spojené se správou aktiv patří:

- komplexnost hybridních prostředí (on-premise vs. cloud),
- správa softwarových licencí a aktualizací v distribuovaných týmech,
- sledování aktiv zaměstnanců pracujících na dálku (např. BYOD zařízení),
- nedostatek integrovaných nástrojů pro správu fyzických i virtuálních aktiv.

ISO 27001 nevyžaduje konkrétní technické řešení, ale jasně stanovuje, že evidence aktiv musí být udržována v souladu s měnícím se prostředím, musí být aktuální, přesná a dostupná relevantním osobám. Dále musí být propojena s politikami řízení rizik, klasifikací informací a přístupovými právy. Organizace by proto měla mít jak formální inventář aktiv, tak i mechanismus pro jeho průběžnou aktualizaci a auditovatelnost.

3.1.3 Řízení přístupu a identit

Jedním ze základních principů informační bezpečnosti je zajistit, aby přístup k informačním aktivům měli pouze oprávnění uživatelé v případě potřeby a za správným účelem. Oblast řízení přístupu tvoří jednu z nejdůležitějších částí ISMS, neboť má přímý vliv na důvěrnost a integritu dat.

Norma ISO/IEC 27001:2022 definuje požadavky na řízení přístupu především v rámci opatření v příloze A. Klíčové jsou zejména:

- **A.5.15 – Politiky řízení přístupu:** organizace musí zavést zásady, které vymezují pravidla přístupu k informačním systémům a službám. [11]
- **A.5.16 – Řízení přístupových práv:** požadavek na zavedení procesů pro přidělování, úpravy a odnímání přístupových práv. [11]
- **A.5.17 – Ověřování uživatelů:** důraz na ověřování identity uživatelů před udělením přístupu. [11]
- **A.5.18 – Řízení privilegovaného přístupu:** specifická opatření pro správce a další uživatele s vyššími oprávněními. [11]

Správně navržené řízení přístupu snižuje riziko neoprávněného přístupu k citlivým datům, zneužití samotných oprávnění nebo lidské chyby. Současně umožňuje zajištění auditovatelnosti – tedy možnost zpětně dohledat, kdo k jakému aktivu přistupoval a kdy [8].

V prostředí menších firem je často výzvou zavedení politik řízení přístupu, ale také jejich důsledné uplatňování v praxi. Problémy bývají následující:

- sdílené uživatelské účty bez evidence změn,
- neexistence nebo nevyužívání centrální správy identit,
- absence vícefaktorového ověřování,
- nedostatečné logování činností uživatelů.

Z pohledu technické realizace přináší další komplikace hybridní prostředí – kombinace on-prem infrastruktury a cloudových služeb, které vyžaduje koordinaci přístupových práv napříč různými systémy. Kromě toho roste potřeba zabezpečení přístupu z různých zařízení a vzdálených lokalit, což klade důraz na robustní ověřovací mechanismy a správu privilegovaných účtů.

V praxi by měl být přístup řízen podle zásady nejnižších oprávnění (principle of least privilege) a v souladu s klasifikací informací. Každý uživatel by měl mít přístup pouze k těm systémům a datům, která jsou nezbytná pro jeho pracovní činnost. [12] Dále by měly existovat procesy pro pravidelnou revizi a odebrání již nepotřebných oprávnění.

Norma vyžaduje nejen zavedení těchto opatření, ale také jejich formální dokumentaci a schopnost prokázat, že jsou v praxi dodržována. Pokud ve firmě chybí centralizovaný systém pro správu identit a přístupových oprávnění, je nutné hledat řešení, která umožní snadno zavést autentizaci, autorizaci i revizi přístupů bez zbytečné administrativní zátěže.

3.1.4 Monitorování a detekce hrozeb

Schopnost včas identifikovat podezřelé aktivity, anomálie či přímo bezpečnostní incidenty je jedním z nejdůležitějších faktorů pro účinnou ochranu informačních aktiv. Monitorování a detekce hrozeb umožňuje organizacím nejen reagovat na vzniklé události, ale také jim předcházet pomocí včasného varování a analýzy trendů.

Norma ISO/IEC 27001:2022 se této oblasti věnuje napříč několika opatřeními, zejména:

- **A.5.26 – Monitorování aktivit:** organizace má zavést a provozovat systémy pro monitorování přístupů, událostí a chování uživatelů. [11]
- **A.5.23 – Prevence malwaru:** včasné detekování škodlivého softwaru je klíčové pro ochranu systémů. [11]
- **A.8.7 – Ochrana před malwarem a hrozbami:** řízení a detekce technických hrozeb včetně jejich sledování. [11]

- **A.8.15 – Protokolování a záznamy** a **A.8.16 – Monitorování systémů**: důraz na zajištění záznamů o bezpečnostních událostech, přístupech a jejich analýzu. [11]

Cílem těchto požadavků je zajistit, aby organizace byla schopna:

- průběžně sledovat stav svého IT prostředí,
- detekovat odchylky od běžného chování,
- identifikovat potenciální hrozby v reálném čase,
- udržovat relevantní záznamy, které mohou být použity při analýze incidentů nebo auditu.

V menších firmách je implementace efektivního monitoringu často náročná kvůli nedostatku personálních i technických zdrojů. Chybějící centralizované logování, roztržitost systémů a absence nástrojů pro korelaci událostí vede k tomu, že potenciální útoky mohou být detekovány pozdě nebo vůbec. Současně čelí malé organizace těmto výzvám:

- zpracování velkého množství logů bez možnosti jejich efektivní analýzy,
- nedostatečné kapacity k nepřetržitému dohledu,
- závislost na outsourcovaných IT službách, kde není jasně definována odpovědnost za bezpečnostní monitoring,
- nízká úroveň integrace mezi jednotlivými informačními systémy a síťovými prvky.

Vzhledem k tomu, že sofistikovanost útoků roste (např. pomocí fileless malware, laterální pohyb v síti či zneužití oprávnění), je detekce pouhými pravidly nedostačující. Proto roste význam pokročilé analýzy logů, korelace událostí napříč systémy (SIEM), a využití behaviorální analýzy či strojového učení pro identifikaci anomálií.

Přestože norma nestanovuje konkrétní nástroje nebo metodiky, vyžaduje, aby byly logy uchovávány v dostatečné kvalitě, měly přiřazeny údaje o datu a čase, byly chráněny proti manipulaci a byly pravidelně vyhodnocovány. Dále musí být určena odpovědnost za jejich sledování a incidenty musí být dokumentovány a řešeny dle interních postupů.

3.1.5 Reakce na incidenty

Ani sebelepší preventivní opatření nezaručí, že organizace nebude čelit bezpečnostnímu incidentu. Klíčovým prvkem každého systému řízení informační bezpečnosti je proto schopnost na incidenty včas a účinně reagovat. Cílem reakce není pouze okamžité řešení vzniklého problému, ale i minimalizace dopadů, obnova provozu, identifikace příčin a zavedení nápravných opatření.

Norma ISO/IEC 27001:2022 se oblasti reakce na incidenty věnuje v několika kontrolách přílohy A, zejména:

- **A.5.25 – Hlášení událostí informační bezpečnosti:** každý zaměstnanec by měl být schopen incident rozpoznat a neprodleně nahlásit. [11]
- **A.5.26 – Odezva na události informační bezpečnosti:** organizace má mít zavedeny procesy pro vyhodnocení a řešení událostí. [11]
- **A.5.27 – Získávání zkušeností z incidentů:** požaduje se analýza příčin a implementace změn vedoucích k prevenci opakování. [11]

Z pohledu normy musí být postupy reakce na incidenty definovány, dokumentovány, testovány a pravidelně aktualizovány. Součástí by mělo být jasné rozdělení rolí, odpovědností a eskalačních mechanismů, včetně napojení na krizové řízení, pokud je to relevantní. [12]

V prostředí malých organizací bývá reakce na incidenty často improvizovaná. Chybí formální hlášení, evidence událostí a systematická analýza. Incidenty jsou řešeny ad hoc, což vede k jejich podcenění nebo opakování. Mezi časté výzvy v této oblasti patří:

- nízká informovanost zaměstnanců o tom, co představuje incident a jak jej hlásit,
- neexistence jednotného systému pro evidenci a řízení incidentů,
- podcenění méně závažných událostí, které mohou být předzvěstí větších útoků,
- absence zpětné vazby a post-mortem analýz po vyřešení incidentu.

Moderní pojetí reakce na incidenty také zahrnuje koordinaci v rámci celého ekosystému organizace, včetně externích dodavatelů, poskytovatelů služeb, zákazníků a případně i regulačních orgánů. Rychlá reakce, eskalace a správně vedená komunikace mohou výrazně ovlivnit dopad incidentu na provoz, reputaci i právní odpovědnost organizace.

Z hlediska souladu s ISO 27001 je důležité, aby incidenty byly nejen řešeny, ale i vyhodnocovány. Organizace by měla vést záznamy o typu incidentu, jeho příčinách, přijatých opatřeních a důsledcích. Tyto poznatky by měly být využity k aktualizaci bezpečnostních opatření, školení zaměstnanců a zlepšování systému jako celku.

3.1.6 Automatizace bezpečnostních procesů

S rostoucí komplexitou informačních systémů a narůstajícím množstvím kybernetických hrozeb se manuální provádění bezpečnostních opatření stává nejen neefektivní, ale často i nedostatečné. Automatizace bezpečnostních procesů představuje moderní přístup k dosažení rychlé, konzistentní a reprodukovatelné reakce na události, a zároveň snižuje závislost na lidském faktoru.

Norma ISO/IEC 27001:2022 pojem automatizace výslovně nezmiňuje jako samostatnou oblast, nicméně řada jejích požadavků předpokládá systémové, pravidelně prováděné a auditovatelné činnosti, jejichž efektivita může být výrazně zvýšena pomocí automatizace. To se týká například:

- **A.5.24 – Příprava na události informační bezpečnosti:** organizace by měla být schopna pružně reagovat na vzniklé hrozby. [11]
- **A.5.25–A.5.27 – Reakce a poučení z incidentů:** vyžadována je koordinovaná, zdokumentovaná reakce s následným zlepšením. [11]
- **A.5.30 – Bezpečnostní aspekty správy změn:** systém změn by měl být řízen, zaznamenáván a schvalován. [11]

Díky automatizaci je možné detekované události okamžitě předávat ke zpracování, spouštět reakční workflow (např. zablokování IP adresy, izolace zařízení v síti, informování odpovědných osob) a eliminovat nutnost manuálního zásahu v prvních minutách incidentu – tedy v době, kdy jde často o rozhodující faktor. Mezi výzvy, které brání zavedení automatizace v menších organizacích, patří:

- nízká úroveň formalizace bezpečnostních procesů – není co automatizovat,
- nedostatek zkušeností s orchestrací systémů a integrací API,
- obava ze „slepého“ zásahu bez lidské validace,
- obavy z dopadu na provoz v případě chybně nastavené reakce.

Moderní nástroje „Security Orchestration, Automation and Response“ (SOAR) dnes umožňují i menším firmám jednoduše nastavit automatické reakce na běžné bezpečnostní události. Typickým příkladem je automatické zpracování alertu z monitorovacího systému, ověření reputace IP adresy nebo okamžité upozornění administrátora.

Automatizace je tak stále důležitější pro zajištění rychlosti reakce, pro odlehčení pracovní zátěže bezpečnostních týmů a pro zajištění konzistence v bezpečnostních postupech. V kontextu ISO 27001 umožňuje efektivní sledování změn, včasnou reakci a zavedení nápravných opatření bez zbytečných prodlev.

4 CHARAKTERISTIKA A VÝBĚR OPEN-SOURCE NÁSTROJŮ PRO ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI

Open-source software představuje v oblasti informační bezpečnosti specifickou kategorii nástrojů, jejichž popularita v posledních letech narůstá. Jeho využití není omezeno pouze na experimentální nebo akademické účely, ale nachází uplatnění i v produkčních prostředích malých a středních firem, veřejné správy i velkých korporací. Z pohledu ISMS mohou open-source nástroje významně přispět ke splnění požadavků normy ISO/IEC 27001, a to zejména v technických oblastech, jako je detekce hrozeb, řízení přístupu, správa aktiv nebo reakce na incidenty.

4.1 Výhody a limity open-source řešení v oblasti bezpečnosti

Jednou z nejčastěji zmiňovaných výhod open-source řešení je jejich transparentnost a dostupnost i s omezenými finančními prostředky, což je zvláště důležité pro malé organizace s omezeným rozpočtem. Open-source nástroje umožňují nasazení, škálování i úpravy podle specifických potřeb daného prostředí. Díky veřejně dostupnému zdrojovému kódu je možné ověřit, jak daný nástroj funguje, a lépe posoudit jeho bezpečnostní vlastnosti. Z tohoto hlediska je open-source model často považován za transparentnější než uzavřený komerční software.

Další výhodou je aktivní vývojová a uživatelská komunita, která často poskytuje rychlou zpětnou vazbu, návody a moduly pro integraci s jinými systémy. U široce používaných nástrojů je běžné, že vzniká rozsáhlý ekosystém rozšíření a podpůrných projektů, které umožňují jejich efektivní začlenění do existujících systémů.

Vedle přínosů je však nutné zmínit také určitá omezení a rizika, která mohou s nasazením open-source řešení souviset. V první řadě je třeba počítat s tím, že odpovědnost za provoz, konfiguraci, údržbu a bezpečnost nástroje leží zcela na straně organizace. Neexistuje záruka oficiální podpory (u některých řešení u neplacených komunitních verzí), a v případě problémů může být řešení závislé na dostupnosti komunity nebo interních znalostech. Pro malé společnosti může být náročné zajistit dostatek kvalifikovaných pracovníků. [13]

Kromě toho bývá u některých nástrojů problematická dokumentace, nekompletní lokalizace, obtížnější instalace a komplikovaná integrace s jinými systémy. Bez důkladné

analýzy a otestování může dojít k chybné implementaci nebo zanedbání bezpečnostních aspektů (např. špatně nastavené oprávnění, neaktualizovaný systém apod.). [14]

Norma ISO/IEC 27001 přitom nijak nespecifikuje, zda má být použit open-source nebo komerční nástroj – klade důraz především na přiměřenost opatření, jejich účinnost, sledovatelnost a soulad s politikou řízení rizik. Open-source nástroje tak mohou být plnohodnotnou součástí ISMS, pokud jsou implementovány správně. Z pohledu této práce je cílem identifikovat takové open-source nástroje, které jsou:

- dostatečně funkčně vyspělé,
- bezpečnostně ověřené,
- aktivně udržované,
- a vhodné pro použití v malých a středních organizacích.

V dalších podkapitolách této kapitoly budou proto definována kritéria výběru nástrojů a popsán metodický přístup k jejich hodnocení.

4.2 Vhodnost použití v malých a středních softwarových firmách

Malé a střední podniky (MSP), zejména v oblasti vývoje softwaru, čelí v oblasti informační bezpečnosti specifickým výzvám. Na rozdíl od velkých korporací disponují omezenými lidskými i finančními zdroji, ale zároveň často spravují kritická data, systémy a zákaznické informace. V této souvislosti představují open-source nástroje vhodnou alternativu ke komerčním řešením, která mohou být finančně nedostupná.

