

Zabezpečení a monitoring rozsáhlých IT infrastruktur

Bc. Jan Kincl

Diplomová práce
2022



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Bc. Jan Kindl
Osobní číslo: A20890
Studijní program: N0613A140022 Informační technologie
Specializace: Kybernetická bezpečnost
Forma studia: Kombinovaná
Téma práce: Zabezpečení a monitoring rozsáhlých IT infrastruktur
Téma práce anglicky: Security and Monitoring of Large IT Infrastructures

Zásady pro vypracování

1. Specifikujte moderní možnosti monitoringu rozsáhlých sítí.
2. Identifikujte kritické prvky chráněné infrastruktury a definujte závažnost výpadků těchto prvků.
3. Navrhněte systém pro provozní i bezpečnostní monitoring sítě s využitím moderních technologií.
4. Proveďte implementaci řešení v testovací infrastruktuře.
5. Ověřte možnosti detekce Vaší imlementace proti běžným cyberútokům a provozním výpadkům.

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

Seznam doporučené literatury:

1. TRAORÉ, Issa, Ahmed AWAD a Isaac WOUNGANG. *Information security practices: emerging threats and perspectives*. Cham, Switzerland: Springer, [2017], 1 online resource. Dostupné z: doi:9783319489476
2. STALLINGS, William a Lawrie BROWN. *Computer security: principles and practice*. Fourth edition. Chennai: Pearson, [2020], 800 atrn. ISBN 978-93-534-3886-9
3. PETRUTI, C.-M., B.-A. PUIU, I.-A. IVANCIU a V. DOBROTA. *Proceedings – 17th RoEduNet IEEE International Conference: Networking in Education and Research, RoEduNet 2018*. 2018. ISBN 9781538671351. Dostupné z: doi:10.1109/ROEDUNET.2018.8514142
4. VAZAO, Ana, Leonel SANTOS, Maria Beatriz PIEDADE a Carlos RABADAO. *SIEM Open Source Solutions: A Comparative Study*. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Information Systems and Technologies (CISTI), 2019 14th Iberian Conference on* [online]. 2019, , 1-5 [cit. 2021-11-30]. ISBN 9789899843493. ISSN edsee.IEEEConferenc. Dostupné z: doi:10.23919/CISTI.2019.8760980
5. UNAL, Ugur, Ceyda Nur KAHYA, Yaprak KURLUTEPE a Hasan DAG. *Investigation of Cyber Situation Awareness via SIEM tools: a constructive review*. *2021 6th International Conference on Computer Science and Engineering (UBMK), Computer Science and Engineering (UBMK), 2021 6th International Conference on* [online]. 2021, , 676-681 [cit. 2021-11-30]. ISBN 9781665429078. ISSN 25211641. Dostupné z: doi:10.1109/UBMK52708.2021.9558964
6. CAKMAKCI, Salva Daneshgadeh, Helmar HUTSCHENREUTER, Christian MAEDER a Thomas KEMMERICH. *A Framework For Intelligent DDoS Attack Detection and Response using SIEM and Ontology*. *2021 IEEE International Conference on Communications Workshops (ICC Workshops), Communications Workshops (ICC Workshops), 2021 IEEE International Conference on* [online]. 2021, , 1-6 [cit. 2021-11-30]. ISBN 9781728194417. ISSN 26942941. Dostupné z: doi:10.1109/ICCWorkshops50388.2021.9473869
7. SERCKUMECKA, Adriano, Iberia MEDEIROS a Alysso BESSANI. *Low-Cost Serverless SIEM in the Cloud*. *2019 38th Symposium on Reliable Distributed Systems (SRDS), Reliable Distributed Systems (SRDS), 2019 38th Symposium on, SRDS* [online]. 2019, , 381-3811 [cit. 2021-11-30]. ISBN 9781728142227. ISSN 25758462. Dostupné z: doi:10.1109/SRDS47363.2019.00057

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2021**

Termín odevzdání diplomové práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan



prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 24. ledna 2022

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne

Jan Kincl, v. r.

ABSTRAKT

Vzhledem k neustálému rozvoji a stále výraznější integraci výpočetní techniky do většiny pracovních prostředí a procesů, jsme v současnosti svědky vzniku stále rozsáhlejších a složitějších IT infrastruktur. V takové infrastruktuře se „setkávají“ zařízení na bázi různých operačních systémů, různého určení a celkově odlišné povahy. Spojení vzrůstající popularity výpočetní techniky a její vzájemné integrace, přináší stále častěji potřebu řešit problematiku zabezpečení infrastruktur. Obecně lze říct, že infrastruktura by měla být zabezpečena proti provozním výpadkům a splňovat požadavky kybernetické bezpečnosti. Limitací takového požadavku je velmi často lidský faktor. Konkrétněji nejen z hlediska chování samotných uživatelů, ale často z důvodu limitace samotného systémového administrátora, případně správcovského týmu. Zjednodušeně pro takový tým není možné, bez využití vhodných nástrojů, udržet přehled o rozsáhlé infrastruktuře a zároveň udržet krátký reakční čas na nově vzniklé problémy.

Z těchto důvodů práce popisuje implementaci monitorovací platformy Zabbix, definuje možné scénáře jejího použití pro monitoring prvků infrastruktury a navržené řešení doplňuje o implementaci systému OSSIM AlienVault. To vše jsou prvky, kterých je možné využít při procesu zabezpečování a správě infrastruktury. Nejen, že vedou k zvednutí úrovně kybernetické bezpečnosti v infrastruktuře, ale také podporují efektivní činnost správcovského týmu.

V neposlední řadě práce také rozšiřuje pole působnosti výzkumné laboratoře PTLAB. Ta se zabývá kybernetickou bezpečností v oblasti kybernetických a síťových hrozeb, ale primárně neřeší problematiku monitorování a správy infrastruktur, nebo jejich návrhu.

Klíčová slova: Kybernetická bezpečnost, informační technologie, monitoring, SIEM, OSSIM, Zabbix, IT infrastruktura, AlienVault, sběr dat, správa infrastruktur.

ABSTRACT

Due to the constant expansion of computer technology and more pronounced integration into most work environments and processes, we experience an emergence of increasingly complex IT infrastructures. In these infrastructures many various devices are operated together. Such devices vary in terms of their operating system, role in the infrastructure and type in general. The combination of the growing number of distinct devices and their congregation into IT infrastructures leads to an increased importance of the need to address infrastructure security. In general, every infrastructure should be resistant to equipment failure and meet the cybersecurity requirements. Very often, the human factor is a limitation for those demands. Not only because of the user behaviour, but often due to the limitations of the system administrator or the administration team. Simply put, for such team, without the use of appropriate tools, it is not possible to maintain overview of managed infrastructure and achieve short reaction time for emerging problems.

Therefore, this thesis describes the implementation of Zabbix monitoring platform, defines scenarios of its possible use for monitoring infrastructure elements and complements the platform by adding OSSIM AlienVault system to the overall solution. These are all elements that can be used in the process of securing and overseeing the infrastructure. Not only do they lead to an increase in the level of cyber security, but they also support the effective operation of IT administration teams.

Last but not least, thesis also expands the scope of the PTLAB research laboratory. Laboratory deals with cyber security in cyber and network threats but does not primarily address the issue of infrastructure monitoring and management or infrastructure design.

Keywords: Cyber Security, Information technology, monitoring, SIEM, OSSIM, Zabbix, IT infrastructure, AlienVault, data gathering, infrastructure management.

Děkuji Ing. Davidu Malaníkovi, Ph.D. za podporu, otevřený přístup, projevenou důvěru a rady při společné práci v laboratoři a při tvorbě diplomové práce. Děkuji kolegům z fakulty, ústavu a laboratoře za inspiraci a podnětné a četné konzultace při řešení problémů. Mým přátelům pak za důležitou podporu a energii, kterou mi poskytují. Mé rodině rovněž děkuji za projevenou trpělivost během nesčetných zkouškových období, probdělých nocí a za cennou podporu při studiu.

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

OBSAH

ÚVOD	10
TEORETICKÁ ČÁST	13
1 IT INFRASTRUKTURA	14
1.1 MOŽNOSTI ČLENĚNÍ INFRASTRUKTUR	15
1.1.1 DĚLENÍ INFRASTRUKTURY NA ZÁKLADĚ CHARAKTERU ZAŘÍZENÍ	16
1.1.2 NÁVRH MOŽNOSTI KLASIFIKACE INFRASTRUKTURY	17
1.2 PROCES TVORBY ZABEZPEČENÉ INFRASTRUKTURY	22
1.2.1 BEZPEČNOSTNÍ SITUACE PRO IT INFRASTRUKTURY	22
1.2.2 AKTUÁLNÍ ÚTOKY A HROZBY PRO INFRASTRUKTURY	24
1.2.3 DOPORUČENÝ POSTUP ZABEZPEČOVÁNÍ INFRASTRUKTURY	28
2 MONITOROVÁNÍ INFRASTRUKTUR	31
2.1 CHARAKTER ZÍSKANÝCH DAT	32
2.1.1 PROVOZNÍ DATA	32
2.1.2 BEZPEČNOSTNÍ DATA	33
2.1.3 SÍŤOVÝ PROVOZ	33
2.2 POŽADAVKY PŘI NÁVRHU MONITOROVACÍHO SYSTÉMU	34
2.3 PŘÍNOSY MONITOROVACÍHO SYSTÉMU	36
3 PŘEHLED MONITOROVACÍCH SYSTÉMŮ	37
3.1 POPIS VYBRANÝCH ŘEŠENÍ	38
3.2 SROVNÁNÍ VYBRANÝCH ŘEŠENÍ	42
PRAKTICKÁ ČÁST	43
4 POPIS ŘEŠENÉ INFRASTRUKTURY	44
4.1 OBECNÉ VLASTNOSTI A ROZDĚLENÍ ŘEŠENÉ INFRASTRUKTURY	44
4.1.1 TOPOLOGICKÉ ROZDĚLENÍ INFRASTRUKTURY	44
4.1.2 POPIS ŘEŠENÉ INFRASTRUKTURY NA ZÁKLADĚ HW VLASTNOSTÍ ZAŘÍZENÍ	45
4.1.3 POPIS ŘEŠENÉ INFRASTRUKTURY NA ZÁKLADĚ SW VLASTNOSTÍ ZAŘÍZENÍ.....	47
4.1.4 POPIS ŘEŠENÉ INFRASTRUKTURY NA ZÁKLADĚ JEJICH UŽIVATELŮ	49
4.2 SÍŤOVÁ STRUKTURA ŘEŠENÉ INFRASTRUKTURY	50
4.3 LOGICKÁ SÍŤOVÁ STRUKTURA ŘEŠENÉ INFRASTRUKTURY	53
4.4 IDENTIFIKACE KRITICKÝCH PRVKŮ ŘEŠENÉ INFRASTRUKTURY	54
4.4.1 PRVEK KRITICKÝ PRO PROVOZ INFRASTRUKTURY	54
4.4.2 PRVKY EKONOMICKY VÝZNAMNÉ PRO INFRASTRUKTURU	59
4.4.3 PRVKY INFORMAČNĚ VÝZNAMNÉ PRO INFRASTRUKTURU	61
4.4.4 VÝZNAMNÁ ZAŘÍZENÍ INFRASTRUKTURY	62
5 NÁVRH IMPLEMENTACE MONITOROVACÍHO SYSTÉMU	64
5.1 POŽADAVKY NA NAVRHOVANÝ MONITOROVACÍ SYSTÉM	64
5.2 VOLBA ŘEŠENÍ PRO IMPLEMENTACI	65
5.3 MOŽNOSTI INTEGRACE SYSTÉMU ZABBIX PRO ŘEŠENOU	