Menší softwarové společnosti mívají vysoký stupeň technologické vyspělosti, ale omezené možnosti formálního řízení bezpečnostních procesů. Open-source nástroje jim umožňují:

- rychle reagovat na bezpečnostní potřeby bez složitých schvalovacích procesů,
- přizpůsobit nástroje konkrétním vývojovým nebo provozním podmínkám (např. verzování, CI/CD, testování),
- integrovat bezpečnostní opatření přímo do vývojového životního cyklu (DevSecOps).

Velkým přínosem je také možnost automatizace rutinních činností, jako je správa zranitelností, logování událostí nebo monitorování síťového provozu. Tím se kompenzuje

absence specializovaného bezpečnostního týmu a snižuje se závislost na externích službách. V organizacích s 10–50 zaměstnanci, typicky bez dedikovaného CISO, mohou rozumně implementované nástroje plnit funkci ekvivalentní několika pracovním úvazkům.

Mezi nejčastější překážky zavádění open-source řešení v MSP patří [15]:

- nedostatek personálu s bezpečnostními nebo administračními kompetencemi,
- obavy z nedostatečné podpory a dostupnosti aktualizací,
- komplikovanější integrace s existující infrastrukturou nebo cloudovými službami,
- potřeba kombinovat více nástrojů pro dosažení požadovaného pokrytí.

Pro MSP je přínosné, že mohou začít v malém rozsahu (např. nasazením nástroje pro správu přístupů nebo logování) a postupně systém rozvíjet podle potřeb a schopností organizace.

Zavedení těchto nástrojů však předpokládá určitou úroveň strategického plánování, neboť nesprávná volba řešení může vést k neefektivitě nebo bezpečnostním mezerám. Proto je nutné volit nástroje nejen podle jejich technických možností, ale také podle toho, jak dobře odpovídají potřebám dané společnosti a požadavkům normy ISO/IEC 27001.

5 ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část této práce poskytla ucelený pohled na systém řízení informační bezpečnosti v kontextu požadavků normy ISO/IEC 27001 a současných potřeb menších softwarových organizací. Byly vysvětleny základní principy informační bezpečnosti, význam řízeného přístupu k ochraně aktiv, a klíčové oblasti, které musí být v rámci ISMS řešeny. Dále byla podrobně analyzována struktura a klíčové požadavky normy ISO/IEC 27001, včetně modelu PDCA, jenž tvoří její metodologický rámec.

Zvláštní pozornost byla věnována těm oblastem ISMS, které vyžadují nebo umožňují technologickou podporu formou nástrojových řešení – identifikace rizik, správa aktiv, řízení přístupu, monitorování, reakce na incidenty a automatizace. Pro každou z těchto oblastí byl rozpracován teoretický základ, aktuální výzvy a důvody, proč je jejich řešení nezbytné i v prostředí malých firem.

Na tuto analýzu navázala kapitola věnovaná charakteristice open-source nástrojů jako alternativy ke komerčním řešením. Byly identifikovány výhody a limity této kategorie nástrojů, a dále specifické aspekty jejich nasazení v menších organizacích s omezenými zdroji.

Praktická část práce na tuto teoretickou základnu bezprostředně navazuje. Bude se zabývat výběrem a analýzou vhodných open-source nástrojů na základě kritérií vytvořených praktickým testováním, jejich přiřazením ke konkrétním požadavkům normy ISO/IEC 27001 a jejich praktickým ověřením v modelovém prostředí. Cílem je ukázat, jak lze i v prostředí menší softwarové společnosti efektivně implementovat prvky ISMS pomocí volně dostupných technických prostředků.

II PRAKTICKÁ ČÁST

6 KRITÉRIA PRO VÝBĚR NÁSTROJŮ V SOULADU S ISO/IEC 27001

Norma ISO/IEC 27001 nestanovuje konkrétní technologické prostředky, které by organizace měly použít k zajištění informační bezpečnosti. Místo toho klade důraz na princip přiměřenosti a efektivity – požaduje, aby organizace zavedla taková opatření, která odpovídají identifikovaným rizikům, rozsahu ISMS a celkovému kontextu činností. Z toho vyplývá, že výběr nástrojů je vždy individuální, ale musí být řízený, odůvodněný a auditovatelný. V praktické části jsou open-source nástroje vybírány na základě následujících hlavních kritérií:

Soulad s požadavky ISO/IEC 27001

Každý zvažovaný nástroj musí být přiřaditelný k alespoň jedné konkrétní oblasti nebo kontrolní položce normy ISO/IEC 27001, zejména podle přílohy A (např. A.5.9 – inventář aktiv, A.8.7 – ochrana proti malware, A.5.26 – monitorování aktivit). Při výběru je brán zřetel na to, zda nástroj reálně přispívá k naplnění požadavku, jaká opatření podporuje a jak lze výsledky jeho použití doložit v rámci auditu ISMS.

Funkční pokrytí a praktická použitelnost

Nástroj musí nabízet funkce, které odpovídají požadované oblasti použití – např. schopnost provádět skenování zranitelností, logovat systémové události, spravovat uživatelské účty nebo evidovat bezpečnostní incidenty. Zohledněna je také schopnost nástroje pracovat v reálném čase, automatizovat procesy nebo poskytovat výstupy vhodné pro další analýzu a reporting.

Aktivní vývoj a komunita

Z hlediska dlouhodobé udržitelnosti je důležité, aby byl nástroj aktivně vyvíjen, aktualizován a podporován komunitou nebo organizací. Tento faktor ovlivňuje nejen bezpečnost (např. reakce na zranitelnosti), ale i schopnost nástroje přizpůsobit se měnícím se potřebám. Nástroje, které nejsou aktualizovány nebo postrádají dokumentaci, jsou vyřazeny z výběru.

Kompatibilita a integrace

Je zohledněno, zda je nástroj možné bez větších obtíží nasadit v prostředí malé společnosti s hybridní infrastrukturou (on-premise a cloud). Dále se hodnotí možnosti integrace s ostatními nástroji, např. prostřednictvím API, standardizovaných formátů výstupů (JSON, syslog) nebo existujících konektorů.

Uživatelská náročnost a provozní efektivita

Vzhledem k omezeným personálním kapacitám malých firem je důležitým faktorem jednoduchost nasazení, konfigurace a provozu. Nástroj by měl mít přehledné rozhraní, dostupnou dokumentaci a pokud možno i vizuální komponenty pro správu a monitoring. Zohledněn je také požadavek na výkon a stabilitu.

Licence a právní aspekty

Všechny zvažované nástroje musí být licencovány jako open-source, a to pod svobodnou licenci (např. GNU GPL, MIT, Apache 2.0), která umožňuje jejich bezplatné používání, úpravy a distribuci v souladu s pravidly FOSS (Free and Open Source Software). Současně je posuzována právní transparentnost projektu a absence kontroverzních komponent

6.1 Metodický přístup této práce k výběru nástrojů

Cílem této práce je identifikovat a otestovat open-source nástroje, které mohou být využity jako podpora pro splnění klíčových požadavků normy ISO/IEC 27001 ve specifických podmínkách malé softwarové organizace. Aby bylo zajištěno, že výběr nástrojů bude systematický, konzistentní a auditovatelný, byl zvolen metodický přístup vycházející ze čtyř navazujících kroků.

Analýza normy ISO/IEC 27001:2022

Na základě podrobného studia normy ISO/IEC 27001:2022 a doplňující literatury (Calder & Watkins, Kenyon) byla vytvořena tabulka požadavků normy, které mohou být technicky podpořeny nástroji. Analýza se soustředila především na oblasti, které lze běžně automatizovat nebo podporovat nástroji, jako jsou správa aktiv, řízení přístupů, logování a monitoring, skenování zranitelností, reakce na incidenty a automatizace procesů..

Výběr kandidátních nástrojů

Výběr proběhl formou rešerše dostupných open-source řešení v komunitních i odborných zdrojích (např. GitHub, Open Source Security Foundation, odborné blogy, komunitní fóra). Dále byly zohledněny již zavedené nástroje s dobrou reputací v oblasti bezpečnosti (např. ELK Stack, Wazuh, TheHive). Nástroje, které nesplňovaly základní požadavky na bezpečnostní účel, aktivní vývoj, licenci nebo dokumentaci, nebo se ukázaly jako nevyhovující během praktického testování, byly vyloučeny.

Praktické ověření a přiřazení

Každý z vybraných nástrojů bude dále:

- přiřazen k příslušné kontrolní položce normy ISO/IEC 27001,
- popsán z hlediska funkce a způsobu použití,
- zhodnocen na základě výběrových kritérií,
- otestován v modelovém prostředí,
- a zařazen do srovnávací tabulky s uvedením výhod a nevýhod.

Tímto přístupem zajistíme, že výběr nástrojů bude odpovídat reálným potřebám organizací podobného typu a zároveň poskytne důvěryhodné výstupy za účelem posouzení jejich využitelnosti v souladu s normou ISO/IEC 27001.

7 MODELOVÁ ORGANIZACE A VÝCHOZÍ STAV BEZPEČNOSTI

Modelovou organizací pro praktickou část této práce je společnost založená v roce 2003 s centrálou v Praze a pobočkami v Brně a středních čechách . Společnost se specializuje na provoz a servis technických zařízení budov, instalaci řídicích systémů a vývoj souvisejících softwarových aplikací. Klíčovým produktem společnosti je cloudová platforma, určená pro měření, řízení a monitoring technologií v budovách.

Organizace má vlastní výzkumné a vývojové oddělení, které se zaměřuje na pokročilé algoritmy řízení a monitorování budov. Tým složený z přibližně 60 zaměstnanců vyvíjí software v jazycích jako C/C++, C#, .NET, SQL, PHP a JavaScript. Společnost také úzce spolupracuje s výzkumnými institucemi, jako jsou České vysoké učení technické v Praze, ETH Zürich a KU Leuven.

Z hlediska infrastruktury využívá firma hybridní model, kombinující on-premise servery s cloudovými službami. Většina softwarových aplikací běžících na serverech je vyvíjena interně, což umožňuje optimalizaci výkonu a funkcionality bez nutnosti placení licenčních poplatků.

8 VÝBĚR A POROVNÁNÍ NÁSTROJŮ PRO PODPORU SYSTÉMŮ ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI

Tato část práce se zaměřuje na výběr konkrétních open-source nástrojů, které odpovídají potřebám společnosti. Cílem není vytvořit univerzální seznam, ale navrhnout řešení, které je realisticky nasaditelné v prostředí s omezenými kapacitami, a přitom pokrývá všechny zásadní oblasti bezpečnosti.

Každá podkapitola se věnuje jedné z těchto oblastí – od správy aktiv a přístupových práv přes detekci událostí až po automatizaci. V rámci jednotlivých částí jsou nejprve představeny možnosti, následně porovnány dostupné nástroje a následně na základě praktického testování v prostředí společnosti stanovena výběrová kritéria a na jejich základě vybrán ten, který nejlépe odpovídá požadavkům.

8.1 Identifikace rizik a zranitelností

V modelové organizaci je v současnosti potenciál pro zavedení formalizovaného a technicky podloženého procesu identifikace zranitelností a hodnocení rizik se zaměřením na pravidelné automatizované skeny infrastruktury. Cílem je proto vybrat nástroje, které umožní:

- provádět pravidelné detekce technických zranitelností,
- podpořit procesní řízení rizik v souladu s ISO 27001:2022, konkrétně články 6.1 a A.8.8,
- integrovat výstupy do širšího rámce ISMS (např. incident handling, reporting).

Požadavky na nástroje pro identifikaci rizik a zranitelností

Pro efektivní podporu identifikace technických zranitelností a shromažďování podkladů pro analýzu rizik by měl vybraný nástroj splňovat následující požadavky:

- Možnost provádět síťové a systémové skenování s detekcí známých zranitelností na základě CVE databází.
- Schopnost generovat výstupy, které lze dále využít při hodnocení rizik (např. seznamy zranitelností, klasifikace dle závažnosti, návrhy nápravných opatření).
- Podporu aktualizace z veřejných zdrojů, zejména databází zranitelností a bezpečnostních standardů (např. NVD, OVAL, CPE).

- Možnost běžet v interním prostředí bez nutnosti cloudového napojení, s ohledem na bezpečnost a kontrolu nad daty.
- Integraci do širšího bezpečnostního ekosystému, zejména s logovacím nebo incident management systémem

Výběr a praktické porovnání nástrojů

Pro oblast identifikace rizik a zranitelností byly vybrány nástroje, které jsou běžně doporučovány v komunitních bezpečnostních přehledech, open-source portálech a technických fórech zaměřených na IT bezpečnost malých a středních organizací. Výběr se zaměřil zejména na řešení schopná provádět síťové a aplikační skenování, poskytovat aktuální informace o zranitelnostech a generovat výstupy využitelné pro následné posouzení rizik.

Tabulka 1 Nástroje pro identifikaci rizik a zranitelností

Nástroj	Zaměření	Výhody v MSP prostředí	Nevýhody / omezení
OpenVAS	Síťové skenování zranitelností	Aktivně udržovaný, široké pokrytí, solidní reporting	Náročnější konfigurace, vyšší zátěž na zdroje
Wazuh	Integrované detekce + logy + rizika	Součást SIEM stacku, korelace alertů, výstupy pro compliance	Vyžaduje integraci dalších komponent (Elastic)
Trivy	Skenování kontejnerů / image	Rychlé, nenáročné, ideální pro CI/CD prostředí	Omezené na kontejnery, bez síťového skenování
OpenSCAP	Hardening, systémové audity	Automatické ověřování bezpečnostních profilů	Vhodné spíše pro compliance než aktivní skenování

(zdroj: vlastní)

Pro prostředí společnosti je nejvhodnější nasadit kombinaci nástrojů:

- **Wazuh** – doporučeno jako nadstavba, pokud bude současně zaveden i centrální log management.

- **OpenVAS** – pro doplnění funkcionality, lze do budoucna uvažovat o OpenVAS pro plnohodnotné síťové a host-based skenování, včetně identifikace CVE a tvorby reportů,

OpenSCAP nebyl doporučen jako hlavní nástroj kvůli nižší flexibilitě a horší integraci do prostředí, kde je primární vývoj a síťová architektura spíše smíšeného charakteru (ne jen Linux hardening).

Tabulka 2 Porovnání nástrojů pro identifikaci rizik a zranitelností

Kritérium	OpenVAS	Wazuh	Trivy	OpenSCAP
Soulad s ISO 27001 (A.8.8)	☑	☑	☑	⚠
Funkční pokrytí	☑	☑☑	⚠	☑
Aktivní vývoj / podpora	☑	☑☑	☑	☑
Možnosti integrace	☑	☑☑	☑	⚠
Snadnost nasazení	⚠	☑	☑	☑
Vhodnost pro MSP	☑	⚠	☑	⚠

☑☑ = velmi vhodné, ☑ = vhodné, ⚠ = omezené

(zdroj: vlastní)

8.2 Správa aktiv

Společnost v současnosti eviduje svá IT aktiva převážně manuálně prostřednictvím tabulky v MS Excel. Za účelem splnění požadavků normy ISO/IEC 27001, konkrétně článků A.5.9 (Inventarizace aktiv) a A.5.10 (Přidělení odpovědnosti za aktiva) je vhodné implementovat řešení vybrané v této části.