INFRASTRUKTURU	67
5.4 INSTALACE SYSTÉMU ZABBIX V TESTOVACÍ INFRASTRUKTUŘE	73
5.4.1 ZPŮSOBY INSTALACE.....	73
5.4.2 INSTALACE ZABBIX SERVERU A JEHO KOMPONENT	75
5.4.3 INSTALACE ZABBIX PROXY A JEJÍCH KOMPONENT.....	81
5.4.4 REGISTRACE PROXY V SYSTÉMU ZABBIX	83
6 SCÉNÁŘE POUŽITÍ MONITOROVACÍHO SYSTÉMU ZABBIX.....	85
6.1 MOŽNOSTI VYUŽITÍ ZABBIX AGENTA PRO MONITORING	
ZAŘÍZENÍ	85
6.1.1 INSTALACE AGENTA NA SLEDOVANÉ ZAŘÍZENÍ	85
6.1.2 REGISTRACE MONITOROVANÉHO ZAŘÍZENÍ V SYSTÉMU ZABBIX	89
6.2 ZÍSKÁVÁNÍ DAT ZE SLEDOVANÝCH ZAŘÍZENÍ.....	91
6.2.1 VYUŽITÍ A TVORBA TEMPLATES V SYSTÉMU ZABBIX.....	94
6.2.2 TVORBA DYNAMICKÝCH PRAVIDEL PRO ZÍSKÁNÍ DAT	95
6.2.3 ZPRACOVÁNÍ LOGŮ POMOCÍ SYSTÉMU ZABBIX.....	101
6.3 MONITORING ZAŘÍZENÍ NEPODPORUJÍCÍCH ZABBIX AGENT.....	102
6.3.1 DALŠÍ VYUŽITÍ MONITOROVACÍHO SYSTÉMU.....	104
6.4 GRAFICKÉ VIZUALIZACE V SYSTÉMU ZABBIX.....	105
7 MOŽNOSTI DETEKCE PROVOZNÍCH VÝPADKŮ	
A KYBERNETICKÝCH ÚTOKŮ.....	108
7.1 VYHODNOCOVÁNÍ PROVOZNÍCH VÝPADKŮ	109
7.2 IDENTIFIKACE BEZPEČNOSTNÍCH INCIDENTŮ	112
7.3 ROZŠÍŘENÍ MOŽNÉ IMPLEMENTACE S VYUŽITÍM OSSIM	
ALIENVault	114
ZÁVĚR	117
SEZNAM POUŽITÉ LITERATURY.....	119
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	126
SEZNAM OBRÁZKŮ	128
SEZNAM TABULEK.....	131
SEZNAM PŘÍLOH.....	132

ÚVOD

V současné době můžeme pozorovat stále intenzivnější expanzi a vznik různých síťových infrastruktur.

Vznikající infrastruktury jsou pak rozsáhlé nejen počtem zařízení, ale i jejich typem. V rámci infrastruktur se společně provozují zařízení, založená na různých operačních systémech, využívána pro jiný účel a vyžadující odlišný přístup při jejich správě a zabezpečení. Také je velmi běžné dělení infrastruktur z geografického hlediska. Scénář, kdy je infrastruktura dělena do více míst, ať už v rámci města, států, nebo globálního měřítka, je v dnešní době naprosto běžný.

Současně s problematikou tvorby IT infrastruktur je nutné řešit otázku jejich provozu a zabezpečení. Bohužel už několik let staré predikce [1] hovoří o stále se zhoršující bezpečnostní situaci a zvyšujícím se riziku převážně pro malé a střední podniky.

Současný pohled na problematiku zabezpečení tuto situaci pouze potvrzuje. Bezpečnostní situace v rámci kybernetického prostoru se neustále zhoršuje a pomyslný „průmysl“ kybernetické kriminality je dlouhodobě označován jako jedno z nejrychleji rostoucích odvětví. Roční ztráty způsobené kybernetickou kriminalitou se pro rok 2021 odhadovaly na cca. US\$ 6 bilionů a předpokládá se, že v roce 2025 by roční ztráty měly dosáhnout takřka dvojnásobku této hodnoty [2].

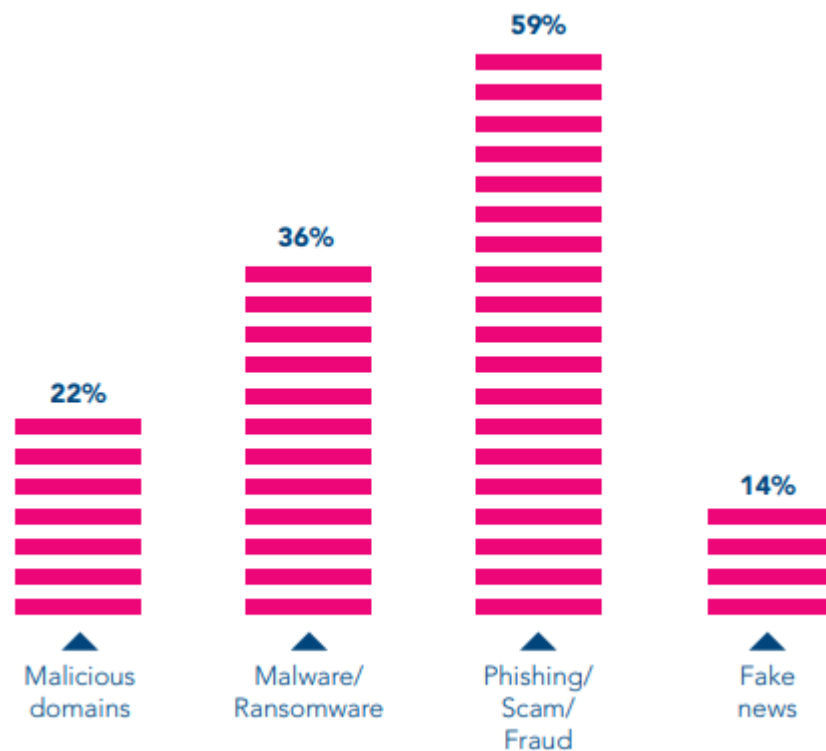
I další zdroje, jako například report [3] firmy SonicWall, Inc. potvrzují tento trend. Rok 2021 je v porovnání s předchozími roky opět označen jako zhoršení bezpečnostní situace. Jmenovitě dochází například k 105% nárůstu v počtu útoků typu ransomware. Cílem kybernetických útoků stále častěji nejsou pouze soukromé prvky, ale také prvky kritické infrastruktury, státní správy, vzdělávací instituce, informační systémy [4], např.:

- Květen 2021 - Napadení ropovodního systému Colonial Pipeline v USA [5] – útok typu ransomware
- Březen 2020 – Napadení FN Brno v České republice [6]

Dalším z problémů, na které report upozorňuje je vznik tisíců nových exploitů – z aktuálních opět například prosinec 2021 – zranitelnost Apache Log4j.

Problém ale nespočívá pouze ve výše zmiňovaných útocích specializovaného charakteru. Stále aktuální jsou útoky prostřednictvím phishingových emailů. Bezpečnostní analytici odhadují, že podvodné emaily a s nimi spojené krádeže identit způsobují největší finanční ztráty v oblasti kybernetické kriminality.

Jedním z důvodů výrazného zhoršení bezpečnostní situace z posledních let je pandemie nemoci Covid 19. Jejím vlivem došlo k výrazné míře „virtualizace“ množství činností – práce z domu, distanční výuka, elektronizace některých služeb státní správy. Organizace Interpol a její členské státy evidují výrazný nárůst kybernetické kriminality právě ve spojitosti s pandemií. V reportu [7], který pojednává o dopadech pandemie na situaci kybernetické bezpečnosti, rovněž potvrzuje zhoršující se situaci a shoduje se, že mezi nejzávažnější hrozby patří útoky typu ransomware a phishing.



Obr. 0-1 Procentuální podíl výskytu klíčového slova COVID-19 z celkového počtu nahlášených incidentů [7]

Výše uvedené informace podtrhují důležitost procesu zabezpečování provozovaných infrastruktur. Základem pro účinné a efektivní zabezpečování infrastruktury je co nejlepší přehled o jejím provozním stavu [8], získávání informací v reálném čase a možnost jejich zpracování. Týmům správců infrastruktury jsou velice často limitovány z hlediska možností své působnosti. Ať už jsou to finanční limitace, kdy firma nebo státní instituce nemá prostředky, případně není ochotná investovat prostředky do boje s kybernetickou kriminalitou (Velice

častý je přístup: „Proč bychom byli pro útočníky zajímaví? Nás se to netýká“ [1]). Nebo samotné limitace lidských zdrojů a následné nemožnosti problémy detekovat, identifikovat priority, přehlcení požadavky uživatelů a neschopnosti udržet krátký reakční čas. Obecně ideální scénář je takový, kdy problémy jsou identifikovány včas, ideálně s předstihem a je jim předcházeno. Nemělo by se stávat, že problémy jsou řešeny ad hoc.