Požadavky na nástroje pro správu aktiv

Pro zajištění souladu s normou ISO/IEC 27001 a efektivní správu aktiv by měl vybraný nástroj umožňovat:

- Automatizovanou inventarizaci hardwarových a softwarových aktiv.
- Sledování životního cyklu aktiv, včetně přidělování, údržby a vyřazení.
- Integraci s dalšími systémy, jako jsou helpdesk nebo monitoringové nástroje.

- Možnost generování reportů a auditních záznamů.

Výběr a praktické porovnání nástrojů

Pro oblast správy aktiv byly porovnány open-source nástroje identifikované na základě veřejně dostupných katalogů OSS nástrojů (např. Awesome-SIEM [16], GitHub repozitáře [17]). Výběr byl omezen na řešení s aktivním vývojem, dokumentací a komunitní podporou, která umožňuje jejich dlouhodobé udržení v provozu. Do užšího výběru byly zařazeny nástroje GLPI, Snipe-IT a OCS Inventory NG, které se nejčastěji vyskytují ve spojení s evidencí hardwaru, softwarových licencí a inventarizací IT prostředků.

Tabulka 3 Nástroje pro správu aktiv

Nástroj	Zaměření	Výhody v MSP prostředí	Nevýhody / omezení
Snipe-IT	Evidence a životní cyklus aktiv	Uživatelsky přívětivé rozhraní, sledování HW/SW/licencí, REST API	Neprovádí automatické skenování, vyžaduje ruční správu
GLPI	ITSM + správa aktiv + helpdesk	Komplexní ITIL řešení, integrace s helpdeskem a OCS, aktivní komunita	Vyšší nároky na správu, robustnější než malé společnosti často potřebují, nutnost placené verze
OCS Inventory NG	Automatická inventarizace zařízení	Automatické zjišťování zařízení v síti, detailní HW/SW data	Nutnost doplnění o nástroj pro správu

(zdroj: vlastní)

Pro potřeby společnosti, se jeví vzhledem k menšímu objemu aktiv jako nejvhodnější nástroj Snipe-IT. Nabízí jednodušší implementaci a uživatelsky přívětivé rozhraní. Zároveň na rozdíl od robustnější kombinace OCS Inventory NG + GLPI odpadá nutnost placené licence.

Tabulka 4 Porovnání nástrojů pro správu aktiv

Kritérium	Snipe-IT	GLPI	OCS Inventory NG
Automatizovaná inventarizace	⚠	☑	☑

Sledování životního cyklu aktiv	☑	☑	⚠
Integrace s helpdesk/monitoringem	⚠	☑	☑
Generování reportů a auditních záznamů	☑	☑	⚠
Uživatelská přívětivost	☑	⚠	⚠
Komunitní podpora a dokumentace	☑	☑	☑

☑ = vhodné, ⚠ = omezené

(zdroj: vlastní)

8.3 Řízení přístupu a identit

V současnosti je řízení přístupů ve firmě částečně centralizováno. V prostředí s hybridní infrastrukturou a přístupem více vývojářů může v případě absence centrálního řízení přístupů vznikat riziko:

- Nejednotného nastavení oprávnění,
- Absence vícefaktorového ověření (MFA),
- Chybějících revizí přístupových práv,
- Nemožnosti efektivního odebrání účtů při odchodu zaměstnance.

Požadavky normy ISO/IEC 27001, které pokrývají tuto oblast jsou opatření A.5.15–A.5.18 (řízení přístupu, přístupová oprávnění, autentizace, privilegované účty).

Požadavky na nástroje pro správu identit

Vybrané řešení musí umožnit:

- jednoduchou centrální správu uživatelů a jejich oprávnění, ideálně přes webové rozhraní.
- podporu základních standardů pro autentizaci, jako je LDAP nebo OpenID Connect, s možností napojení na ostatní interní systémy.
- základní auditní funkce, tedy záznamy o přihlášení a změnách přístupových práv.

- možnost zavedení dvoufaktorového ověřování (MFA) pro administrativní účty nebo vzdálený přístup.

Tabulka 5 Nástroje pro řízení přístupů a identit

Nástroj	Technologie	Výhody v MSP prostředí	Nevýhody / omezení
Keycloak	Identity Provider (IdP), OIDC, SAML	Moderní, podporuje federaci, MFA, jednoduché GUI	Vyšší nároky na provoz, méně vhodný pro čistě LDAP prostředí
OpenLDAP	LDAP directory service	Osvědčený, stabilní, nízké nároky na prostředí	Nutnost manuální konfigurace, žádné UI, složitější integrace
Authelia	Reverse proxy + MFA gateway	Dobrá integrace s webovými aplikacemi, podpora 2FA	Omezené na webový přístup, neřeší centrální správu identit
FreeIPA	LDAP + Kerberos + DNS + CA	Komplexní řešení, vhodné pro Linux-based infrastrukturu	Vysoké nároky na nasazení, nevhodné do Windows prostředí

(zdroj: vlastní)

Pro prostředí společnosti, je nejvhodnějším řešením nástroj Keycloak, který nabízí moderní řízení identit, širokou podporu autentizačních metod (včetně MFA), podporu pro federaci a jednoduché webové rozhraní pro správu. Je vhodný pro integraci s cloudovými službami, vývojovými nástroji a interními aplikacemi.

Doporučená konfigurace zahrnuje:

- napojení aplikací přes OIDC/SAML,
- role-based access control (RBAC),
- připojení k internímu LDAP (např. synchronizace s OpenLDAP),
- povinné dvoufázové ověření pro administrátorské účty.

OpenLDAP může být nasazen jako doplňkové řešení pro základní adresářové služby, zejména v prostředích s jednoduchou strukturou bez potřeby federace.

Tabulka 6 Porovnání nástrojů pro řízení přístupů a identit

Kritérium	Keycloak	OpenLDAP	Authelia	FreeIPA
Soulad s ISO 27001 (A.5.15–A.5.18)	☑	☑	⚠	☑
MFA / silné ověřování	☑	⚠	☑	☑
Podpora federace (OAuth2/OpenID/SAML)	☑	✗	⚠	⚠
Možnost auditování	☑	⚠	⚠	☑
Nasazení a správa	⚠	⚠	☑	⚠
Kompatibilita s hybridní infrastrukturou	☑	⚠	⚠	⚠

☑ = vhodné, ⚠ = omezené, ✗ = nevyhovující

(zdroj: vlastní)

8.4 Monitorování a detekce hrozeb

Společnost v současnosti pro detekci hrozeb nevyužívá žádný systém pro monitorování bezpečnostních událostí a detekci hrozeb. Potenciálem k rozšíření schopností je zde doplnění o systematické sledování logů, detekce anomálií a korelace událostí napříč infrastrukturou. Požadavky normy ISO/IEC 27001, které pokrývají tuto oblast jsou A.5.25 (Monitoring aktivit) a A.5.26 (Události informační bezpečnosti).

Požadavky na nástroje pro monitorování a detekci hrozeb

Pro zajištění efektivního monitorování a detekce hrozeb by měl vybraný nástroj umožňovat:

- Shromažďování a analýzu logů z různých systémů a aplikací.
- Detekci anomálií a potenciálních bezpečnostních incidentů.
- Generování alertů a notifikací v reálném čase.
- Možnost integrace s dalšími bezpečnostními nástroji a systémy.
- Podporu pro compliance a auditní požadavky.

Tabulka 7 Nástroje pro monitorování a detekci hrozeb

Nástroj	Zaměření	Výhody v MSP prostředí	Nevýhody / omezení
Wazuh	SIEM, HIDS, log management	Komplexní řešení pro sběr a analýzu logů, detekci hrozeb a compliance; škálovatelné	Vyšší nároky na konfiguraci a správu; může být složitější pro malé týmy
Zeek	Síťová analýza a detekce hrozeb	Detailní analýza síťového provozu; flexibilní skriptování; vhodné pro detekci anomálií	Vyžaduje hlubší znalosti síťové bezpečnosti; méně vhodné pro začátečníky
Suricata	IDS/IPS, síťová bezpečnost	Vysoký výkon; podpora vícevláknového zpracování; detekce na základě signatur a anomálií	Vyšší nároky na systémové prostředky; složitější konfigurace pravidel
OSSEC	HIDS, log analýza	Lehký a efektivní nástroj pro monitorování systémových událostí; snadná integrace	Omezené možnosti vizualizace a korelace událostí; méně funkcí oproti komplexnějším SIEM
Falco	Runtime bezpečnost pro kontejnery	Monitorování systémových volání v reálném čase; vhodné pro kontejnery a cloudové prostředí	Omezené na runtime prostředí; vyžaduje integraci s dalšími nástroji pro kompletní SIEM

(zdroj: vlastní)

Pro potřeby společnosti je nejvhodnějším řešením nasazení nástroje Wazuh, který bude implementován i pro pokrytí identifikace rizik a zranitelností. Nabízí komplexní funkce pro sběr a analýzu logů, detekci hrozeb a správu souladu s normami a certifikacemi (PCI DSS, HIPAA, NIST800-53 atd.). Jeho škálovatelnost a flexibilita umožňují přizpůsobení potřebám malé společnosti s možností budoucího rozšíření.

Pro doplnění síťové detekce hrozeb lze zvážit integraci nástroje Zeek, který poskytuje detailní analýzu síťového provozu a detekci anomálií. V prostředích využívajících kontejnery a cloudové služby může být vhodným doplňkem nástroj Falco pro monitorování runtime prostředí.

Tabulka 8 Porovnání nástrojů pro monitorování a detekci hrozeb

Kritérium	Wazuh	Zeek	Suricata	OSSEC	Falco
Soulad s ISO 27001 (A.5.25–A.5.26)	☑	☑	☑	☑	☑
Detekce anomálií	☑	☑	☑	⚠	☑
Integrace s dalšími systémy	☑	☑	☑	⚠	☑
Uživatelská přívětivost	⚠	⚠	⚠	☑	⚠
Nároky na systémové prostředky	⚠	⚠	⚠	☑	☑
Vhodnost pro malé a střední podniky	☑	⚠	⚠	☑	☑

☑ = vhodné, ⚠ = omezené

(zdroj: vlastní)

8.5 Reakce na incidenty

Detekce incidentů je v současnosti ve firmě řešena ad-hoc pomocí vestavných funkcí OS Windows na uživatelské úrovni. K rozšíření schopností o systematickou analýzu, vyhodnocení dopadů incidentů a zpětnou vazbu pro zlepšování procesů je vhodné implementovat samostatné technické řešení v souladu s požadavky normy ISO/IEC 27001, konkrétně A.5.25–A.5.27 (identifikace, odezva a poučení z bezpečnostních událostí).

Požadavky na nástroje pro řízení incidentů

Vybraný nástroj by měl umožnit:

- evidenci a klasifikaci incidentů podle typu, závažnosti a zdroje,
- přiřazení odpovědných osob a sledování postupu řešení,
- integraci s ostatními nástroji (SIEM, EDR, log management),
- podporu pro reporting a metriky (čas do odezvy, počet incidentů), napojení na threat intelligence (např. MISP, VirusTotal).

Tabulka 9 Nástroje pro správu incidentů

Nástroj	Zaměření	Výhody v MSP prostředí	Nevýhody / omezení
TheHive	Incident response platforma	Webové rozhraní, spolupráce více uživatelů, propojení s MISP a Cortex, REST API	Vyšší nároky na nasazení a správu (Elastic backend)
Cortex	Automatizace analýzy IoC	Integrace s TheHive, obsahuje stovky analyzátorů (hash, IP, URL)	Slouží pouze jako doplněk – vyžaduje propojení s jiným systémem
MISP	Threat intelligence sharing	Distribuovaný threat feed, sdílení IoC, napojení na další platformy	Není incident response nástroj v užším smyslu
RTIR	Request Tracker for Incident Response	Formální záznamy, workflow, přizpůsobení, vhodné pro ITIL prostředí	Zastaralejší UI, vyšší složitost přizpůsob

(zdroj: vlastní)

Pro potřeby společnosti je nejvhodnější nasazení platformy TheHive, která pokrývá celý cyklus zpracování bezpečnostního incidentu – od evidence, přiřazení úkolů, až po zpětnou analýzu. V kombinaci s nástrojem Cortex lze případně výrazně urychlit analýzu indikátorů kompromitace bez nutnosti ručního ověřování.

Tabulka 10 Porovnání nástrojů pro správu incidentů

Kritérium	TheHive	Cortex	MISP	RTIR
Soulad s ISO 27001 (A.5.25–A.5.27)	☑	⚠	⚠	☑
Evidence a workflow incidentů	☑	✗	✗	☑
Automatizace analýzy / playbooky	⚠	☑	✗	⚠
Integrace s log/SIEM nástroji	☑	☑	☑	⚠

Snadnost nasazení a obsluhy	⚠	⚠	☑	⚠
Vhodnost pro MSP	☑	⚠	☑	⚠

☑ = vhodné, ⚠ = omezené, ✗ = nevyhovující

(zdroj: vlastní)

8.6 Automatizace bezpečnostních procesů

Ve stávajícím prostředí společnosti chybí centralizovaný systém pro automatizaci bezpečnostních úloh. Události z logovacích systémů nejsou navzájem nijak propojeny, reakce na incidenty probíhá manuálně, a nejsou zavedeny žádné bezpečnostní playbooky nebo pravidla pro automatické akce při výskytu detekované hrozby. To vede k prodlevám v době reakce na incident.

Norma ISO/IEC 27001 sice explicitně nedefinuje "automatizaci", ale podporuje ji v rámci kontrol A.5.24–A.5.27 a A.5.30 (řízení změn, připravenost na incidenty a odezvu).

Požadavky na automatizační nástroje

Vybrané řešení by mělo umožnit:

- definovat a provádět bezpečnostní „playbooky“ – předdefinované reakce na určité události,
- integrovat různé bezpečnostní systémy (SIEM, skenery, EDR, alertovací nástroje),
- provádět analýzu, korelaci a reakce v reálném čase,
- být škálovatelné, rozšiřitelné a přizpůsobitelné malému týmu.

Tabulka 11 Nástroje pro automatizaci bezpečnostních procesů

Nástroj	Zaměření	Výhody v MSP prostředí	Nevýhody / omezení
Shuffle	SOAR platforma s vizuálními workflowy	Lehká, open-source SOAR platforma; jednoduché vizuální rozhraní; REST API	Méně modulů než u komerčních SOAR řešení; slabší dokumentace

StackStorm	Automatizační engine + workflows	Silná integrace s nástroji jako Wazuh, Ansible, GitHub; podporuje rule-based akce	Vyšší nároky na konfiguraci, spíše pro technicky vyspělé týmy
n8n.io	Obecný automatizační nástroj (i pro bezpečnost)	Intuitivní UI, rozsáhlý ekosystém integrací, napojení na SIEM, email, Slack	Nutnost pečlivé validace bezpečnostní relevance každé integrace
Rundeck	Automatizace provozních úloh	Ideální pro plánování a spouštění úloh na základě triggerů	Nepokrývá nativně bezpečnostní scénáře, spíše DevOps nástroj

(zdroj: vlastní)

Pro potřeby společnosti je nejvhodnější nástroj Shuffle, který nabízí jednoduché a vizuálně přehledné prostředí pro tvorbu workflow reakcí na incidenty (např. izolace IP, odeslání alertu, vytvoření záznamu v TheHive). Výhodou je snadná integrace s REST API ostatních komponent (např. Wazuh, Cortex, SMTP, Slack).