Bez využití vhodných nástrojů je scénář předcházení a včasné identifikace problémů takřka nemožný.

V návaznosti na předchozí zmiňované problémy práce cílí na popis možností monitoringu infrastruktur, selekci a návrh vhodného řešení a specifikování několika scénářů možného použití. Klade důraz na obecnou aplikovatelnost a rozšiřitelnost navrženého řešení, jehož cílem je realizovat monitoring infrastruktury.

Tímto způsobem může práce pomoci při vlastní implementaci monitorovacích systémů, a tudíž může přispět ke snaze o zlepšení bezpečnostní situace. Rozšiřuje pole působnosti Laboratoře penetračního testování PTLAB [9], v rámci které je na Fakultě aplikované informatiky UTB ve Zlíně [10] řešené problematika kybernetické bezpečnosti, ale ne problematika monitoringu a sběru dat z infrastruktury. Zároveň by výsledky a postupy stanovené v práci měly být využitelné při další výzkumné činnosti laboratoře.

I. TEORETICKÁ ČÁST

1 IT INFRASTRUKTURA

Při řešení práce je často využíváný pojem IT infrastruktura, případně rozsáhlá IT infrastruktura.

Pro jednoduché pochopení je vhodné definovat a vysvětlit tento pojem, objasnit možné dělení infrastruktur a popsat vhodné postupy při jejich tvorbě.

Jako IT infrastrukturu označujeme systém, který je tvořen spojením HW a něm provozovaného SW za účelem umožnění vykonání pracovní činnosti a provozem IT procesů. [11]

K zavedení pojmu **rozsáhlá IT infrastruktura** v současnosti dochází z důvodu narůstající komplexity vznikajících infrastruktur. Rozsáhlost infrastruktury nemusí nutně spočívat pouze v její velikosti, ale spíše označuje její charakter. V rozsáhlých infrastrukturách jsou společně provozována zařízení různé povahy, různého určení, s jinou SW vybaveností a požadavky. Některá zařízení jsou pohyblivá, jiná statická. Infrastruktura může být rozsáhlá svou rozlohou a členěním – je možné, že se rozprostírá v rámci několika budov, měst, případně států. To vše zvyšuje komplexitu infrastruktury, a zároveň zpřísňuje požadavky na její provoz. V neposlední řadě je nutné vzít v úvahu jednu z dalších součástí počítačových infrastruktur, a to samotné uživatele, kteří s infrastrukturou přicházejí do styku a svým jednáním ji ovlivňují.

V rámci řešení této práce je pojem rozsáhlá IT infrastruktura (případně pouze IT infrastruktura) definován jako souhrn všech HW zařízení, provozovaných SW komponent a uživatelů, kteří mají přístup k prvkům infrastruktury. Kdy tento celek je organizovaný do logické struktury a spadá do kompetence jednoho subjektu.

Moderní infrastruktury se tedy vyznačují svou složitostí, spojením mnoha typů zařízení a uživatel. Vzhledem k tomu a zaměření práce na problematiku monitoringu infrastruktury je vhodné definovat základní kategorie zařízení a možnosti členění IT infrastruktur.

1.1 Možnosti členění infrastruktury

Způsobů, jak rozdělit IT infrastruktury je celá řada. Některé z nich již byly naznačeny v předchozích oddílech. Pro potřeby práce je problematika členění infrastruktur zpracována na základě informací dostupných od firem IBM [12] a Red Hat [13].

Obě společnosti se shodují, že jednou z možností klasifikace IT infrastruktur, je rozdělení na základě způsobu jejich provozu. Infrastruktury můžeme následně dělit na:

Tradiční	Cloudové
<p>Jako tradiční infrastruktury se označují takové, kdy všechny komponenty sloužící k jejímu provozu, tj. HW zařízení a SW jsou provozovány a spravovány subjektem, který infrastrukturu využívá.</p>	<p>V případě cloudových infrastruktur pak dochází k řešení, kdy subjekt pouze požaduje a platí výpočetní výkon. Ke službám cloudové infrastruktury má následně přístup prostřednictvím Internetu a přistupuje ke službám více uživatelským přístupem.</p>
<p>Tradiční infrastruktury tedy vyžadují, aby subjekt byl schopný zajistit veškerou správu, prostory, energii pro provoz apod.</p>	<p>O servis a správu Cloudové infrastruktury se plně stará poskytovatel cloudových služeb.</p>

Hybridní

V současnosti je obvyklé, že nedochází ke striktnímu dělení infrastruktur. Je běžné, že subjekt, který převážnou část své infrastruktury provozuje pod svou správou, zároveň využívá cloudové služby, které například zpřístupňuje svým uživatelům. Další z možností je, že subjekt sám provozuje svůj Cloud pouze pro své potřeby.

Infrastruktury, které tímto způsobem kombinují přístup tradiční a cloudový označujeme jako Hybridní a lze takto označit většinu moderních infrastruktur.

Tab. 1-1 Klasifikace infrastruktur dle způsobu provozu

Z důvodu zaměření práce, je takovéto jednoduché rozdělení nedostatečné. Pro potřeby monitoringu nás více než organizace infrastruktury z hlediska jejího provozu, zajímá organizace a typy zařízení, které se v infrastruktuře pohybují.

1.1.1 Dělení infrastruktury na základě charakteru zařízení

S využitím zdrojů [12] [13] zmíněných v předchozím oddíle a doplněním o informace z článků firmy Atatus [14], případně článku Polytechnického institutu východního pobřeží – ECPI [15], které rovněž řeší problematiku klasifikace infrastruktur a zařízení v nich, můžeme stanovit základní klasifikaci prvků IT infrastruktury.

Základem rozdělení, které takto může vzniknout je identifikace tří kategorií:

Hardware	Software	Počítačová síť
Veškeré HW vybavení.	SW, který je využíván k provozu, nebo je záměrně provozován.	Prostředky zajišťující vzájemnou komunikaci a propojení jednotlivých zařízení.
<ul style="list-style-type: none"> • Počítače • Servery • Datová úložiště • Routery • Switche • Apod... 	<ul style="list-style-type: none"> • Operační systémy • Webové služby • Cloudy • Služby • Správcovské systémy • Aplikace • Apod... 	<ul style="list-style-type: none"> • Routery • Switche • Firewally • Access pointy • Pravidla provozu • Apod...

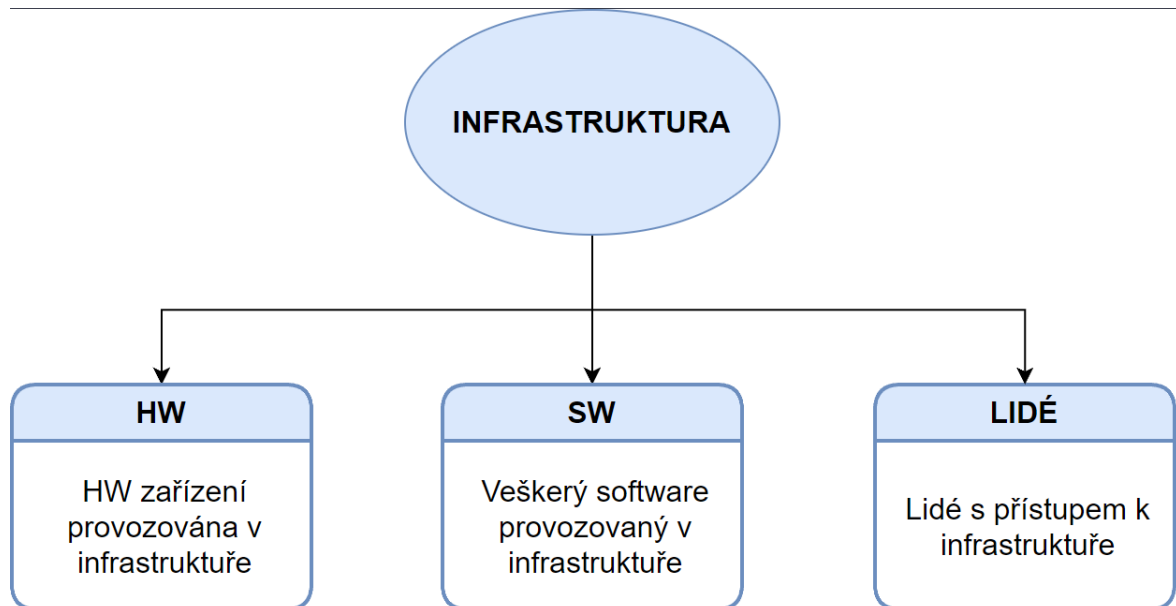
Tab. 1-2 Rozdělení prvků infrastruktur do kategorií podle literatury

Rozdělení uvedené v tabulce vzniká průnikem dostupných informací. Vzhledem k jeho povaze je nutné upozornit na jeho nedokonalost a objasnit jednotlivé nedostatky. V člancích často bývá tvořena čtvrtá a případně další kategorie, které lze zahrnout do kategorií předchozích. Jedním z příkladů například může být tvorba oddělené kategorie pro operační systémy nebo servery. Dále pak samotná kategorie počítačové sítě je zahrnutelná do kategorie HW a SW. V neposlední řadě bývá kompletně opomenuta kategorie uživatelů infrastruktury.

1.1.2 Návrh možnosti klasifikace infrastruktury

Z důvodu nedostatků uvedených v předchozím oddíle práce navrhuje model, dle kterého bude infrastruktura dělena při řešení další problematiky.