Alternativní volbou je nástroj n8n.io, který je obecnější, ale může být dobře využit i pro automatizaci reakčních kroků v jednoduchém prostředí.

Tabulka 12 Porovnání nástrojů pro automatizaci bezpečnostních procesů

Kritérium	Shuffle	StackStorm	n8n.io	Rundeck
Možnost reakce na bezpečnostní události	☑	☑☑	⚠	⚠
Integrace s log/SIEM nástroji	☑	☑	☑	⚠
Vizuální workflow editor	☑	⚠	☑	☑
Technická náročnost nasazení	☑	⚠	☑	☑
Vhodnost pro MSP	☑	⚠	☑	⚠

☑☑ = velmi vhodné, ☑ = vhodné, ⚠ = omezené

(zdroj: vlastní)

8.7 Shrnutí: Výběr open-source nástrojů pro podporu ISMS

Na základě systematického porovnání a hodnocení dostupných open-source řešení byla vybrána sada nástrojů, které pokrývají klíčové technické oblasti systému řízení informační bezpečnosti dle požadavků normy ISO/IEC 27001:2022. Výběr reflektuje potřeby společnosti, která disponuje omezenými personálními a finančními kapacitami, ale zároveň potřebuje plnohodnotnou technickou podporu ISMS.

Důvody výběru:

- **Soulad s normou ISO/IEC 27001:** Každý z nástrojů byl přiřazen ke konkrétním požadavkům a kontrolám normy.
- **Open-source licence:** Všechny nástroje jsou bezplatně dostupné a otevřené pro přizpůsobení.
- **Vhodnost pro malé společnosti:** Výběr zohledňuje nároky na provoz, správu a škálovatelnost.
- **Možnost integrace:** Nástroje byly voleny tak, aby je bylo možné propojit do funkčního celku (např. přes API, SIEM, SOAR).

Tabulka 13 Vybrané nástroje pro implementaci a jejich vtaž ke kontrolám ISO/IEC 27001:2022

Oblast ISMS	Vybraný nástroj	Relevantní kontroly ISO/IEC 27001:2022
Identifikace rizik a zranitelností	Wazuh	6.1, A.5.9, A.8.8
Správa aktiv	Snipe-IT	A.5.9, A.5.10, A.7.9
Řízení přístupu a identit	Keycloak	A.5.15–A.5.18, A.8.2
Monitorování a detekce hrozeb	Wazuh (+ Zeek)	A.5.25, A.5.26, A.8.7, A.8.15, A.8.16
Reakce na incidenty	TheHive	A.5.25, A.5.26, A.5.27
Automatizace bezpečnostních procesů	Shuffle	A.5.24, A.5.25, A.5.30

(zdroj: vlastní)

Tímto výběrem je pokryto všech šest klíčových oblastí ISMS, jejichž technické zajištění bylo identifikováno jako kritické pro řízení informační bezpečnosti ve zvolené modelové firmě. Tato sada nástrojů tvoří základ pro implementační plán, který bude rozpracován v následující kapitole.

9 IMPLEMENTACE

Tato kapitola popisuje, jakým způsobem bude v praxi zaveden systém nástrojů pro řízení informační bezpečnosti ve firmě. Cílem je nejen popsat, co se bude nasazovat, ale hlavně jak a proč – s ohledem na konkrétní podmínky ve firmě, dostupné zdroje a potřeby každodenního provozu.

Před samotnou implementací byla navržena kombinace nástrojů pokrývajících základní bezpečnostní funkce: dohled nad stanicemi a servery, analýzu síťového provozu, správu identit a reakci na incidenty. Každý nástroj byl zvolen s ohledem na své konkrétní uplatnění v systému řízení bezpečnosti informací a na možnost propojení s ostatními komponentami. Řešení je navrženo tak, aby bylo vzájemně provázané, technicky proveditelné a připravené na následné rozšíření dle potřeb organizace.

Plán je rozdělen do několika kroků, které na sebe logicky navazují: od základního nasazení nástrojů, přes jejich propojení a integraci do infrastruktury, až po ověření funkčnosti a připravenosti organizace pracovat s novým řešením. Kromě technické instalace bude součástí i základní nastavení rolí, definice odpovědností a zajištění, že zavedené nástroje budou skutečně používány efektivně.

Výstupem této části bude ucelený návrh, jak v prostředí společnosti vybudovat funkční a udržitelný bezpečnostní rámec s využitím open-source nástrojů.

9.1 Postup nasazení a integrace nástrojů

Implementace navrženého bezpečnostního řešení bude probíhat postupně – po částech, které na sebe logicky navazují. Cílem je vyhnout se zbytečnému přetížení technického týmu a zároveň co nejrychleji pokrýt oblasti, kde aktuálně existují největší rizika. Nasazení proběhne ve třech hlavních fázích.

Fáze I – Základní zabezpečení a inventarizace

Cíl: Zavést základní přehled o infrastruktuře a nastavit řízení přístupových práv.

Krok	Popis
1.1	Instalace Snipe-IT – evidence aktiv
1.2	Konfigurace základních aktiv (servery, stanice, vývojová zařízení)
1.3	Nasazení Keycloak pro správu identit.

1.4 Nastavení oprávnění a autentizace pro interní aplikace

Výstup: Firma má centrální přehled o aktivech a jednotné řízení přístupů.

Fáze II – Monitoring a detekce hrozeb

Cíl: Získat přehled o tom, co se děje v síti a na klíčových systémech.

Krok	Popis
2.1	Instalace Wazuh – nasazení agentů na servery a pracovní stanice
2.2	Zprovoznění Zeek pro monitorování síťového provozu
2.3	Konfigurace pravidel a alertů, prvotní testy detekce
2.4	Vytvoření dashboardů pro sledování stavu a vývoje incidentů

Výstup: Organizace má centralizovaný log management a funkční základ pro detekci hrozeb.

Fáze III – Incidenty a automatizace

Cíl: Zvládat bezpečnostní události rychle a opakovatelně.

Krok	Popis
3.1	Instalace TheHive – řízení incidentů, automatizovaná analýza
3.2	Propojení s Wazuh – automatické vytváření případů na základě alertů
3.3	Instalace Shuffle – nastavení základních workflow (notifikace, reakce)
3.4	Testování reakčních scénářů (např. podezřelá IP, změna konfigurace)

Výstup: Incidenty jsou zachyceny, evidovány, analyzovány a řešeny systematicky.

Nasazení bude probíhat převážně v prostředí Linux (Ubuntu Server) a využije virtuální stroje (VM). Pro datové úložiště bude využita existující infrastruktura (on-premise storage + záloha v cloudu). Konfigurace bude dokumentována za účelem opakovatelnosti a auditovatelnosti.

9.2 Ověření technických a organizačních předpokladů

Zavedení bezpečnostního řešení nutně vyžaduje organizační podporu a technickou připravenost. Bez těchto předpokladů může i sebelepší software selhat. [18] V této části shrnujeme klíčové požadavky, které musí být před spuštěním ostrého provozu splněny

9.2.1 Technické předpoklady

Než může být bezpečnostní řešení uvedeno do plného provozu, je nezbytné ověřit, zda je dostatečně připravené technické zázemí. Jednotlivé nástroje mají specifické nároky na výkon, úložiště, síťovou infrastrukturu i zabezpečení přístupu. Tabulka níže shrnuje klíčové oblasti a požadavky, které byly zohledněny při návrhu a přípravě implementace. U každé oblasti je uveden aktuální stav, který odráží reálnou připravenost systému před spuštěním ostrého provozu.

Tabulka 14 Technické požadavky na provozní prostředí před nasazením řešení

Oblast	Požadavek	Stav
Serverová infrastruktura	Virtuální servery s Linux (Ubuntu 24.04.2 LTS), min. 4 CPU, 8–16 GB RAM	✓ dostupné
Síťová architektura	Segmentace pro monitorování provozu	⚠ částečně připraveno
Úložiště	Minimálně 500 GB pro logy a data z monitorovacích nástrojů	✓ zajištěno
Záloha a obnova	Zálohování konfiguračních souborů, databází a incident dat	✓ zajištěno
Přístup a zabezpečení	VPN přístup pro administrátory	⚠ v plánu

(zdroj: vlastní)

9.2.2 Organizační předpoklady

Kromě technického zajištění hraje zásadní roli také organizační připravenost. Efektivní fungování systému řízení informační bezpečnosti vyžaduje jasné stanovené odpovědnosti, podporu ze strany vedení a alespoň základní povědomí zaměstnanců o bezpečnostních pravidlech. Tyto faktory zásadně ovlivňují nejen úspěšné nasazení nástrojů, ale i jejich každodenní používání. [18] V této části jsou uvedeny hlavní organizační podmínky.

Tabulka 15 Organizační požadavky na provozní prostředí před nasazením řešení

Oblast	Požadavek	Stav
Odpovědnost za ISMS	Jmenovaná osoba zodpovědná za řízení informační bezpečnosti	☑ zajištěno

Podpora vedení	Schválení návrhu řešení a souhlas s provozními dopady	☑ potvrzeno
Školení zaměstnanců	Úvodní školení o základních bezpečnostních zásadách	⚠ částečně realizováno
Definice bezpečnostních rolí	Určení rolí pro správu přístupů, správu incidentů a dohled nad nástroji	⚠ v přípravě
Dokumentace a postupy	Vytvoření základních bezpečnostních směrnic a provozních postupů	⚠ v přípravě
Odpovědnost a vlastnictví	Jasně definovaná role pro bezpečnostní správu (Security Officer)	⚠ určeno, ale neformálně
Zajištění údržby	Plán pravidelných kontrol, aktualizací, reakce na incidenty	⚠ v přípravě

(zdroj: vlastní)

9.3 Harmonogram implementace

Implementace navržených nástrojů bude probíhat postupně ve čtyřech týdnech. Cílem je vyhnout se zahlcení malého interního týmu a zároveň udržet logickou návaznost jednotlivých kroků – od základní evidence aktiv a správy přístupů až po monitoring, reakci na incidenty a automatizaci bezpečnostních procesů.

Tabulka 16 Seznam jednotlivých úkolů a časový plán implementace

Týden	Aktivity	Zodpovědná role	Poznámka
1. týden	• Instalace a základní konfigurace Snipe-IT • Definice kategorie aktiv • Nasazení Keycloak • Testování a validace, aktualizace dokumentace	IT správce + vývojový vedoucí	Důraz na zmapování aktiv
2. týden	• Nasazení Wazuh agentů a serveru • Aktivace Zeek v síti • Nastavení dashboardů pro incidenty • Nastavení logování a alertů • Testování a validace, aktualizace dokumentace	IT správce	Vyžaduje přístup do produkční sítě

3. týden	• Instalace TheHive + Cortex • Instalace Shuffle + workflow • Propojení s Wazuh (automatizovaný výstup alertů jako případů) • Testovací scénáře reakce na incidenty • Testování a validace, aktualizace dokumentace	Security Officer + admin	Tvorba postupů evidence a eskalace incidentů
4. týden	• Nastavení reakčních workflow (např. alert → email + ticket) • Otestování reakčních workflow • Finalizace dokumentace a školení • Závěrečná kontrola funkčnosti konfigurace systémů	IT správce + vedení + správce ISMS	Příprava na přechod do rutinního provozu

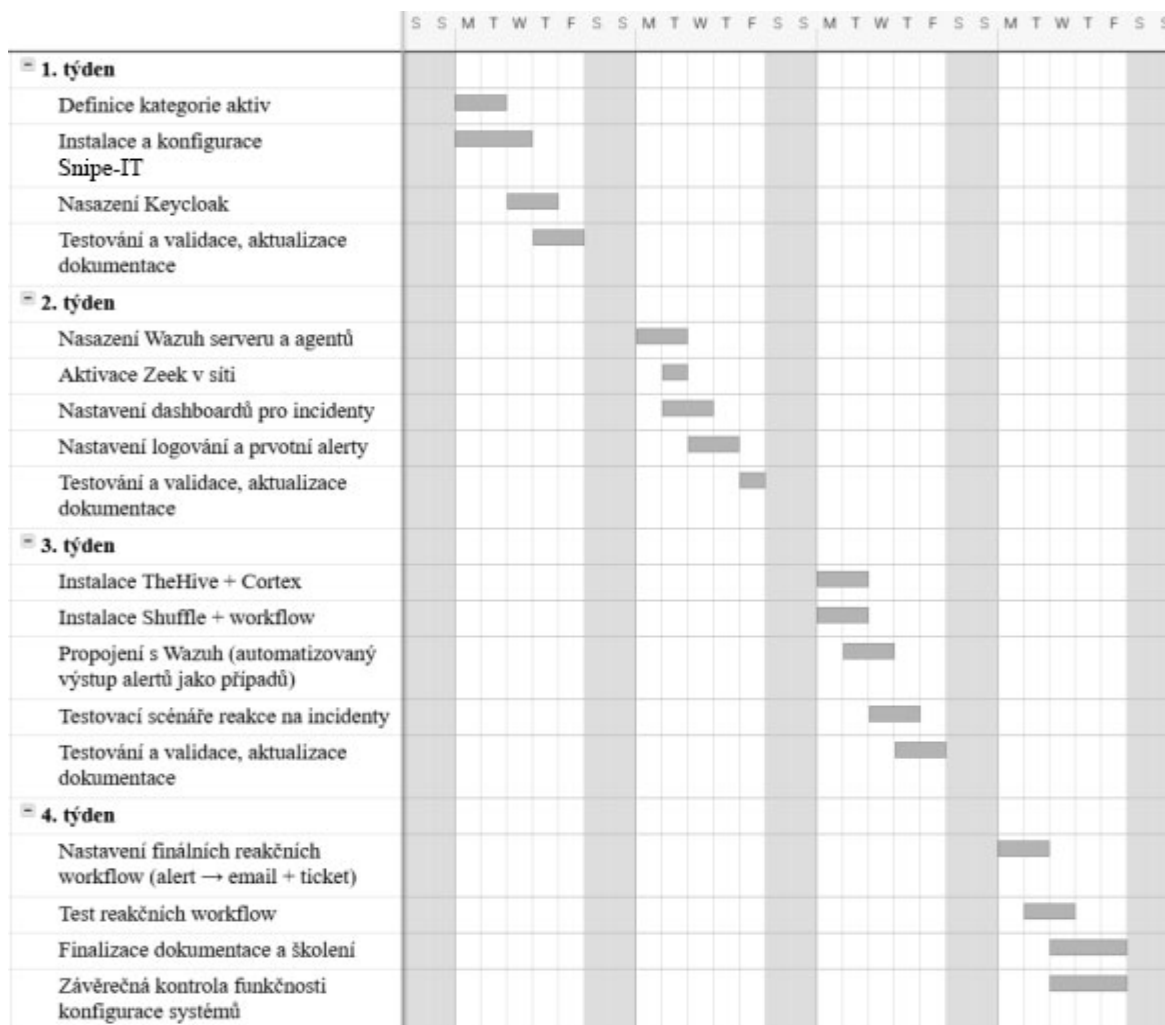
(zdroj: vlastní)

Každá fáze je navržena tak, aby přinesla měřitelný přínos i v případě, že se z jakýchkoli důvodů nepodaří nasadit celý balík řešení. Tím minimalizujeme riziko neefektivního vynaložení času a zdrojů. Harmonogram počítá s tím, že firma disponuje jedním hlavním IT správcem, a proto byl plán záměrně rozložen na čtyři týdny.

Navržený harmonogram zahrnuje čtyři týdny intenzivní práce, během kterých dochází k postupnému nasazení, propojení a otestování všech klíčových nástrojů systému řízení informační bezpečnosti. Každý týden je strukturován jako funkční celek, zahrnující instalaci, konfiguraci, validaci i dokumentaci dané části řešení.

Plán zohledňuje omezené kapacity malé organizace, a proto jsou jednotlivé aktivity rozděleny mezi více odpovědných osob podle odbornosti. Výrazný důraz je kladen na dokumentaci, testování a validaci v průběhu každého kroku – tak, aby bylo možné v případě problémů rychle reagovat a předejít selhání v ostrém provozu.

Ve čtvrtém týdnu je počítáno s finálním doladěním automatizačních scénářů a s interním školením, které zajistí, že nasazené řešení bude provozně udržitelné i bez potřeby externí podpory. Tento přístup umožňuje hladký přechod z fáze implementace do stabilního provozu, při zachování kontroly nad všemi součástmi systému.



Obrázek 2 Časový harmonogram implementace

(zdroj: vlastní)

9.4 Rizika během implementace a návrhy jejich mitigace

Při zavádění bezpečnostních nástrojů je potřeba počítat s některými úskalími, která se netýkají jen technické stránky, ale často se objevují i v oblasti organizace práce, přístupu lidí nebo časového vytížení. V této části se proto zaměříme na některá rizika, která nás mohou při implementaci zpomalit nebo ohrozit, a zároveň navrhujeme konkrétní kroky, jak těmto problémům předejít.

9.4.1 Nejasné rozdělení odpovědností

V menších firmách bývá běžné, že jeden člověk má na starosti všechny provozní záležitosti okolo IT infrastruktury. Pokud se nepřidělí a nezadokumentuje konkrétní zodpovědnost za správu jednotlivých nástrojů, stane se z implementace jen jednorázový projekt, který se postupně rozpadne.

Mitigace: Jasně určit správce pro jednotlivé nástroje – ideálně přímo při jejich nasazení. Může jít o jednu osobu, ale ta musí mít dostatek kapacity v rámci svých pracovních povinností a podporu vedení.

9.4.2 Nedostatek času

Zavedení nových nástrojů je časově náročné, obzvlášť když tým zároveň pracuje na vývoji, správě infrastruktury a dalším běžném provozu. Rizikem je odkládání úkolů, nedotažená konfigurace a chybějící dokumentace.

Mitigace: Naplánovat implementaci po částech. Začít u systémů, které mají největší přínos za s nejmenším úsilím (např. GLPI a Wazuh) a ostatní nasazovat postupně.

9.4.3 Slabá motivace týmu

Bezpečnost často není pro většinu lidí ve firmě prioritou dokud nedojde bezpečnostnímu incidentu, jako např. ransomware nebo únik dat. Nové postupy, někdy vnímané jako omezení, pak mohou být vnímána jako zbytečná komplikace.

Mitigace: Vysvětlit účel jednotlivých opatření a nástrojů, že jde hlavně o prevenci – a že nástroje jako Wazuh nebo TheHive pomůžou nejen při útoku, ale i při běžných provozních incidentech. Vysvětlit, že pokud jsou opatření a nástroje implementovány správně, nepředstavují větší omezení a významně zvýší bezpečnost infrastruktury.

9.4.4 Podcenění a absence dokumentace

ISO 27001 vyžaduje rozsáhlou dokumentaci, což může být pro malé společnosti náročné na čas i zdroje. V malých firmách bývá psaní dokumentace často až poslední na seznamu úkolů. Absence dokumentace však může již během několika měsíců způsobit, že se nebude nikdo orientovat v tom, co a proč bylo nastaveno.

Mitigace: Vést si základní technický deník už při implementaci – ideálně v nástroji, který se už zároveň používá (např. poznámky v GLPI). Využít předpřipravené šablony, zavést systém správy dokumentů a pravidelně revidovat a aktualizovat dokumentaci

9.4.5 Nedostatečná podpora vedení

Bez aktivní podpory vrcholového vedení může implementace ISMS postrádat potřebné zdroje, směr a motivaci zaměstnanců. [18]

Mitigace: Zajistit zapojení vedení od počátku projektu, prezentovat přínosy ISMS pro podnikání a pravidelně informovat o postupu implementace.

9.4.6 Omezené zdroje a kapacity

Malé společnosti často čelí omezeným personálním a finančním zdrojům, což může zpomalit nebo ohrozit implementaci ISMS. [15]

Mitigace: Provést důkladnou analýzu potřebných zdrojů, využít open-source nástroje a zvážit externí konzultace pro klíčové oblasti.

9.4.7 Integrace s existujícími procesy

Nová bezpečnostní opatření mohou být v konfliktu s již zavedenými procesy, což komplikuje jejich implementaci.

Mitigace: Provést mapování stávajících procesů, identifikovat oblasti překryvu a přizpůsobit nové postupy tak, aby byly kompatibilní s existujícími procesy.

9.4.8 Udržitelnost a kontinuální zlepšování

Po počáteční implementaci může dojít k poklesu zájmu o ISMS, což vede k zastarání opatření a zvýšení rizik. [18]

Mitigace: Zavedení pravidelných interních auditů, přezkumy a aktualizace politik, podpora kultury neustálého zlepšování a sledování nových hrozeb a technologie.

9.5 Instalace a základní konfigurace nástrojů

Po návrhu architektury a vytvoření implementačního plánu následuje praktická část, ve které byly vybrané nástroje postupně nasazeny v produkčním prostředí společnosti. Cílem této kapitoly je zachytit klíčové kroky instalace jednotlivých komponent, popsat zvolený přístup k jejich konfiguraci a zdokumentovat první výsledky, které potvrzují jejich funkčnost a připravenost k ostrému provozu.

Vzhledem k omezeným zdrojům a charakteru společnosti byl zvolen modularizovaný přístup: každý nástroj byl nasazen samostatně a teprve následně integrován do širšího bezpečnostního rámce. Popis postupně zahrnuje všechny hlavní oblasti ISMS, od správy aktiv a řízení přístupů až po detekci hrozeb, správu incidentů a automatizaci procesů.

Instalace byla realizována v souladu s harmonogramem implementace (viz kap. 9.4), ve třech základních fázích. V této kapitole bude podrobně zachycen průběh každé fáze,

včetně případných omezení, specifik prostředí a praktických poznatků získaných během zavádění jednotlivých nástrojů.

9.5.1 Nasazení a konfigurace Snipe-IT

Pro oblast správy IT aktiv byla v rámci implementace zvolena platforma Snipe-IT, která oproti kombinaci GLPI a OCS Inventory NG nabízí jednodušší nasazení a správu, a zároveň plně vyhovuje požadavkům malé organizace na přehlednou evidenci zařízení, licencí a jejich životního cyklu, bez nutnosti pořízení placené verze.

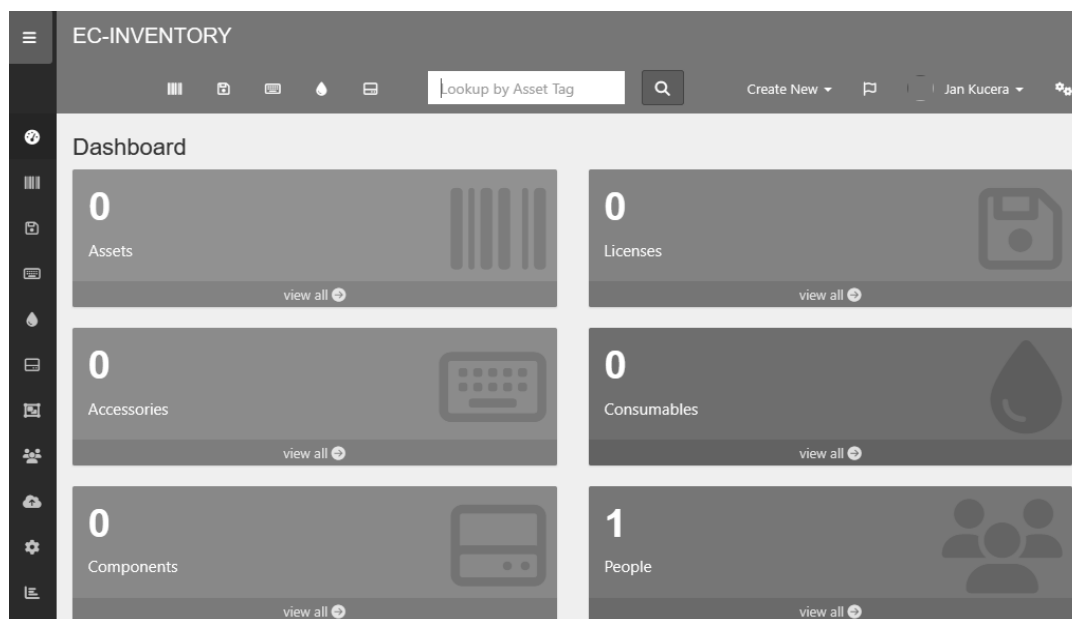
Tabulka 17 Použité prostředí – Snipe-IT

Oblast	Požadavek	Stav
Serverová infrastruktura	Virtuální server s Ubuntu Server 24.04.2 LTS, 2 CPU, 4 GB RAM, 40 GB disk	✓ dostupné
Síťové prostředí	Interní VLAN s přístupem do LAN a vývojových zařízení	✓ připraveno
Základní služby	Docker, Docker Compose, otevřený port 8080, správné síťové routování	✓ nasazeno
Verze Snipe-IT	Stabilní build z oficiálního Docker repozitáře (2024)	✓ aktuální

(zdroj: vlastní)

Postup instalace:

- Instalace Docker a Docker Compose
- Vytvoření složky pro Snipe-IT
- Stažení a modifikace souboru `docker-compose.yml` z oficiálního repozitáře <https://github.com/grokability/snipe-it/blob/master/docker-compose.yml> a vytvoření souboru `.env`
- Pomocí `docker-compose up -d` dojde k vytvoření a spuštění všech definovaných služeb.“
- Přístup na webové rozhraní přes port 8080 a následování instrukcí k instalaci



Obrázek 3 Výchozí dashboard instance EC-INVENTORY po inicializaci Snipe-IT

Základní nastavení

- Byla vytvořena testovací struktura IT aktiv pro import: notebooky, servery, síťové prvky.

	A
1	Asset Tag, Name, Model, Status, Serial, Location
2	LAPTOP-001, Dell XPS - Marketing, Dell XPS 15, In Use, ATC2233, PRG
3	SERVER-101, ProLiant - Database, HP ProLiant DL380, Ready to Deploy, DEF456, Data Center

Obrázek 4 Náhled CSV souboru pro import aktiv

- Vytvoření základních kategorií zařízení (hardware/software, server, laptop atd.)
- Ověření úspěšného importu dat

Shrnutí a výsledky

Instalace proběhla úspěšně, Snipe-IT běží ve vnitřní síti a je přístupný přes webové rozhraní. Data jsou úspěšně importována. Tento nástrojový blok tak zajišťuje základní požadavek ISO 27001 na správu aktiv (kontroly A.5.9–A.5.10).

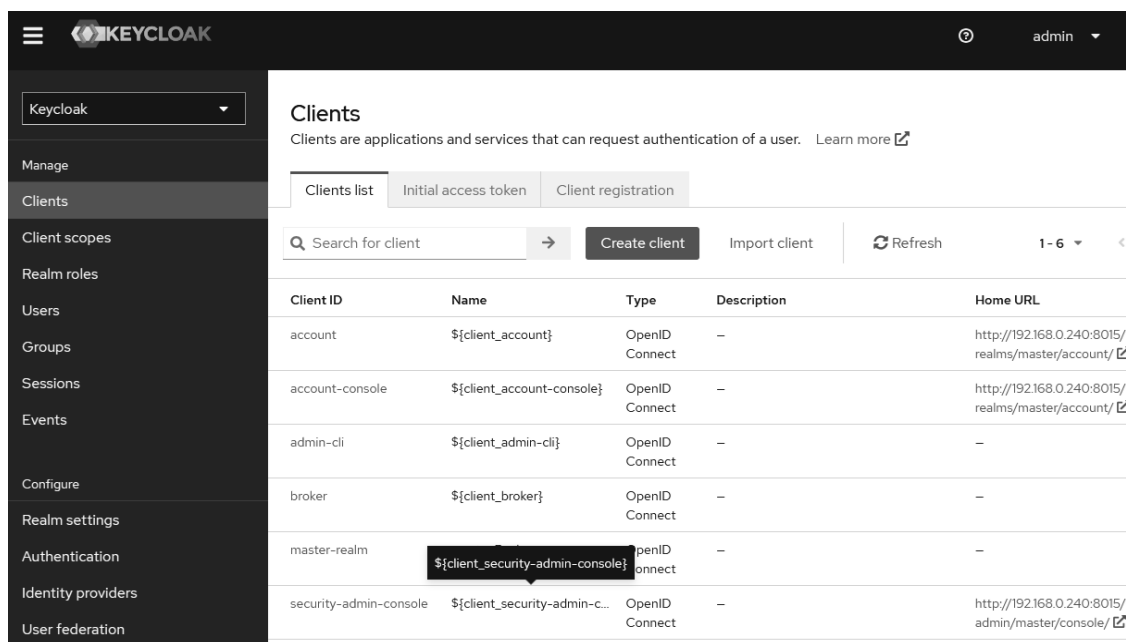
9.5.2 Nasazení a konfigurace Keycloak

Cíl této části spočíval v zavedení centrálního systému pro správu identit a přístupových práv v rámci interních aplikací a administrativních nástrojů. S ohledem na plánovanou integraci

více bezpečnostních komponent bylo nezbytné vytvořit jednotný autentizační mechanismus s podporou víceúrovňového přístupu, který lze dále rozšiřovat o moderní autentizační standardy (OpenID, OpenID Connect, OAuth2, SAML).

Postup instalace:

- Instalace Docker a Docker Compose
- Vytvoření složky pro Keycloak
- Vytvoření souboru docker-compose.yml dle šablony z oficiálních stránek <https://www.keycloak.org/server/containers>
- Pomocí `docker-compose up -d` dojde k vytvoření a spuštění všech definovaných služeb.



Obrázek 5 Výchozí stránka admin rozhraní instance Keycloak po úspěšné instalaci

Počáteční nastavení

Během inicializace byl vytvořen správce (realm admin), základní realm („ec-local“) a dvě uživatelské role:

- admin-it (správce infrastruktury),
- user-dev (vývojářský přístup)

Zabezpečení přístupu

- Základní autentizace probíhá pomocí uživatelského jména a hesla, pro budoucí fáze je připravena podpora dvoufaktorové autentizace (TOTP).