Při dělení infrastruktury jsou dle charakteru jednotlivých komponent odlišeny 3 skupiny:



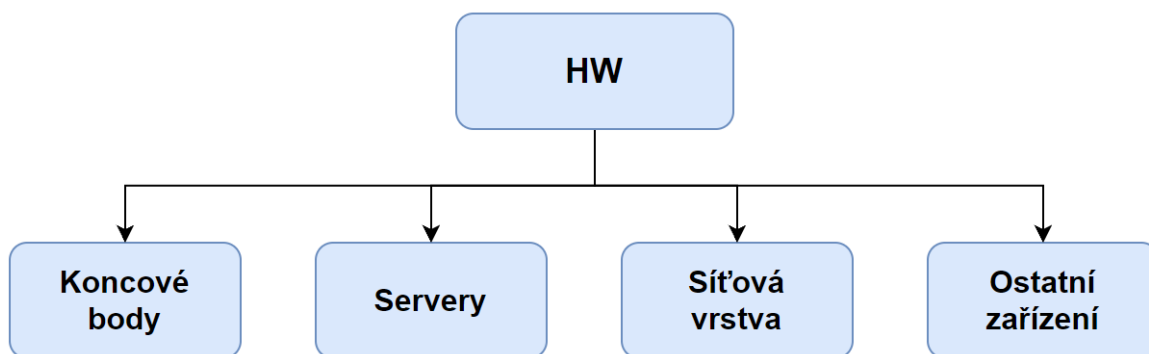
Obr. 1-1 Navržená struktura pro primární dělení prvků infrastruktur [zdroj vlastní]

Takové rozdělení ale určitě není dostatečné a jednotlivé kategorie lze dále dělit a specifikovat jejich povahu.

1.1.2.1 Dělení HW vrstvy infrastruktury

Tak jako v předchozím případě popsaném v oddíle 1.1.1 obsahuje kategorie HW všechna zařízení, která jsou v rámci infrastruktury provozována a propojena. Narozdíl od předchozího případu ale vlastní návrh blíže specifikuje kategorie zařízení.

Samotná HW vrstva infrastruktury může být dále dělena dle charakteru použití samotných zařízení.



Obr. 1-2 Navržené rozdělení kategorie HW zařízení [zdroj vlastní]

Pro každou z identifikovaných kategorií je také definována charakteristika povahy zařízení:

<p><i>Koncové body</i></p>	<p>Pojmem koncový bod infrastruktury rozumíme prvky běžně dostupné uživatelům infrastruktury. Nejčastěji se tedy jedná o stolní a přenosné osobní počítače.</p> <p>V rozsáhlé infrastruktuře často není známá přesná konfigurace a povaha těchto zařízení.</p>
<p><i>Servery</i></p>	<p>Servery rozumíme dedikovaná zařízení v rámci infrastruktury, která jsou velmi často provozována za účelem poskytování služeb uživatelům a samotné realizaci chodu infrastruktury. K serverovým zařízením by běžný uživatel měl mít přístup pouze formou určených služeb a samotné servery by neměly být snadno fyzicky přístupné. HW konfigurace serverů by vždy měla být známá odpovědnému týmu správců.</p>

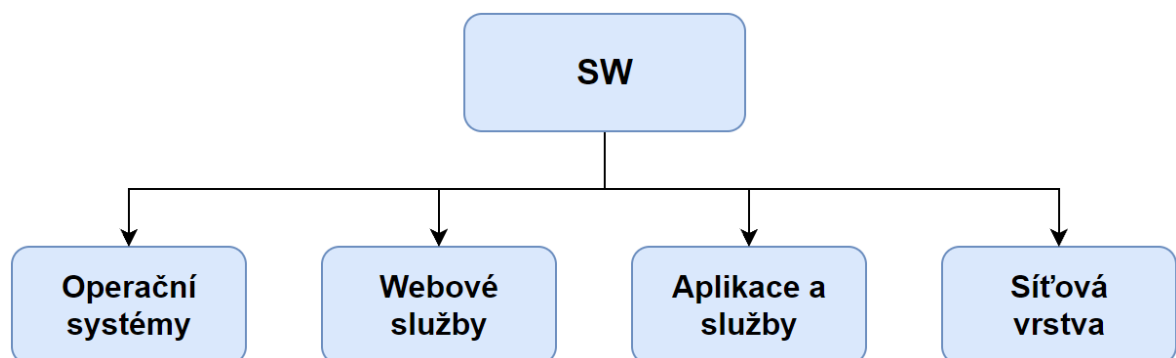
<i>Sít'ová vrstva</i>	Oddělením sít'ové vrstvy v rámci HW zařízení jsou myšlena ta zařízení, která se podílejí na provozu počítačové sítě. Stejně jako v předchozím dělení zde zahrnujeme zařízení typu switch, router, AP, HW firewally apod.
<i>Ostatní zařízení</i>	Ostatní zařízení jsou pak taková, která svou povahou přesně neodpovídají jedné z předchozích kategorií. Pro přiblížení se často může jednat například o tiskárny, chytré televize, projektory připojené k síti apod.

Tab. 1-3 Popis kategorií HW vrstvy infrastruktury

1.1.2.2 Dělení SW vrstvy infrastruktury

Stejně jako předchozí oddíl, dělení SW vrstvy navazuje na oddíl 1.1.1 a rozšiřuje klasifikaci kategorie SW o bližší definici určení jednotlivých prvků.

Bližší rozdělení SW vrstvy:



Obr. 1-3 Navržené rozdělení kategorie SW infrastruktury [zdroj vlastní]

Opět, jako v předchozím případě je pro každou kategorii blíže specifikované její určení:

<i>Operační systémy</i>	Do kategorie operačních systémů jsou zahrnuty všechny operační systémy, které se podílejí na chodu, případně jsou provozovány v rámci infrastruktury. Spadají sem uživatelské OS koncových bodů infrastruktury, ale i SW vybavenost serverů a sít'ových zařízení.
--------------------------------	---

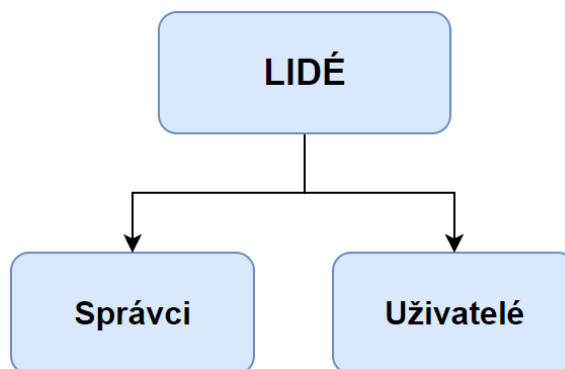
Webové služby	Služby dostupné uživatelům infrastruktury prostřednictvím Internetu/intranetu v podobě webových stránek.
Aplikace a služby	Do této kategorie lze zahrnout ostatní SW vybavenost infrastruktury. Mohou být zahrnuty aplikace v rámci koncových bodů, aplikace provozované na serverech, služby dostupné pro uživatele, mailové služby, databáze apod.
Síťová vrstva	SW vybavenost síťové vrstvy je nedílnou součástí odpovídající kategorie v rámci HW zařízení. V rámci kategorie SW vybavenosti síťové vrstvy zahrnujeme samotnou konfiguraci síťových zařízení, bezpečnostní pravidla, konfiguraci FW apod.

Tab. 1-4 Popis kategorií SW vrstvy infrastruktury

1.1.2.3 Dělení uživatelů infrastruktury

Uživatelé jsou nedílnou součástí každé IT infrastruktury. I tuto kategorii lze blíže specifikovat, a to na základě míry oprávnění a přístupu k infrastruktuře.

Návrh členění infrastruktury rozlišuje dva typy uživatelů:



Obr. 1-4 Navržené rozdělení osob s přístupem k infrastruktuře [zdroj vlastní]

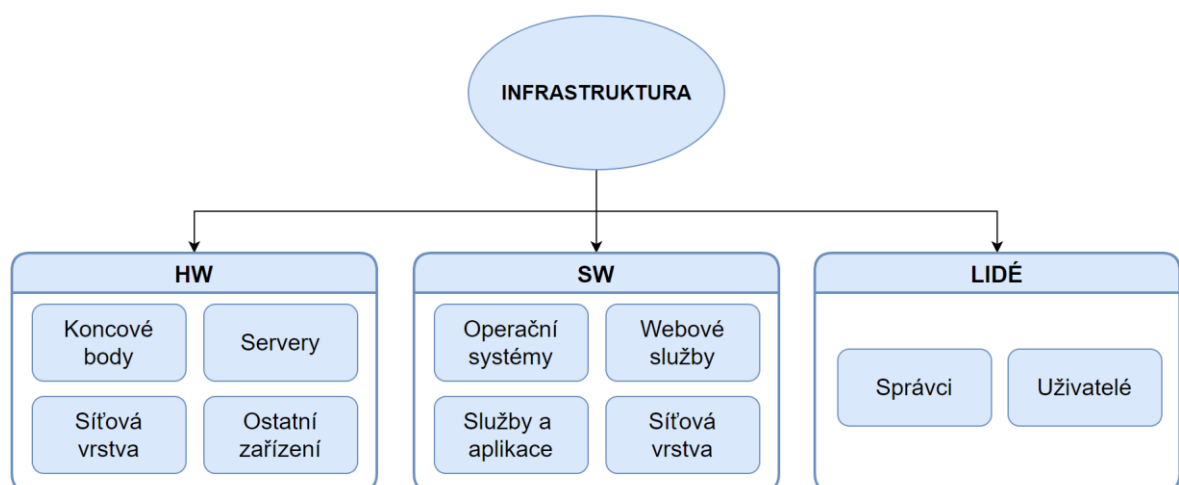
Rozdíl mezi uvedenými rolemi osob je zřejmý, rozdělení můžeme upřesnit takto:

Uživatelé	Jako uživatele můžeme označit jakéhokoliv člověka s přístupem k infrastruktuře, který zároveň infrastrukturu nějakým způsobem využívá. Uživatelé mají přístup pouze k určené kategorii zařízení, jejich činnost je omezená. SW komponenty infrastruktury využívají v uživatelském režimu a nijak nezodpovídají za provoz a konfiguraci jednotlivých prvků
------------------	---

	<p>infrastruktury.</p> <p>Možnou podskupinou uživatelů infrastruktury jsou hosté. Pro ty platí ještě více omezení užívání a přístup je poskytován jen na omezenou dobu.</p>
<i>Správci</i>	<p>Na druhou stranu jako správce, nebo administrátory, označujeme pouze úzkou skupinu lidí. Tato skupina odpovídá za provoz infrastruktury, za řešení problémů, které v infrastruktuře vzniknou, správnou konfiguraci zařízení a dodržování zásad kybernetické bezpečnosti.</p> <p>Kategorie správců by se obecně dala rozdělit na další podkategorie, primárně dle typu činnosti správce. Nejjednodušší dělení by bylo na podskupiny správců odpovídajících za provoz a odpovídajících za bezpečnost.</p> <p>Dodatečnou podskupinou může být skupina tzv. externí podpory. Skupina externí podpory často má správcovský přístup k některým prvkům a podílí se na provozu infrastruktury.</p> <p>Další členění není podstatné pro řešení této práce. Zároveň již v úvodu bylo upozorněno na časté limitace správcovských týmů, nedostatečný rozpočet a lidské zdroje pro bližší určení zaměření jednotlivých členů. Proto je v rámci této práce uvažováno, že IT oddělení zodpovídá za infrastrukturu jako celek, včetně kybernetické bezpečnosti.</p>

Tab. 1-5 Popis rolí osob s přístupem k infrastruktuře

Spojením kapitol 1.1.2.1, 1.1.2.2, 1.1.2.3, které blíže specifikovaly jednotlivé kategorie, vzniká zjednodušené schéma, dle kterého je možné dělit prvky infrastruktury:



Obr. 1-5 Schéma navrhovaného způsobu dělení infrastruktur [zdroj vlastní]

1.2 Proces tvorby zabezpečené infrastruktury

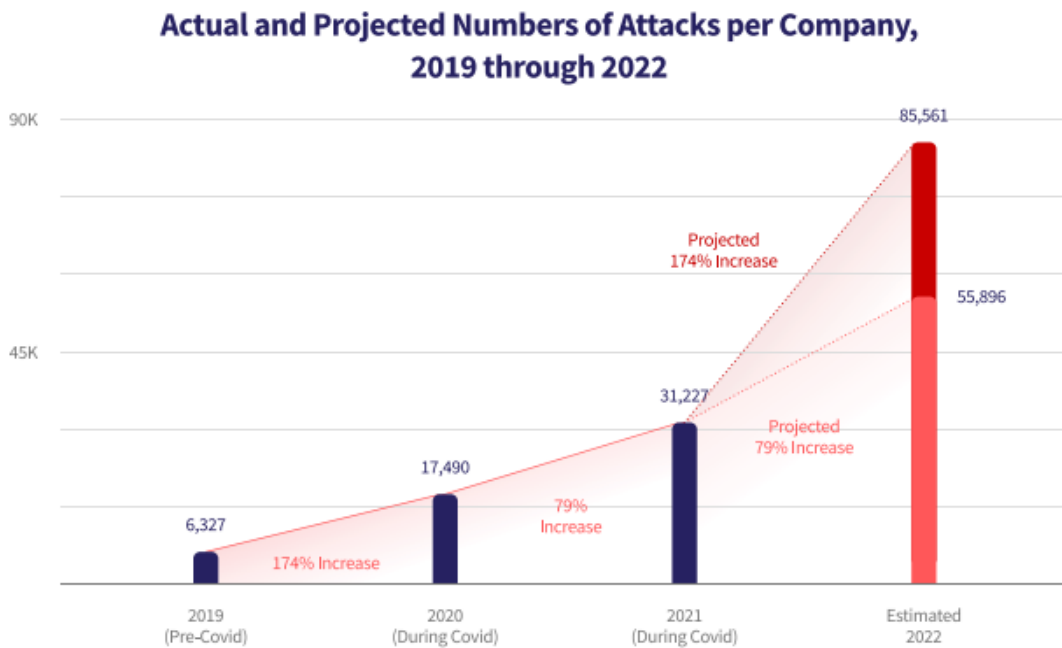
Pokud opět navážeme na informace z úvodu práce, můžeme dojít k závěru, že jedním z hlavních problémů souvisejících s moderními infrastrukturami, je otázka jejich bezpečného a spolehlivého provozu.

1.2.1 Bezpečnostní situace pro IT infrastruktury

V úvodu bylo řečeno, že situace spojená s kybernetickou bezpečností infrastruktur není dobrá. Odvětví kybernetické kriminality je na stálém vzestupu a vznikají nové hrozby, kterým je potřeba čelit. Také byla zmíněna pandemie nemoci COVID-19, která negativně přispěla ke zhoršení bezpečnostní situace v posledních 2 letech, viz. Úvod a report organizace INTERPOL [7].

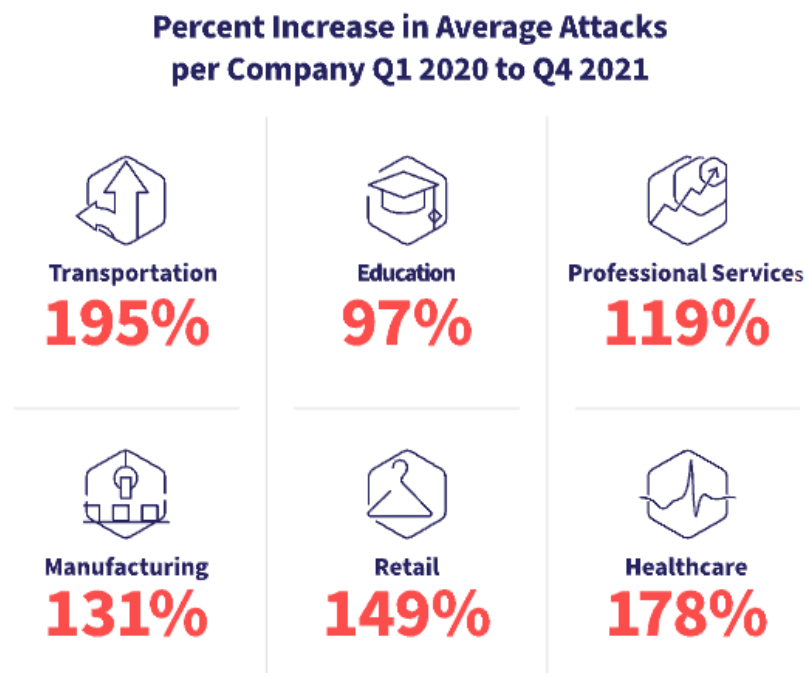
Je důležité k problematice přistupovat s vědomím, že cílem kybernetického útoku může být naprosto každý. Otázkou už není, zda dojde k bezpečnostnímu incidentu, ale kdy. A cílem každé infrastruktury by měla být příprava na takovou událost, předcházení a mitigace případných dopadů.

Reporty porovnávající bezpečnostní situaci z posledních let, upozorňují na nárůst míry útoků v jednotlivých oblastech kybernetické kriminality [3]. Mezi rizikové cíle patří malé a střední podniky. Necelá polovina dotazovaných malých firem se v roce 2021 stala obětí kybernetického útoku [16] a necelých 45 % z této skupiny pak útoků více. Pojišťovací společnost Hiscox v jednom ze svých reportů upozorňuje na velký nárůst průměrné finanční škody způsobené kybernetickým útokem [17] (Pro malé firmy v Evropě je průměr odhadován na necelých US\$ 200 000). Takto způsobené finanční škody mohou být pro řadu firem likvidační a odhaduje se, že až 60 % napadených firem ukončí činnost do půl roku od incidentu [18]. Pro větší firmy je situace obdobná, report firmy CORO [19] uvádí při porovnání let 2019 a 2021 zvýšení rizika možného útoku o necelých 500 %. A je předpokládáno, že v roce 2022 může být firma do 1000 zaměstnanců cílem 56-80 tisíců pokusů o útok ročně – viz. Obr. 1-6.



Obr. 1-6 Porovnání počtu útoků na střední firmy v letech 2019 – 2022 [19]

Špatná situace se ale netýká pouze soukromých firem. Dochází k neustálému nárůstu počtu útoků na vládní organizace, nemocnice, vzdělávací instituce.



Obr. 1-7 Procentuální nárůst počtu útoků na jednotlivá odvětví průmyslu Q1 2020 – Q4 2021 [19]

Problematika útoků na zdravotnictví je často zmiňována. Pravidelně vycházejí upozornění na vysoké riziko pro zdravotnická zařízení a jiné instituce provozující významné informační systémy – např. univerzity. Viz. varování a doporučení NÚKIB [20] [21].

Špatnou situaci pro zdravotnické, vzdělávací a vládní instituce potvrzuje například i zmiňovaný report společnosti CORO [19] – výsledky studie označují zdravotnický sektor jako nejčastější cíl útoků (platné ke konci roku 2021).

Zároveň je potřeba upozornit na výsledky studie společnosti Sophos [22]. Studie se zúčastnilo 5400 respondentů, kteří zastávají pozice odpovědných IT pracovníků, z nichž 100 je z České republiky.

Jedním z výsledků výzkumu je, že vládní a vzdělávací instituce se nejčastěji samy označují jako potenciální cíle útoků a jsou si často vědomy svých nedostatků v oblasti bezpečnosti. Zároveň firma Sophos dodává, že právě v těchto odvětvích nejčastěji dochází k problémům s financováním IT oddělení a investic do kybernetické bezpečnosti.

1.2.2 Aktuální útoky a hrozby pro infrastruktury

Pro stanovení vhodné strategie zabezpečení infrastruktury je důležité seznámit se s možnými hrozbami.

Při sestavování žebříčku nejčastějších útoků bylo využito informací již zmiňovaných reportů firmy Sophos – The State of Ransomware [22], Coro - THE BIGGEST CYBER SECURITY THREATS COMING IN 2022 [19], SonicWall – 2022 Cyber Threat Report [3] a informací dostupných v reportu organizace FBI – Internet Crime Report 2021 [23].

Vybrané typy hrozeb jsou seřazeny v tabulce v závislosti na míře jejich využití.

<i>Ransomware</i>	<p>Při útoku typu ransomware dochází k odcizení citlivých dat společnosti, zablokování přístupu k datům (nejčastěji zašifrování) a požadování výkupného za navrácení dat.</p> <p>Útok typu ransomware často bývá spojen s jiným typem útoku (popsány níže), kdy například pomocí phishingu dojde k zavlečení SW ransomwaru do infrastruktury.</p> <p>Tyto útoky často způsobují velké finanční ztráty. Průměrné výkupné za ztracená data bylo pro rok 2021 cca US\$ 170 000 [22].</p>
--------------------------	---

Částka se samozřejmě pohybuje v závislosti na velikosti cíle a zároveň vznikají další náklady spojené s odstávkou infrastruktury. Průměrná finanční ztráta zahrnující veškeré náklady způsobené útokem je stanovena na US\$ 1.85 mil. [22]. Průměrná délka odstávky infrastruktury pak 23 dní [24].