Napojení na ostatní systémy

- Prvotní testovací integrace s TheHive byla úspěšně nakonfigurována: Keycloak bude použit jako centrální poskytovatel identity pro TheHive, a to prostřednictvím SSO pomocí OpenID.
- Integrace s ostatními systémy bude probíhat postupně dle možností

Shrnutí a výsledky

Keycloak byl úspěšně nasazen a konfigurován jako jednotný nástroj pro správu identit a řízení přístupu k interním systémům. Systém je připraven pro další rozšiřování – např. přidání politik přístupu, MFA nebo externích autentizačních providerů. Už nyní však plní klíčovou funkci pro pokrytí požadavků normy ISO/IEC 27001 v oblasti přístupových práv (kontroly A.5.15–A.5.18).

9.5.3 Nasazení Wazuh a základní konfigurace detekce hrozeb

Cílem této části je zavést nástroj pro monitorování bezpečnostních událostí a detekci hrozeb na úrovni serverů a koncových zařízení. Zvolen byl open-source nástroj Wazuh, který plní funkci základní SIEM platformy. V rámci implementace byl systém nastaven tak, aby umožnil centralizovaný sběr logů, základní analýzu incidentů a jejich vizualizaci.

Tabulka 18 Použité prostředí - Wazuh

Oblast	Požadavek	Stav
Serverová infrastruktura	Virtuální stroj s Ubuntu Server 24.04.2 LTS, 4 vCPU, 8 GB RAM, 200 GB SSD	✓ dostupné
Verze nástroje	Wazuh 4.6.x	✓ aktuální
Instalační metoda	Oficiální Wazuh All-in-One (docker-compose stack)	✓ úspěšně nasazeno
Způsob sběru dat	Agenti pro Linux a Windows, Syslog vstup z externích zařízení	✓ funkční

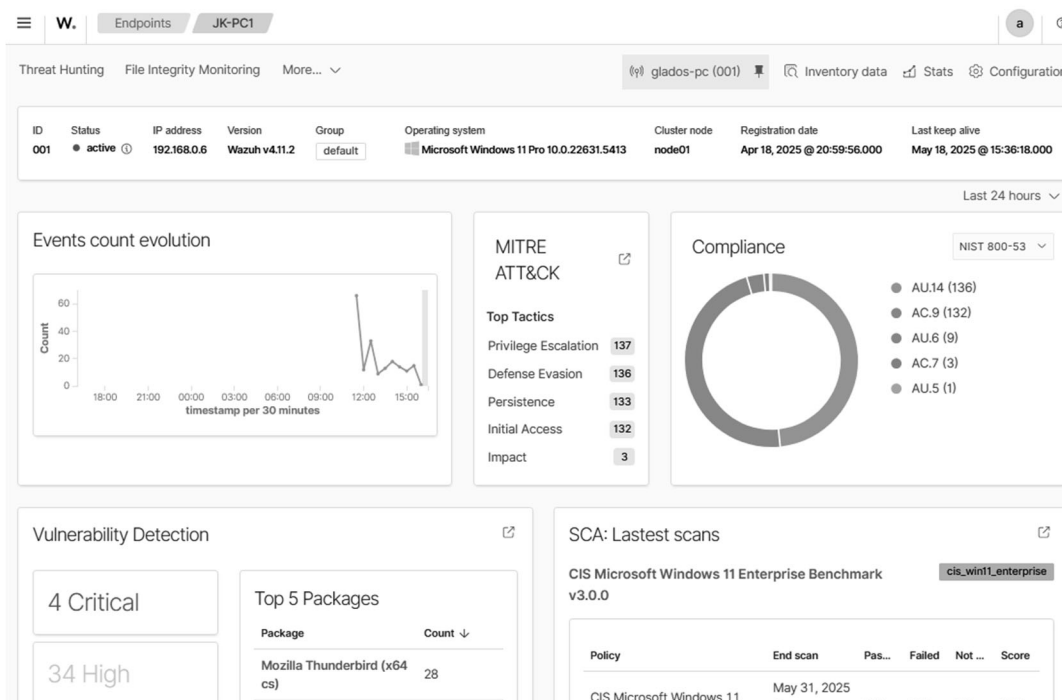
(zdroj: vlastní)

Postup instalace

1. Pomocí nástroje git byl stažen oficiální Wazuh deployment stack z repozitáře <https://github.com/wazuh/wazuh-docker>.
2. Konfigurace jednotlivých služeb (Wazuh manager, Kibana, Elasticsearch) byla provedena úpravou .env souboru před spuštěním.
3. Pomocí docker-compose byly všechny kontejnery spuštěny jako služba, přístup ke konzoli byl nastaven přes reverzní proxy s HTTPS.
4. V databázi byly inicializovány indexy pro logování a analýzu událostí.

Základní konfigurace

1. Na tři testovací zařízení (Linux server, vývojářský notebook, Windows stanice) byly nainstalovány Wazuh agenti a registrováni u Wazuh managera.
2. Aktivovány byly moduly pro sledování integrity souborů (FIM), detekci rootkitů a auditů přihlášení.
3. Konfigurační šablony byly přizpůsobeny pro potřeby prostředí malé společnosti – zaměřeno na:
 - změny systémových souborů,
 - neoprávněné přístupy,
 - podezřelé procesy a síťové chování.



Obrázek 6 Dashboard s detaily o monitorované pracovní stanici “JK-PC1”

(zdroj: vlastní)

Integrace a omezení

Dashboards v Kibana byly upraveny pro snadné sledování událostí podle zařízení a typů alertů. Emailová notifikace alertů byla nastavena přes SMTP relay na interní bezpečnostní schránku.

Shrnutí a výsledky

Wazuh byl úspěšně nasazen a konfigurován jako centrální systém pro detekci hrozeb a správu bezpečnostních událostí. Již během prvních testů byly zachyceny reálné případy – např. pokus o spuštění neautorizovaného PowerShell skriptu nebo neúspěšná autentizace u vývojářské stanice. Nástroj tak plně pokrývá požadavky normy ISO/IEC 27001, zejména v oblastech:

- **A.5.25** (monitorování systémů),
- **A.5.26** (detekce událostí),
- **A.5.27** (reakce na incidenty),
- **A.8.7** (ochrana proti malwaru).

9.5.4 Instalace a konfigurace TheHive

Pro efektivní řízení bezpečnostních incidentů je nezbytné mít nástroj, který umožňuje systematicky pracovat s událostmi detekovanými v monitorovacích systémech. Cílem této části bylo nasadit platformu, která umožní incidenty evidovat, analyzovat a sledovat jejich řešení. Zvolen byl nástroj TheHive, který poskytuje rozhraní pro řízení bezpečnostních událostí, a s ním integrovaný Cortex, určený k automatizované analýze tzv. indikátorů kompromitace (např. IP adres, hashů souborů, domén).

Oba nástroje byly zprovozněny ve vzájemně provázané konfiguraci a slouží jako centrální bod pro správu alertů z Wazuh i jiných zdrojů. Jejich hlavní výhodou je možnost pracovat s incidenty ve strukturované podobě a udržet přehled o tom, kdo co řeší, v jakém je to stavu a jaká opatření byla provedena.

Tabulka 19 Použité prostředí – The Hive

Oblast	Požadavek	Stav
Serverová infrastruktura	Ubuntu Server 24.04.2 LTS (VM), 4 vCPU, 8 GB RAM, 100 GB SSD	✓ dostupné
Verze nástrojů	TheHive 5.x, Cortex 3.x	✓ aktuální
Instalační metoda	Docker Compose (TheHive-Project image)	✓ úspěšně nasazeno
Databázové backendy	Cassandra + Elasticsearch	✓ nasazeno
Komunikační rozhraní	REST API a webové uživatelské rozhraní	✓ funkční

(zdroj: vlastní)

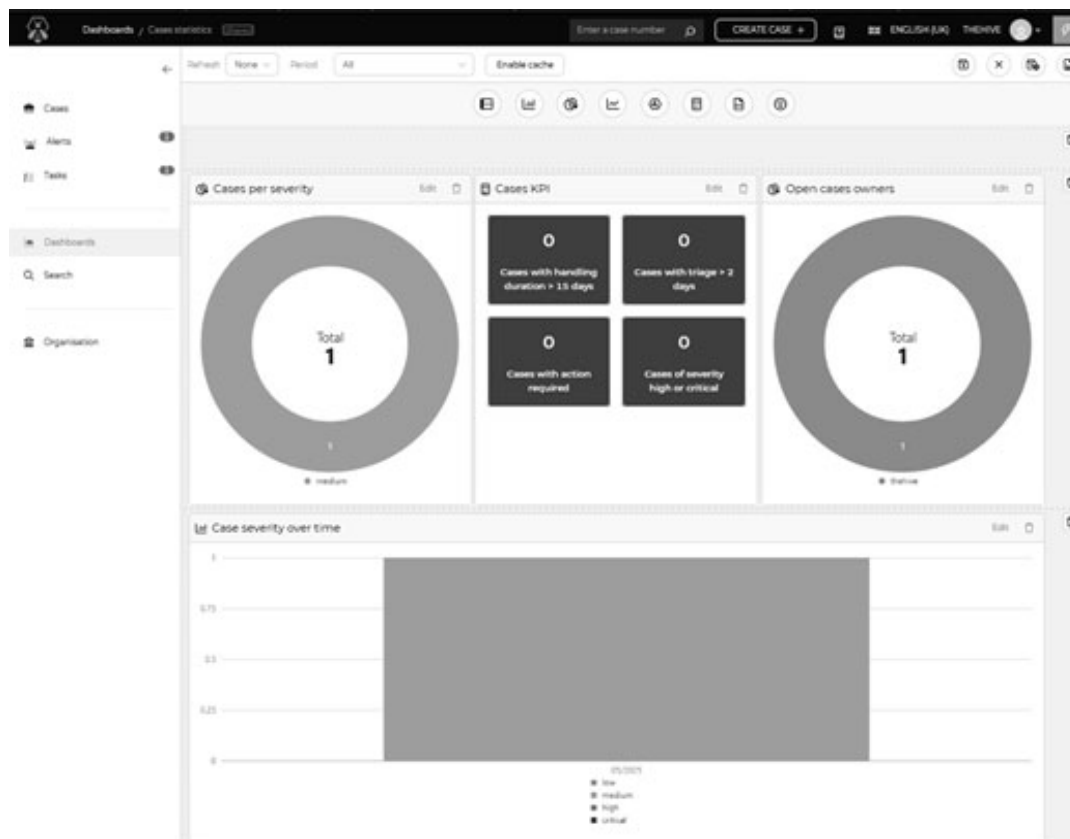
Postup instalace

1. Stažen byl oficiální Docker Compose balíček pro TheHive z repozitáře <https://github.com/TheHive-Project>.
2. Služby byly konfigurovány pomocí .env a application.conf – zejména autentizace, porty, adresy backendů a šifrování.
3. Spuštěny kontejnery: thehive, cortex, cassandra, elasticsearch, nginx (SSL proxy).
4. Po spuštění byla vytvořena organizace, první účty s rolemi admin a analyst.

Základní konfigurace

V rámci testování byly vytvořeny dvě šablony případů:

- **Neoprávněné přihlášení** (zdroj: alert z Wazuh),
- **Podezřelá síťová aktivita** (ručně nahlášeno).



Obrázek 7 Dashboard The Hive po úspěšném vytvoření testovacího incidentu

(zdroj: vlastní)

Integrace a omezení

Integrace s Wazuh zatím probíhá manuálně (alert → incident), automatizované napojení pomocí webhooku je připraveno k následující implementaci nástroje Shuffle.

Shrnutí a výsledky

TheHive a Cortex byly úspěšně nainstalovány a připraveny pro praktické využití při vyhodnocování bezpečnostních událostí. V aktuálním režimu umožňují jednoduše zaznamenávat podezřelé události (např. alerty z Wazuh), třídit je podle typu a závažnosti, přiřazovat ke zpracování konkrétním osobám a sledovat jejich vyřešení. Cortex rozšiřuje

možnosti o automatizovanou kontrolu domén, IP adres nebo hashů souborů, což urychluje analýzu.

Při testování se ukázalo, že nástroje umožňují reagovat na incidenty strukturovaně a opakovatelně, bez nutnosti řešit vše ad hoc. Systém je zároveň připraven k napojení na další zdroje alertů a úlohy automatizace. Tato část řešení odpovídá požadavkům normy ISO/IEC 27001 především v oblastech:

- **A.5.26** (detekce bezpečnostních událostí),
- **A.5.27** (řízení incidentů),
- **A.5.30** (učení se z událostí a zlepšování procesů).

9.5.5 Instalace a konfigurace systému pro automatizaci bezpečnostních procesů (Shuffle)

S přibývajícím počtem nástrojů roste i potřeba tyto komponenty vzájemně propojit a zautomatizovat opakující se úkoly. Právě pro tento účel byl zvolen nástroj Shuffle, který umožňuje vytvářet jednoduché i komplexní automatizační scénáře bez nutnosti složitého programování. Jedná se o open-source platformu typu SOAR (Security Orchestration, Automation and Response), jejímž cílem je zrychlit reakce na incidenty, minimalizovat manuální zásahy a zvýšit celkovou efektivitu bezpečnostních procesů.

Tabulka 20 Použité prostředí – Shuffle

Oblast	Požadavek	Stav
Serverová infrastruktura	Ubuntu Server 24.04.2 LTS (VM), 4 vCPU, 6 GB RAM, 60 GB SSD	✓ dostupné
Verze nástroje	Stabilní build Shuffle (2024, oficiální repozitář)	✓ aktuální
Instalační metoda	Docker Compose – monolitická architektura	✓ úspěšně nasazeno
Komunikační rozhraní	REST API, JSON, Webhooky	✓ funkční

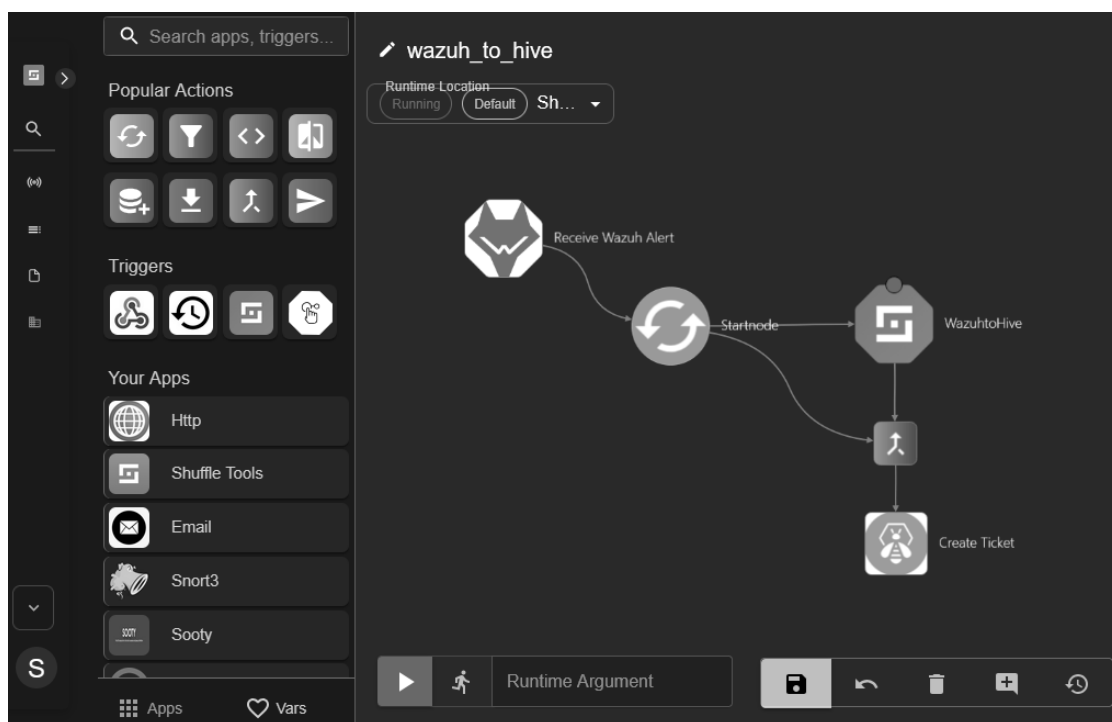
(zdroj: vlastní)

Postup instalace

1. Instalace byla provedena stažením repozitáře z <https://github.com/frikky/shuffle> a úpravou proměnných v docker-compose.yml.
2. Spuštěny byly kontejnery: shuffle-orchestrator, shuffle-ui, mongodb, nginx-proxy.
3. Po úspěšném startu byla inicializována admin instance a základní autentizace.