Jako jedny z nejčastějších cílů těchto útoků jsou označovány vládní a vzdělávací instituce a zdravotnická zařízení [22].

Phishing

Phishing je jedna z metod útoku využívající sociální inženýrství. Útočník využívá podvodnou komunikaci – nejčastěji formou e-mailu s cílem získat citlivá data oběti, případně rozšířit škodlivý SW. [25]

Phishingové útoky se často využívají pro šíření škodlivého SW a k realizaci předchozích útoků typu ransomware, nebo k odcizení dat.

Odhaduje se, že 85 % datových úniků je nějak spojeno s lidským faktorem, necelých 40 % jsou právě útoky typu phishing [26].

FBI pak ve svém reportu upozorňuje na problematiku napadání pracovních e-mailů – tzv. BEC ¹ a celkově odhaduje takto způsobené ztráty na US\$ 2.4 mld. [23].

Útok na podnikový mail spočívá nejčastěji v získání přístupu k pracovní adrese vysoce postaveného pracovníka. S pomocí takto získané autority následně dochází ke schvalování podvodných plateb apod.

Společnost IBM odhaduje průměrnou cenu datového úniku na US\$ 4.24 mil. [27].

Informace také naznačují, že v průběhu pandemie došlo k nárůstu počtu těchto útoků a také jejich specializaci a propracovanosti. Dřívější útoky tohoto typu spoléhaly hlavně na kvantitu a lidský faktor, ty modernější bývají často přesně zacílené. [19]

¹ Business email compromise

Malware attack	<p>Kategorie útoků využívajících jakýkoliv škodlivý software, který infikuje infrastrukturu – trojské koně, viry, spyware. Technicky vzato sem patří i SW odpovědné za ransomware útoky.</p> <p>Je běžné, že jednotlivé metody útoků se kombinují a častým způsobem šířením malwaru je právě předchozí metoda phishingových útoků.</p> <p>Dalším způsobem infikace infrastruktury je zavlečení malwaru na dostupné koncové body infrastruktury [19].</p> <p>Nejčastější cíle malwarových útoků pak jsou vzdělávací instituce, vládní sektor a zdravotnictví [3].</p>
Exploitate	<p>Pojmem exploitate označujeme zneužití bezpečnostní zranitelnosti, nebo chyby v konfiguraci zařízení. Cílem exploitate nejčastěji bývá získání přístupu k zařízení za účelem získání dat, případně zavlečení škodlivého softwaru [28].</p> <p>Nejčastější příčinou možné exploitate jsou zastaralé komponenty infrastruktury, neaktuální SW, špatná konfigurace. V některých případech je možná exploitate dosáhnout pomocí přetížení výpočetní kapacity stroje.</p> <p>Rok 2021 se vyznačuje rekordním počtem objevených zranitelností (CVEs²). Poprvé v historii jejich počet překonal hranici 20 000 [3].</p> <p>Jeden z aktuálních příkladů může být zranitelnost Apache – Log4j, objevena v prosinci 2021, umožňující vzdálené spuštění kódu.</p> <p>V rámci kategorie exploitate můžeme také zahrnout specifické útoky typu SQL injection [29], Cross-site scripting (XSS) [30], DNS spoofing [31] (apod.), které zneužívají zranitelnosti v databázových aplikacích, webových stránkách, respektive zranitelnosti samotného DNS serveru.</p>

² Common Vulnerabilities and Exposures

<p><i>Password attack</i></p>	<p>Jedno z dalších rizik spojených s provozem infrastruktur je špatně nastavená politika týkající se práce s hesly. Často se stává, že používaná hesla nejsou dostatečně složitá, případně je uživatelé využívají napříč několika službami.</p> <p>Jednoduchá hesla s sebou nesou riziko rychlého prolomení útočníky. Hesla využívaná napříč službami (zejména využití firemního hesla také pro externí služby) jsou více náchylná k úniku a jakákoliv kompromitace hesla může vést k výraznější narušení integrity infrastruktury a ke ztrátě dat.</p> <p>I v případě, že hesla mají dostatečnou složitost, stále hrozí riziko sociálního inženýrství a phishingového útoku. Na nárůst počtu phishingových útoků již bylo upozorněno v rámci předchozích oddílů a FBI zároveň upozorňuje na výraznou hrozbu útoků formou vydávání se za technickou podporu [23]. Infrastruktuře hrozí, že sami její uživatelé vyzradí heslo útočníkům.</p> <p>V úvodu zmiňovaný útok na ropovod Colonial Pipeline v USA [5] z května 2021, byl útok typu ransomware. K jeho realizaci bylo využito kompromitované heslo, prodané na Dark Webu³ [3].</p>
<p><i>Denial of service</i></p>	<p>Útoky označovány jako DOS útoky případně DDOS – distribuovaný DOS útok. Jejich cílem je znedostupnění služeb infrastruktury. Realizace probíhá zahlcením dostupné služby množstvím dotazů a požadavků, což vede k výpadku, případně úplnému zničení prvků infrastruktury [3].</p>

Tab. 1-6 Aktuální typy hrozeb pro infrastruktury

³ Jako Dark Web je označována neindexovaná část internetu, nedostupná pomocí běžných nástrojů [70]

1.2.3 Doporučený postup zabezpečování infastruktury

Základem pro tvorbu a další zabezpečování infrastruktury je již zmiňovaná myšlenka, že před kybernetickou hrozbou není nikdo v bezpečí. Při tvorbě infrastruktury je vhodné udržovat přehled o aktuálních hrozbách a identifikovat možné zranitelnosti v infrastruktuře.

Popisem předchozích zranitelností a na základě práce publikované na konferenci CSCI 2019 [8] a doporučení vydaných firmou LoginRadius [32], je možné sestavit seznam základních doporučení pro zabezpečení infastruktury:

<p><i>Udržovat aktuální přehled o infrastruktuře</i></p>	<p>Jedním ze základních kroků při správě a zabezpečování infrastruktury je přehled o jejím využití. Je nutné mít přehled o počtu zařízení, míře jejich využití, sledovat datové toky v rámci infrastruktury.</p> <p>Právě zde vzniká kritická potřeba monitorovacího systému – tím správců bez něj není schopný tyto informace získat.</p>
<p><i>Dělit oprávnění přístupu</i></p>	<p>V rámci uživatelů je nutné jasně definovat jednotlivé role a možnosti přístupu k datům.</p> <p>V rámci správcovského týmu pak distribuovat povinnosti a odpovědnost. Zásadní by mělo být vyhnout se přetížení správců, tato skutečnost často vede ke vzniku chyb v systému.</p>
<p><i>Využít šifrování dat</i></p>	<p>Data v rámci infrastruktury by měla být šifrována. Obzvláště zařízení, na kterých se pohybují citlivá data, data spadající pod GDPR apod.</p>
<p><i>Udržovat přehled o nově vznikajících hrozbách</i></p>	<p>V ideálním případě existuje v rámci správců infrastruktury tým starající se o bezpečnost provozu. V rámci tohoto týmu by měla být sledována bezpečnostní situace, identifikována nová rizika a plánována adekvátní opatření pro minimalizaci rizik.</p> <p>V dalších kapitolách práce proto bude popsána možná integrace systému OSSIM.</p> <p>Další možností pak je provádět pravidelný audit systému s cílem odhalit existující zranitelnosti.</p>

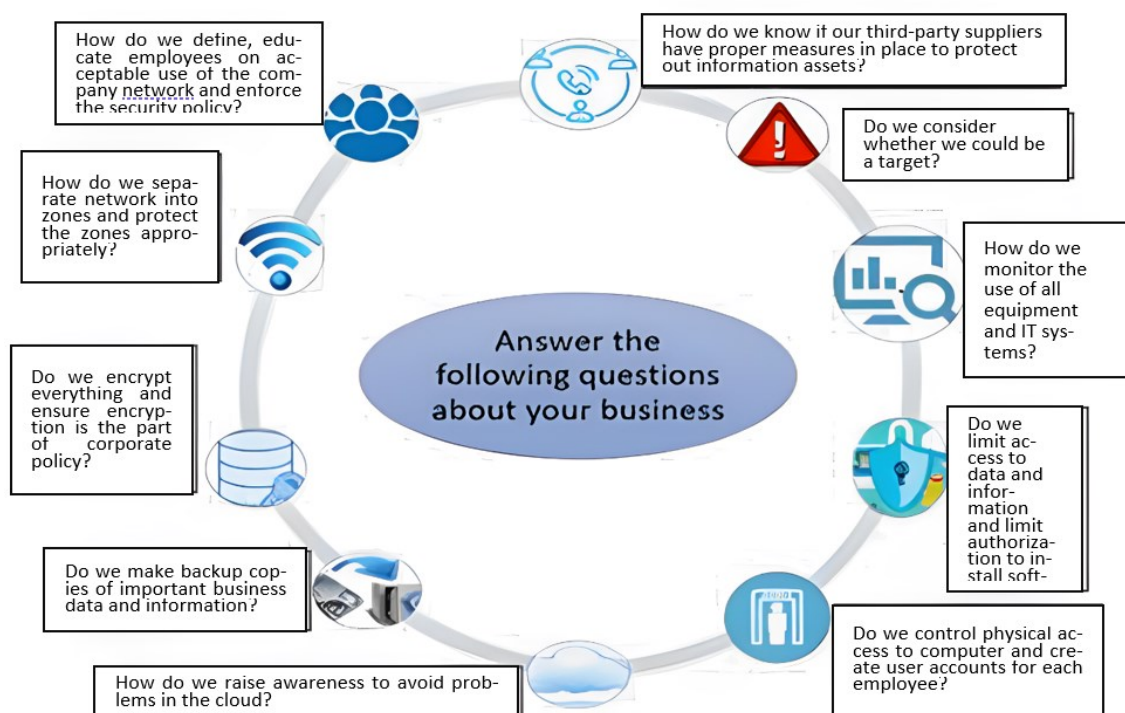
<p><i>Pravidelné zálohy systémů a redundance</i></p>	<p>Pro kritické systémy infrastruktury by měly být implementovány systémy záloh.</p> <p>Ideální systém záloh pak bude obsahovat minimálně 2 „vrstvy“. Jedna ve formě aktivních záloh systémů, vrstva druhá pak pro „zálohy záloh“. Obecně platí, že druhá vrstva záloh by měla být i fyzicky oddělena od zbytku infrastruktury – například jiná budova, z důvodu minimalizace rizika ztráty při vzniku požáru nebo jiné katastrofy v rámci lokality.</p> <p>Kritické prvky a systémy infrastruktury by měly být odolné vůči výpadku – je možné dosáhnout redundancí zařízení.</p>
<p><i>Zabezpečit přenosnou elektroniku</i></p>	<p>Zabezpečení přenosné, případně snadno dostupné elektroniky jako jsou mobilní telefony zaměstnanců, notebooky a osobní počítače, je velmi úzce spojené s šifrováním. Šifrování zařízení, v případě jeho ztráty nebo odcizení, snižuje riziko úniku dat. U přenosných zařízení by také měla být implementována možnost jejich vzdáleného smazání.</p>
<p><i>Bezpečné metody přístupu</i></p>	<p>Problematika týkající se hlavně hesel. Je vhodné stanovit vhodnou politiku pro nutnou složitost hesla. Dobrým přístupem je implementovat systémy pro ověření přístupu bez hesla – generování tokenů, přístupové klíče, systémy 2FA⁴.</p>
<p><i>Správná konfigurace síťové vrstvy</i></p>	<p>Síťová vrstva infrastruktury by měla být rozdělena na podsítě. Mezi jednotlivými podsítěmi implementována pravidla omezující příchozí a odchozí data. Přístup k jednotlivým prvkům je co nejvíce omezen.</p> <p>Přístupový bod infrastruktury do Internetu je v nejlepším případě realizován s využitím firewallu, jsou implementována pravidla na příchozí a odchozí komunikaci a udržován aktuální systém a soubor bezpečnostních pravidel.</p>