Základní konfigurace

1. Bylo vytvořeno několik testovacích workflow scénářů:
 - Wazuh alert → vytvoření případu v TheHive,
 - Nový případ v TheHive → odeslání notifikace e-mailem,
 - Příchozí alert → detekce podezřelé aktivity (modifikace registru ve Windows)
2. Propojeny byly následující systémy:
 - REST API instance TheHive (včetně autentizace tokenem),
 - Webhooky z Wazuh pro simulované alerty,



Obrázek 8 Při tvorbě workflow v Shuffle byly využity vizuální komponenty

(zdroj: vlastní)

Integrace a omezení

- Integrace s reálným provozem Wazuh zatím není plně automatizovaná – probíhá v testovacím režimu s kontrolovaným importem alertů.
- Nejsou zatím nasazeny pokročilé moduly (např. síťové blokace, aktivní zásahy na firewallu).
- Plánováno je propojení s interním ticketing systémem GLPI pro synchronizaci úkolů mezi analytiky a správci.

Shrnutí a výsledky

Shuffle byl nasazen jako lehká a flexibilní platforma pro automatizaci rutinních bezpečnostních činností. V rámci testování byly úspěšně vytvořeny jednoduché automatizační scénáře propojující nástroje Wazuh, TheHive a Cortex. Díky vizuálnímu editoru workflow je možné sestavit reakce na bezpečnostní události bez nutnosti hlubokých programovacích znalostí.

Během provozních zkoušek se potvrdilo, že nástroj výrazně zrychluje reakci na alerty – například tím, že při detekci události ve Wazuh může být automaticky založen případ v TheHive, nebo odeslán e-mail či notifikace správci.

V této fázi nasazení funguje Shuffle jako nástroj pro propojení jednotlivých komponent bezpečnostní architektury a vytváří předpoklady pro budoucí rozšíření o pokročilejší automatizační scénáře, např. zablokování IP adresy nebo synchronizaci s interními systémy podpory.

Z hlediska požadavků normy ISO/IEC 27001 tento nástroj přispívá zejména k:

- **A.5.25** (monitorování systémů),
- **A.5.27** (odezva na incidenty),
- **A.5.30** (kontinuální zlepšování na základě získaných dat a automatizace operací).

10 TESTOVÁNÍ FUNKČNOSTI NASAZENÝCH NÁSTROJŮ V PRODUKČNÍM PROSTŘEDÍ

Tato část navazuje na předchozí instalační kroky a slouží k ověření, zda nástroje v praxi plní očekávané funkce, a zda jsou schopny reagovat na reálné bezpečnostní události. Vzhledem k prostředí malé společnosti bylo testování provedeno přímo v produkci – za pečlivě kontrolovaných podmínek.

10.1 Cíl a přístup k testování

Cílem této části je ověřit, zda nasazené open-source nástroje skutečně plní požadované funkce v prostředí modelové organizace a zda efektivně podporují jednotlivé oblasti systému řízení informační bezpečnosti (ISMS), jak bylo navrženo v předchozích kapitolách a důraz byl kladen na praktické scénáře, které odpovídají běžnému provozu.

Testovací přístup byl zvolen tak, aby odrážel jak provozní realitu, tak klíčové požadavky normy ISO/IEC 27001, zejména v oblastech identifikace rizik, monitorování událostí, řízení incidentů a správy přístupů. Vzhledem k velikosti organizace a omezenému času na implementaci bylo upuštěno od budování samostatného testovacího prostředí. Místo toho byly nástroje zavedeny přímo do provozní infrastruktury v kontrolovaných fázích s možností jejich zpětné deaktivace či izolace.

Testování bylo zaměřeno na ověření:

- funkčnosti jednotlivých nástrojů dle očekávaných scénářů použití,
- kompatibility mezi nástroji a jejich schopnosti vzájemné integrace,
- odezvy systému na bezpečnostní události a efektivitu reakce,
- reálné provozní zátěže a dopadu na prostředí.

10.2 Testovací scénáře a průběh

Pro ověření funkčnosti a spolupráce jednotlivých nástrojů byly navrženy a realizovány čtyři testovací scénáře. Každý z nich simuluje konkrétní typ bezpečnostního incidentu nebo provozní situace, která má být systémem detekována a adekvátně zpracována.

10.2.1 Scénář 1: Neoprávněný pokus o přihlášení (test detekce Wazuh)

Cíl: Ověřit schopnost nástroje Wazuh detekovat podezřelé přihlášení a zaznamenat incident.

Postup: Na testovací Windows stanici byl několikrát za sebou zadán nesprávný přihlašovací údaj.

Výsledek: Wazuh vygeneroval alert o více po sobě jdoucích neúspěšných pokusech o přihlášení. Událost byla zobrazena v dashboardu a zaznamenána do logu.

Vyhodnocení: Detekce proběhla úspěšně, odpovídající pravidla Wazuh byly aktivní a správně reagovaly.

```

f data.win.system.message

"An account failed to log on.

Subject:
  Security ID:          S-1-5-18
  Account Name:         JK-PC1$
  Account Domain:       ECPR0D1
  Logon ID:             0x3E7

Logon Type:             2

Account For Which Logon Failed:
  Security ID:          S-1-0-0
  Account Name:         jank-testacc1
  Account Domain:       JK-PC1

Failure Information:
  Failure Reason:       Unknown user name or bad password.
  Status:               0xC000006D
  Sub Status:           0xC000006A

Process Information:
  Caller Process ID:    0x918
  Caller Process Name:  C:\Windows\System32\svchost.exe

Network Information:
  Workstation Name:     JK-PC1
  Source Network Address: 127.0.0.1
  Source Port:          0

Detailed Authentication Information:
  Logon Process:        User32
  Authentication Package: Negotiate
  Transited Services:   -
  Package Name (NTLM only): -
  Key Length:           0

```

Obrázek 9 Detekce neoprávněného pokusu o přihlášení zaznamenaná ve Wazuh

(zdroj: vlastní)

10.2.2 Scénář 2: Založení incidentu v TheHive na základě alertu

Cíl: Ověřit manuální převod detekované události do strukturovaného incidentu.

Postup: Alert z předchozího testu byl ručně zadán jako nový případ ve webovém rozhraní TheHive.

Výsledek: Byl vytvořen incident se všemi příslušnými metadaty, přiřazen k řešení konkrétní osobě, a byla připojena poznámka s popisem události.

Vyhodnocení: Vytvoření i správa případu proběhly bez problému. Bylo ověřeno, že workflow v TheHive odpovídá požadavkům na evidenci a řízení bezpečnostních incidentů.

The screenshot shows the 'Create case' form in TheHive. At the top is a dark header with a back arrow and the text 'Create case'. Below this are several sections:

- * Title:** A text input field containing 'Podezrele prihlaseni - JK-PC1'.
- * Date:** A date input field containing '2025-05-08'.
- Severity:** Four buttons: 'LOW', 'MEDIUM' (selected), 'HIGH', and 'CRITICAL'.
- TLP:** Five buttons: 'TLP:CLEAR', 'TLP:GREEN', 'TLP:AMBER' (selected), 'TLP:AMBER-STRICT', and 'TLP:RED'.
- PAP:** Four buttons: 'PAP:CLEAR', 'PAP:GREEN', 'PAP:AMBER' (selected), and 'PAP:RED'.
- Tags:** A horizontal list of tags, with 'failedlogin' and 'prodpc' visible.
- * Description:** A rich text editor area containing the text: 'Autentikace selhala 3x pred uspesnym prihlasenim k developerske stanici. Log nize: "An account failed to log on. Subject: Security ID: S-1-5-18'.

Obrázek 10 Vytvoření a klasifikace incidentu v The Hive

(zdroj: vlastní)

10.2.3 Scénář 3: Automatizované workflow mezi nástroji (Shuffle)

Cíl: Ověřit základní automatizaci reakce na alert a přenos dat mezi systémy.

Postup: Pomocí testovacího webhooku byl simulován alert o spuštění potenciálně škodlivého souboru, který spustil workflow v Shuffle. Pro potřeby testování byl použit soubor EICAR, který byl vyvinut Evropským institutem pro výzkum počítačových antivirů (EICAR) a Organizací pro výzkum počítačových antivirů (CARO) za účelem testování odezvy počítačových antivirových programů [56].

Výsledek: Workflow vytvořil nový incident v TheHive a odeslal e-mail správci systému.

Vyhodnocení: Automatizace proběhla úspěšně. Data byla správně přenesena mezi nástroji, jednotlivé kroky workflow byly zaznamenány a jejich výstupy dostupné.

10.2.4 Scénář 4: Falešně pozitivní alert a jeho uzavření

Cíl: Ověřit schopnost systému zpracovat nesprávně vyhodnocený alert a učit se z něj.

Postup: Na známém zařízení byl spuštěn skript, který způsobil bezpečnostní alert (změna konfiguračního souboru). Po kontrole byl incident označen jako falešně pozitivní.

Výsledek: Incident byl uzavřen v TheHive a systém byl doplněn o poznámku vysvětlující chování.

Vyhodnocení: Možnost reakce na falešné pozitivy je funkční. Správce má k dispozici auditní stopu i poznámky k incidentu.

Tyto scénáře ověřily základní schopnosti systému detekovat, zpracovat a dokumentovat bezpečnostní události v souladu s požadavky normy ISO/IEC 27001. Výsledky jednotlivých scénářů jsou dále vyhodnoceny v následující podkapitole.

10.3 Vyhodnocení výsledků testování

Testování nasazených nástrojů v reálném prostředí společnosti prokázalo, že navržený bezpečnostní rámec je funkční a v souladu s požadavky normy ISO/IEC 27001. Vybrané open-source nástroje byly schopny detekovat předem definované bezpečnostní události, umožnit jejich evidenci a následné zpracování, a v některých případech i automatizovaně reagovat.

Tabulka 21 Výsledky testování jednotlivých nástrojů

Testovaný prvek	Výsledek	Poznámka
Detekce incidentu (Wazuh)	Úspěšná detekce nepovedeného pokusu o přihlášení	Detekce proběhla téměř okamžitě, záznam v logu, vizualizace v Kibana
Evidence incidentu (TheHive)	Incident zaznamenán, úkol přiřazen	Přehledný formulář, možnost sledovat stav i historii a přiřadit dílčí úkoly analytikovi.
Automatizace (Shuffle)	Workflow aktivní, alert předán do TheHive a malware analyzován v virustotal	Notifikace odeslána správně, vizuální přehled v rozhraní
Vyhodnocení falešného alertu	Incident uzavřen s poznámkou	Podpora manuální klasifikace a zpětné vazby

(zdroj: vlastní)

Systém umožňuje komplexní pohled na bezpečnostní události: od detekce přes analýzu až po řízené řešení. V praxi to znamená, že jakýkoli významný incident v infrastruktuře společnosti bude zachycen, zdokumentován a jeho řešení dohledatelné.

10.4 Přínos pro ISMS

Z výsledků testování vyplývá, že:

- monitorovací nástroj Wazuh plně pokrývá základní požadavky na detekci hrozeb (kapitoly A.5.25–27),
- TheHive umožňuje vést evidenci incidentů v souladu s požadavky na řízený přístup k událostem (A.5.27, A.5.30),
- Shuffle umožňuje propojit jednotlivé nástroje do jednoho funkčního řetězce a vytvářet procesy typu „alert → reakce → dokumentace“.

Celkově lze konstatovat, že řešení je použitelné a škálovatelné. Z pohledu malé společnosti přináší výrazné zvýšení přehledu o bezpečnostní situaci a vytváří základ pro systematický rozvoj ISMS.

11 ZÁVĚREČNÁ DOPORUČENÍ

V závěrečné fázi implementace systému řízení informační bezpečnosti (ISMS) je nezbytné nejen vyhodnotit technickou funkčnost nasazených řešení, ale rovněž formulovat konkrétní doporučení pro jejich efektivní každodenní využívání. Vzhledem k tomu, že práce byla zaměřena na potřeby malých firem, které zpravidla disponují omezenými personálními i finančními kapacitami, byla navržená architektura postavena na otevřených nástrojích s důrazem na jednoduchost, škálovatelnost a přímou využitelnost v reálném provozu.

Následující doporučení reflektují praktické zkušenosti z implementace, výsledky testování a rovněž osvědčené přístupy z odborných zdrojů a komunitní praxe. Jejich cílem je poskytnout rámec pro dlouhodobě udržitelné řízení bezpečnosti v malých a středních podnicích (MSP), které nemusí disponovat vyspělým bezpečnostním aparátem, ale přesto čelí obdobným hrozbám jako větší organizace.

11.1 Stanovení odpovědnosti a udržitelnosti ISMS v prostředí malé organizace

Jedním z nejdůležitějších faktorů dlouhodobě udržitelného ISMS je jasně definovaná odpovědnost za jeho správu. Ve velkých organizacích tuto roli většinou často zastává samostatné oddělení, ale malé společnosti mají typicky omezené personální kapacity. Z toho důvodu může spadat správa bezpečnostních nástrojů a dohled nad plněním bezpečnostních politik pod širší agendu IT oddělení nebo být dokonce pouze doplňkovou činností vedoucího vývoje.

Z praktického hlediska je potřeba formálně určit roli, která bude v organizaci zodpovědná za dohled nad bezpečností – například v podobě interního bezpečnostního koordinátora. Tato pozice nemusí být vázána na konkrétního pracovníka, ale důležité je, aby byly jasně stanoveny kompetence a zodpovědnosti. Do náplně práce této osoby potom spadá jak technická správa nástrojů (např. pravidelné aktualizace, kontrola přístupových oprávnění, analýza alertů), tak i dohled nad tím, jestli jsou nastavené procesy v organizaci skutečně dodržovány.

S ohledem na zkušenosti při implementaci můžeme doporučit, aby role koordinátora bezpečnosti podléhala pravidelné revizi, např. jednou za čtvrtletí. Vedení organizace by zároveň mělo zajišťovat základní metodickou a časovou podporu pro výkon této role. Tím by mělo být zajištěno, že nástroje implementované v rámci ISMS budou provozovány bez

problémů a efektivně využívány a rozvíjeny tak, aby splňovaly aktuálními potřeby společnosti.