⁴ Dvou-faktorová autentizace – po zadání hesla je nutné potvrdit přístup např. z mobilního telefonu.

Práce s uživateli	<p>V neposlední řadě je nutné vhodně pracovat s uživateli infrastruktury.</p> <p>Je vhodné provádět pravidelná školení zaměstnanců, upozorňovat je na možná rizika a vysvětlit vhodné chování v kybernetickém prostoru.</p> <p>Je příhodné stanovit komunikační kanál pro uživatele, prostřednictvím kterého můžou hlásit podezřelou aktivitu a jiné anomálie – nejčastěji helpdeskové systémy.</p>
--------------------------	---

Tab. 1-7 Doporučení pro zabezpečení infrastruktury

Samotné zabezpečování infrastruktury lze označit za cyklický proces, který je vhodně interpretován obrázkem ze zmiňované práce [8]:



Obr. 1-8 Grafické znázornění procesu zabezpečování infrastruktury z publikace na CSCI 2019 [8]

Z Obr. 1-8 i předchozího seznamu doporučení je zřejmé, že monitoring infrastruktury je jedním ze základních kroků při jejím zabezpečování. Bez znalosti systému není možné s ním pracovat.

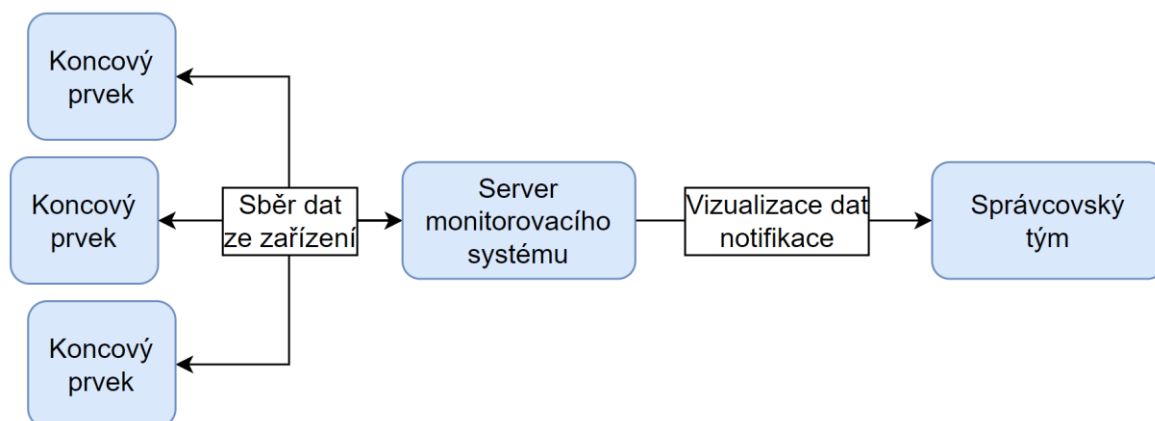
2 MONITOROVÁNÍ INFRASTRUKTUR

V předchozích oddílech bylo vysvětleno, že z důvodu rozsáhlosti infrastruktury a její složitosti, není možné efektivně plánovat a implementovat kroky k její správě, bez dostatečného přehledu o infrastruktuře.

Při monitorování infrastruktury není možné spoléhat pouze na činnost správcovského týmu. Takový tým je sice schopný reagovat na podněty uživatelů, ale není schopný všechny problémy včas detekovat a případně jim předcházet. Zároveň není možné, aby takový tým udržoval přehled o infrastruktuře v reálném čase a manuálně získával provozní data.

Proto je potřebné implementovat v rámci infrastruktury systém jejího monitorování.

Zjednodušeně lze monitorování infrastruktury vysvětlit jako proces, při kterém dochází ke sběru dat z provozovaných prvků. Data jsou shromažďována s cílem jejich následné analýzy, vyhodnocení stavu infrastruktury a předání informací správcovskému týmu [33].



Obr. 2-1 Schéma procesu monitorování infrastruktury [zdroj vlastní]

2.1 Charakter získaných dat

Existuje více způsobů, jak kategorizovat data, která jsou v rámci infrastruktury sledována a sbírána. V rámci problematiky práce můžeme sbíraná data dělit do třech hlavních kategorií:

Provozní data

Bezpečnostní data

Síťový provoz

2.1.1 Provozní data

Jak už název napovídá, tak do kategorie provozních dat patří parametry spojené s provozem zařízení. Mimo jiné zejména:

<i>Sledování vytížení zařízení</i>	Vytíženost procesoru, operační paměti, cache, počet běžících procesů apod.
<i>Vytíženost diskového prostoru</i>	Míra zaplněnosti diskového prostoru, počet diskových jednotek, připojených přenosných zařízení apod.
<i>Síťový provoz</i>	Kvantifikace objemu síťového provozu zařízení, síťových rozhraní, dostupnost v síti.
<i>Operační systém</i>	Verze operačního systému, typ.
<i>Běžící služby a aplikace</i>	Sledování dostupnosti síťových služeb, sledování běhu aplikací a služeb v rámci zařízení.
...	...

Tab. 2-1 Možné typy sledovaných dat při provozním monitoringu

2.1.2 Bezpečnostní data

Bezpečnostní data na rozdíl od předchozí kategorie popisují bezpečnostní stav jednotlivých zařízení. Pro jejich získání nejčastěji dochází ke zpracování logů systému nebo aplikací a následné analýze s cílem odhalení anomálie, nebo konkrétní události související s bezpečností provozu.

V souvislosti se sběrem takových dat jsou v literatuře často skloňovány systémy SIM a SEM:

- **SIM – Security Information Management [34]**

Touto zkratkou označujeme systém, který se stará o automatizovaný sběr logů a informací ze zařízení, jejich uložení v přehledné formě na centrálním uložišti a identifikaci událostí spojených s bezpečností provozu.

- **SEM – Security Event Management [35]**

Drobným rozdílem oproti systému SIM je, že systém SEM v rámci analýzy získaných dat vyhledává převážně konkrétně definované typy bezpečnostních událostí. [36]

Kvůli vysoké podobnosti zaměření výše uvedených systémů se v současné době spíše využívá kombinace těchto systémů, takový systém je pak označen jako **SIEM – Security information and event management**.

2.1.3 Síťový provoz

Pro monitorování síťového provozu infrastruktury se v současné době nejvíce využívá protokol NetFlow a jeho alternativy [37]. Tento protokol byl původně představený společností CISCO, jako náhrada předešlých řešení a využívá se pro sledování toku dat skrz síťové rozhraní [38]. Ostatní výrobci síťových zařízení posléze implementují své vlastní alternativy se stejnou funkcionalitou.

Získaná data následně obsahují informace o zachycené komunikaci, například:

- Zdrojová / cílová IP adresa komunikace
- Objem datového toku v čase
- Objem packetů toku v čase
- Typ síťového protokolu
- Zdrojový / cílový port komunikace
- Původce datového toku

2.2 Požadavky při návrhu monitorovacího systému

Před návrhem monitorovacího systému je nutné stanovit si kritéria a cíle, které by monitorovací systém měl splňovat a stanovit jakým způsobem bude realizován.

Základním cílem monitorovacího systému je poskytovat správcovskému týmu zpětnou vazbu o stavu provozované infrastruktury. Bez této zpětné vazby není možné ověřit funkčnost implementovaných řešení.

V rámci nasazení monitorovacího systému je podstatných několik věcí. Je vhodné, aby platforma monitorovacího systému byla, pokud možno co nejjednodušší z hlediska samotného provozu. Je rozumnější snažit se co největší část monitoringu obsáhnout v rámci jednoho systému, vyhnout se realizaci oddělenými systémy. Každý nový systém by vyžadoval své správce a vědomostní bázi, jak s ním pracovat. Také by bylo nutné řešit vzájemnou kompatibilitu systémů a sjednocovat formát získávaných dat.

Složitost a komplexita monitorovacího systému je ovlivněna hlavně požadavky na typ získávaných dat. Před volbou samotného systému řešení je nutné ujasnit jaká data mají být v infrastruktuře sledována a na kterých prvcích.

Určením monitorovaných prvků a potřebných možností nasazení monitorovacího systému vznikají další kritéria, které výsledný systém musí splnit. Je nutné, aby na zvolených prvcích byla zajištěna kompatibilita, a tedy možnost sběru dat.