11.2 Údržba, aktualizace a správa bezpečnostní infrastruktury

Technické nástroje implementované v rámci ISMS podléhají častým aktualizacím, změnám konfigurace i měnícímu se prostředí. Tam kde chybí specializovaný tým, je důležité, aby procesy administrace a údržby byly nastaveny co nejjednodušeji, ale zároveň spolehlivě. Praxe ukazuje, že právě nedostatek systematické údržby může být nejčastějším důvodem postupného snižování účinnosti a spolehlivosti celého řešení.

Pro všechny klíčové komponenty – od Wazuh po TheHive či Snap-IT doporučujeme zavést pravidelný plán, který bude obsahovat kontrolu aktualizací, ověření integrity dat a zálohování konfigurací. Každou aktualizaci je vhodné naplánovat ideálně v měsíčních intervalech. Vzhledem k použití open-source nástrojů je výhodou možnost přímého sledování vývoje v oficiálních repozitářích, případně na komunitních diskuzních fórech, kde máme možnost předem identifikovat případná rizika související s přechodem na novou verzi, nebo nové zranitelnosti, kterým tyto systémy mohou podléhat.

Pozornost musí být věnována také dokumentaci všech změn. Přehledná evidence zásahů, změn v konfiguraci a účelu těchto kroků pomáhá k transparentnosti systému a usnadňuje jak případné auditování činnosti, tak i školení nových zaměstnanců, kteří se budou na správě ISMS podílet. V malé firmě je navíc výhodou, pokud je tato dokumentace co nejvíce integrovaná s každodenními procesy, např. přímo v prostředí helpdesku či sdíleného interního wiki systému.

11.3 Integrace nástrojů do každodenního provozu organizace

Nasazení technických řešení samo o sobě nezaručí vyšší úroveň bezpečnosti, pokud je dostatečně nepropojíme s běžnými pracovními procesy. Bezpečnostní nástroje musí být maximálně funkční, ale zároveň nesmí zbytečně zatěžovat zaměstnance nebo narušovat běžný provoz.

V oblasti správy aktiv a přístupů je vhodné propojit evidenci na stávající procesy a např. začlenit správu zařízení a uživatelů do při nástupu zaměstnanců do společnosti a stejně tak i v případě, že zaměstnanec firmu opouští.

V oblasti detekování hrozeb a reagování na incidenty by měly být výstupy z monitorovacích nástrojů snadno pochopitelné a rychle dostupné. Pokud nebudou dashboardy v nástrojích typu Wazuh nebo alerty zasílané e-mailem či notifikací přehledné, může docházet k tomu, že jim nebude věnována dostatečná pozornost, nebo budou v horším případě ignorovány. Zapojením nástroje pro automatizaci jako je Shuffle umožňuje automatizovat přijetí alertu, vytvoření případu v TheHive a jeho následné vyhodnocení čímž se při správném nastavení snižuje manuální zátěž, respektive klesají nároky na pracovní sílu a současně roste rychlost reakce.

Zaměstnanci musí také vědět, proč dané nástroje používají a jak tím přispívají k ochraně společnosti, jinak hrozí, že se ISMS stane pouhým souborem pravidel a ne přirozenou součástí firemního provozu.

11.4 Školení zaměstnanců a rozvoj bezpečnostního povědomí (Security Awareness)

I v prostředí, kde zaměstnanci mají vyšší úroveň IT gramotnosti, zůstává lidský faktor jedním z největších bezpečnostních rizik. Nemusí jít jen o úmyslné zneužití. V častých případech jsou příčinou incidentů nevědomost, nepozornost nebo podcenění rizik za účelem zjednodušení, nebo rychlejšího řešení technických či jiných problému a překážek. Budování základního bezpečnostního povědomí mezi pracovníky by proto mělo být vnímáno jako jeden z klíčových prvků efektivního ISMS.

Zavedení technických nástrojů by měla provázet transparentní komunikace ohledně jejich významu a ohledně pravidel jejich používání. V může docházet k tomu, že zaměstnanci se začnou těmto nástrojům vyhýbat, budou ignorovat bezpečnostní postupy a nebo je dokonce obcházet.

Školení u menšího kolektivu mohou být i ve formě krátkých workshopů nebo prezentací a e-mailových newsletterů se zaměřením na praktické scénáře, se kterými se zaměstnanci reálně setkávají. To mohou být např. phishingové e-maily, bezpečné zacházení s repozitáři kódu, secure coding best practices nebo proaktivní hlášení podezřelých událostí a znalost postupu jak takové události hlásit.

11.5 Provozní náklady, rozšiřitelnost a další rozvoj systému

Použité nástroje většinou nevyžadují placené licence ani specializovaný hardware a i u některých komerčních řešení založených na open-source je často k dispozici komunitní verze s určitými omezeními. Náklady tak mohou zůstat nízké. Přesto je dobré počítat s časem, který je nutný pro základní správu, aktualizace a případné úpravy konfigurace. Pokud je prostředí dobře nastavené od začátku, provozní režie zůstává minimální.

System je navržen tak, aby šel bez větších zásahů rozšířit (či naopak konsolidovat). Pokud bude potřeba přidat další uživatele, zařízení nebo nástroje, není nutné nic zásadního měnit. Nasazené systémy umožňují škálování v rámci stávající infrastruktury nebo přechod do cloudu.

Všechny nástroje, které byly nasazené, mají aktivní komunitu a pravidelně vycházejí nové verze u kterých se často setkáváme nejen s opravami chyb, ale i s novými funkcemi, které mohou zlepšit přehled o dění v síti, zjednodušit správu nebo posílit detekční schopnosti. Doporučuje se pravidelně kontrolovat vývoj jednotlivých projektů, sledovat oznámení o aktualizacích a zvažovat, zda některé novinky mohou být přínosné i pro dané prostředí.

12 ZÁVĚR

Cílem této práce bylo navrhnout a prakticky implementovat sadu open-source nástrojů, které pokrývají klíčové oblasti systému řízení informační bezpečnosti (ISMS) dle normy ISO/IEC 27001, a to v podmínkách menší společnosti zabývající se vývojem software, ve které nebyla pokročilejší bezpečnostní infrastruktura. Při návrhu byl kladen důraz na udržení nízkých provozních nákladů, přehlednost řešení, snadnou údržbu a automatizaci.

Výsledné bezpečnostní řešení sestavené z nástrojů jako Wazuh, Snipe-IT, Keycloak, TheHive a Shuffle umožňuje firmě nejen lépe sledovat a řídit svá aktiva, ale také efektivněji detekovat bezpečnostní události a incidenty, reagovat na ně řídit rizika. V praxi se při implementaci osvědčila především dvojice Wazuh a TheHive jakožto jádra bezpečnostního monitoringu a incident response, zatímco Keycloak přinesl firmě možnost jednotné správy identit a bezpečného přístupu k interním systémům.

Zvolený přístup se ukázal jako dobře realizovatelný v malém technicky zaměřeném prostředí. Díky tomu, že jsou použité nástroje modulární, bylo možné systém snadno přizpůsobit konkrétním potřebám a provozním omezením. Společnosti tak vznikl základ pro další rozvoj bezpečnostních procesů i bez nutnosti významnějších investic do komerčních řešení.

Z pohledu další optimalizace by se firma mohla v budoucnu zaměřit například na konsolidaci služeb a infrastruktury, což by dále snížilo provozní nároky. V oblasti detekce hrozeb se nabízí soustředit se na detection engineering, tedy další tvorbu a ladění vlastních detekčních pravidel na základě konkrétního provozu, změn v infrastruktuře a nově vznikajících rizik. Práce na této oblasti pomůže výrazně zvýšit schopnost systému zachytit méně zjevné typy útoků nebo interní chyby a zefektivnit detekce vyloučením falešně pozitivních alertů.

Práce potvrdila, že i bez větších investic je možné vytvořit funkční bezpečnostní rámec ISMS, který odpovídá klíčovým požadavkům mezinárodní normy. Klíčovým faktorem úspěchu přitom nebyla jen volba nástrojů, ale také jejich správná integrace a pochopení provozního kontextu, ve kterém budou fungovat.

SEZNAM POUŽITÉ LITERATURY

- [1] Check Point Software Technologies. Elektronických útoků na české společnosti přibylo, ukazují data kyberbezpečnostní skupiny Check Point [online]. 2024. Dostupné z: <https://archiv.hn.cz/c1-67347780-elektronickych-utoku-na-ceske-spolecnosti-pribylo-ukazuji-data-kyberbezpecnostni-skupiny-check-point>
- [2] CrowdStrike. What is Zero Trust? - Guide to Zero Trust Security. [online]. 2025-03-13 Dostupné z: <https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/>
- [3] HOLLOWAY, A. Cybersecurity in Nuclear Facilities [online]. Stanford University, 2015 Dostupné z: <http://large.stanford.edu/courses/2015/ph241/holloway2/>
- [4] DEATH, Darren. Information Security Handbook: Develop a Threat Model and Incident Response Strategy to Build a Strong Information Security Framework. Birmingham: Packt Publishing, 2017. ISBN 978-1788478830.
- [5] MICROSOFT. Co je umělá inteligence pro kybernetickou bezpečnost? [online]. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-ai-for-cybersecurity>
- [6] Cloud Security Alliance. SaaS Challenges, Solutions, and Best Practices for 2024. [online]. 2024-09-12 Dostupné z: <https://cloudsecurityalliance.org/blog/2024/09/12/7-essential-saas-security-best-practices>
- [7] Overt Software Solutions. ISO 27001:2022 vs 2013 – What’s New and Why It Matters. [online]. Dostupné z: <https://www.overtsoftware.com/iso-27001-2022-vs-2013-whats-new-and-why-it-matters/>
- [8] CALDER, Alan. ISO 27001/ISO 27002: A Complete Guide to the Information Security Management System. 8th ed. IT Governance Publishing, 2023. ISBN 978-1787783799.
- [9] ASQ. Plan-Do-Check-Act Cycle. [online]. Available at: <https://asq.org/quality-resources/pdca-cycle>
- [10] ESECURE360. ISO 27001 Certification [online]. [cit. 2025-06-01]. Dostupné z: <https://esecure360.com/iso-27001-certification/>
- [11] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2022.

- [12] BAARS, Hans, HINTZBERGEN, Jacco a HINTZBERGEN, Kees. Foundations of Information Security based on ISO27001 and ISO27002. 4th revised ed. Zaltbommel: Van Haren Publishing, 2023. ISBN 978-9401809589.
- [13] COBALT. Risks of Open-Source Software: How to Protect Your Code. [online]. 2023. Dostupné z: <https://www.cobalt.io/blog/risks-of-open-source-software>
- [14] BAIRESDEV. The Pros and Cons of Open-Source Software: A Guide for Developers and Executives. [online]. 2023. Dostupné z: <https://www.bairesdev.com/blog/the-pros-and-cons-of-open-source-software-a-guide-for-developers-and-executives/>
- [15] GERBER, Scott. 12 challenges businesses face when using open-source software. [online]. 2019 [cit. 2025-06-01]. Dostupné z: <https://thenextweb.com/news/12-challenges-businesses-face-when-using-open-source-software>
- [16] VEGA, Jose. awesome-siem [online]. GitHub, 2024. Dostupné z: <https://github.com/jvega/awesome-siem>
- [17] GITHUB, Inc. GitHub – open-source repositories for security tools [online]. GitHub, 2024. Dostupné z: <https://github.com/topics/security-tools>
- [18] CALDER, Alan. Nine Steps to Success: An ISO 27001:2022 Implementation Overview. Ely: IT Governance Publishing, 2024. ISBN 978-1-78778-541-0.

SEZNAM OBRÁZKŮ

Obrázek 1 Schéma modelu PDCA [10]	21
Obrázek 2 Časový harmonogram implementace	61
Obrázek 3 Výchozí dashboard instance EC-INVENTORY po inicializaci Snipe-IT	65
Obrázek 4 Náhled CSV souboru pro import aktiv.....	65
Obrázek 5 Výchozí stránka admin rozhraní instance Keycloak po úspěšné instalaci	66
Obrázek 6 Dashboard s detaily o monitorované pracovní stanici “JK-PC1”	69
Obrázek 7 Dashboard The Hive po úspěšném vytvoření testovacího incidentu	71
Obrázek 8 Při tvorbě workflow v Shuffle byly využity vizuální komponenty.....	73
Obrázek 9 Detekce neoprávněného pokusu o přihlášení zaznamenaná ve Wazuh	76
Obrázek 10 Vytvoření a klasifikace incidentu v The Hive.....	77

SEZNAM TABULEK

Tabulka 1 Nástroje pro identifikaci rizik a zranitelností.....	43
Tabulka 2 Porovnání nástrojů pro identifikaci rizik a zranitelností.....	44
Tabulka 3 Nástroje pro správu aktiv	45
Tabulka 4 Porovnání nástrojů pro správu aktiv	45
Tabulka 5 Nástroje pro řízení přístupů a identit	47
Tabulka 6 Porovnání nástrojů pro řízení přístupů a identit.....	48
Tabulka 7 Nástroje pro monitorování a detekci hrozeb.....	49
Tabulka 8 Porovnání nástrojů pro monitorování a detekci hrozeb	50
Tabulka 9 Nástroje pro správu incidentů	51
Tabulka 10 Porovnání nástrojů pro správu incidentů	51
Tabulka 11 Nástroje pro automatizaci bezpečnostních procesů	52
Tabulka 12 Porovnání nástrojů pro automatizaci bezpečnostních procesů	53
Tabulka 13 Vybrané nástroje pro implementaci a jejich vta h ke kontrolám ISO/IEC 27001:2022	54
Tabulka 14 Technické požadavky na provozní prostředí před nasazením řešení.....	58
Tabulka 15 Organizační požadavky na provozní prostředí před nasazením řešení.....	58
Tabulka 16 Seznam jednotlivých úkolů a časový plán implementace.....	59
Tabulka 17 Použité prostředí – Snipe-IT	64
Tabulka 18 Použité prostředí - Wazuh.....	67
Tabulka 19 Použité prostředí – The Hive	70
Tabulka 20 Použité prostředí – Shuffle.....	72
Tabulka 21 Výsledky testování jednotlivých nástrojů.....	78

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
API	Application Programming Interface
APT	Advanced Persistent Threat
AV	Antivirus
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
EDR	Endpoint Detection and Response
ESM	Enterprise Security Management
GDPR	General Data Protection Regulation
GLPI	Gestionnaire Libre de Parc Informatique
GPO	Group Policy Object
GRC	Governance, Risk and Compliance
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
LDAP	Lightweight Directory Access Protocol
MITM	Man In The Middle
MSP	Managed Service Provider
NIST	National Institute of Standards and Technology
OCS	Open Computer and Software Inventory
OS	Operating System
OTP	One Time Password
PDCA	Plan–Do–Check–Act
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOP	Standard Operating Procedure
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSH	Secure Shell
SNI	Server Name Indication

TTP	Tactics, Techniques and Procedures
URL	Uniform Resource Locator
VPN	Virtual Private Network