Sběr dat následně může probíhat ve dvou režimech:

Agent monitoring	Agent-less monitoring
Při formátu monitorování prvků pomocí tzv. agenta dochází k instalaci komponenty monitorovacího systému na sledované stroje. Tato komponenta se označuje jako agent. Instalovaný agent následně na základě požadavků monitorovacího systému realizuje proces získání dat v rámci zařízení	V režimu monitoringu agent-less nedochází k instalaci agenta na zařízení. Pro sběr dat z prvků je využíván některý z komunikačních protokolů. Nejčastěji například protokoly SNMP ⁵ , SSH ⁶ nebo dříve zmiňovaný protokol NetFlow a jeho obdoby. Zároveň také virtualizační platformy typu VMware

⁵ Simple network management protokol

⁶ Secure shell

a řídí komunikaci s monitorovacím serverem.	vSphere disponují zabudovanými možnostmi agent-less monitoringu.
Při volbě systémů s agentem je nutné si ověřit, zda existují vhodné kompatibilní verze agenta pro provozované systémy.	Limitace této realizace pak spočívá pouze v kompatibilitě a schopnosti zařízení využít některý z použitelných protokolů.

Tab. 2-2 Agent vs agent-less monitoring

Mezi další vlastnosti monitorovacího systému by měla patřit možnost určitým způsobem vyhodnocovat získaná data a předzpracovávat je pro tým správců. Právě automatický sběr dat a identifikace definovaných stavů je jedním z přínosů a důvodů proč implementovat monitorovací systém.

Při samotné konfiguraci je potřebné, aby systém umožňoval týmu správců definovat pravidla, dle kterých bude docházet nejen ke sběru dat ale i k jejich následnému vyhodnocení. Při vyhodnocování dat je potřebné mít možnost definovat a identifikovat krizové stavy – např. přetížení procesoru systému apod. Po identifikaci krizového stavu je nutné vytvořit upozornění pro tým správců na vznik události v infrastruktuře.

Upozornění nejčastěji bývá realizováno prostřednictvím grafického dashboardu, na kterém může správce sledovat aktuální stav systému a přehled vzniklých událostí. Nebo odesláním upozornění do vybraného komunikačního kanálu – např.: e-mailu. Komunikační možnosti monitorovacího systému mohou být jedno z dalších kritérií ovlivňující volbu řešení k implementaci.

Při definování podmínek krizových stavů a následných upozornění na ně je také potřeba dbát tzv. prioritizace upozornění. Je nutné odlišit důležitost jednotlivých událostí a zajistit, že nedojde k přehlcení komunikačních kanálů velkým množstvím nevýznamných událostí. Takový stav může vést k nechtěné ignoraci kritických událostí, kdy pro množství upozornění správcovský tým ztratí přehled.

Zároveň je potřebné, aby monitorovací systém v rámci zpracování dat umožňoval identifikaci anomálního chování. Nejčastěji dochází k identifikaci neobvyklých odchylek v systému oproti již získaným datům z infrastruktury.

Posledním krokem monitorovacích systémů pak bývá automatizace reakce na definované stavy. Poté co dojde k identifikaci krizového stavu, bude systém schopný provést automatický pokus o vyřešení krizové události – jedná se o automatizaci managementu infrastruktury.

Monitoring infrastruktury označuje výše popsaný proces sběru dat a definování podmínek a identifikace problémů. **Management infrastruktury** pak označuje proces využití těchto informací při správě infrastruktury. Obecně platí, že monitoring infrastruktury umožňuje její management.

2.3 Přínosy monitorovacího systému

Z požadavků na monitorovací systém v předchozím oddíle nepřímo vyplývají také výhody a přínosy jeho implementace.

V první řadě monitoring infrastruktury umožní správcovskému týmu získat přehled o infrastruktuře a jejím stavu. To vede k efektivnějšímu využití lidských zdrojů v rámci oddělení. Správcovský tým není nucen věnovat tolik úsilí identifikaci problémů v infrastruktuře, zároveň také není v pozici, kdy se o problémech často dozvídá až od uživatelů. Takový scénář většinou znamená, že problém už reálně existuje, není tedy možné mu zabránit a už byl ztracen čas pro jeho vyřešení.

Dalším přínosem tedy je, v případě vhodného definování pravidel, nejen identifikace problémů samotných, ale také identifikace možných indikátorů, které naznačují potenciální vznik problému v blízkém čase. Díky tomu je následně možné včas podniknout kroky vedoucí k potlačení problému. Ve výsledku tedy nedojde k omezení činnosti infrastruktury.

Z hlediska upozornění na problémy a stav systému nebo grafické vizualizace, je pak přínos v přehledném zobrazení vybraných dat v reálném čase. Možnost sledovat data v reálném čase následně může být využita při trasování problémů v infrastruktuře, optimalizaci její činnosti, rozložení zátěže, nebo návrhu optimalizace datových tras.

V neposlední řadě je monitorovací systém možné využít pro forenzní analýzu. Pokud jsou uchovávána data ze zařízení, je možné tato data analyzovat i v případě ztráty sledovaného zařízení, protože ta jsou uchována na monitorovacím serveru. Zpětně je tedy možné provést forenzní analýzu s cílem určit příčinu ztráty zařízení, vyšetření události, předání informací k trestnímu řízení apod.

3 PŘEHLED MONITOROVACÍCH SYSTÉMŮ

V přechodí kapitole 2 byla popsána problematika monitoringu infrastruktur, konkrétně možné požadavky a cíle monitorovacího systému. Stanovení podobných požadavků je kritické po následnou volbu konkrétního řešení, které v rámci infrastruktury bude implementováno. Kromě zmíněných požadavků je taky vhodné vzít v úvahu kompatibilitu řešení se stávajícím stavem infrastruktury, případně složitost instalace a nasazení.

V současné době existuje celá řada monitorovacích systémů. I přes stejné určení se často vyznačují různými odlišnostmi, různým určením, cenou apod. Právě z tohoto důvodu je nutné stanovit požadavky na sběr dat, zvolit vhodné řešení a přejít k implementaci zvoleného řešení.

V rámci praktické části je řešena implementace konkrétního řešení v testovací infrastruktuře, v této kapitole je uveden jednoduchý přehled vybraných monitorovacích systémů a jejich funkcionalit. Základem pro sestavení seznamu dostupných řešení byl článek [39] publikovaný ve sborníku IEEE Software, který se zabýval právě problematikou monitoringu infrastruktur a dostupných řešení pro monitoring.

Autoři článku vytvořili základní přehled formou tabulky, ve které srovnávají možnosti zvolených řešení.

Tool	License	Support	User interface	Alerts	Web or mobile client	Help desk integration	Automation	OS support	Target business size	Strengths
Nagios	Open source (GPL*)	Active support community	Improved Web GUI†	Email, SMS*, custom	Web interface	Yes	Yes†	Linux, Unix, Windows via proxy agent	Small, medium, and large	Flexible and highly configurable, robust and reliable
Zabbix	Open source (GPL)	Active support community, email, forums, help desk, phone, wiki	Well-designed Web GUI	Email, SMS, custom	Web interface	Yes	Yes with API	Windows, Mac, Linux, Unix	Enterprise	Flexibility to organize monitoring data, configurability, scalability
Hyperic	Open source (GPL v2)	Support community, email, help desk	Good Web interface	Email, SMS	Web interface	Yes	Yes†	Windows, Mac, Linux, Unix	Small and medium	Native management for Unix, Linux, Windows, and Mac; scalability
Solar-Winds	Proprietary	Active support community, email, forums, help desk, phone	Excellent GUI	Email, custom	Web interface, mobile	Yes	Yes	Windows, Mac, Linux, Unix	Small and medium	Quick and easy deployment, affordability, native support for VMware
Manage-Engine OpManager	Proprietary	Email, forums, help desk	Unconventional UI that's hard to navigate	Email, custom	Web interface, mobile	Yes	Yes	Windows, Mac, Linux, Unix	Small and medium	Great feature set
HP Operations Manager	Proprietary	Forums, help desk, webinars	Good Web interface	Email, SMS, custom	Web interface, mobile	Yes	Yes	Windows, Linux, Unix	Large	Integration with other products from the same company; integration with HPIC, which can integrate with SCCM or SCOM.*
IBM Tivoli	Proprietary	Email, forums, help desk	Good, intuitive Web interface	Email, SMS	Web interface	Yes	Yes	Windows, Linux, Unix	Enterprise	Automatic analysis and repair, efficient where many resources

Obr. 3-1 Tabulka řešení srovnávaných v článku zabývajícím se problematikou monitoringu infrastruktur [39]

Vzhledem ke stáří původního článku je vhodné rozšířit informace o dostupných řešení o nové systémy a vytvořit obdobné srovnání.

Srovnáním s dalšími zdroji [40], [41], [42] bylo pro vytvořené srovnání zvoleno 10 zástupců monitorovacích systémů:

- Zabbix
- Nagios
- Pulseway
- Solar-Winds
- Elastic Stack
- Prometheus
- Datadog IM
- ManageEngine OpManager
- WhatsUp Gold
- Dynatrace

3.1 Popis vybraných řešení

<p><i>Datadog infrastructure monitoring</i></p>	<p>Systém od firmy Datadog vznikl jako řešení pro monitorování cloudových infastruktur, ale je stejně dobře aplikovatelný v rámci infrastruktury klasické. Sběr dat probíhá pomocí agenta, kterého je nutné instalovat na sledovaná zařízení, konfigurace a tvorba dashboardů je prováděna skrze aplikaci systému. Systém je schopný ze zařízení zpracovávat provozní metriky, logy, vyhodnocovat jejich síťový provoz, zařízení mohou být fyzická, případně virtualizovaná. Zároveň je toto řešení dostupné také v režimu SaaS. [43]</p>
<p><i>Dynatrace</i></p>	<p>Systém firmy Dynatrace rovněž nabízí komplexní možnosti aplikovatelné jak v rámci cloudového prostoru, tak klasické infrastruktury. Podobně jako předchozí systém probíhá sběr informací z infrastruktury pomocí agenta. Systém je následně schopný vyhodnocovat stav zařízení, aplikací, virtuálních strojů, databází apod. Monitoring je zahrnut v rámci jednotné platformy firmy Dynatrace, pomocí které je možné sledovat také bezpečnostní situaci, implementovat prvky automatizace infrastruktury apod. Řešení SaaS je také dostupné. [44]</p>

<i>Elastic Stack</i>	<p>Tzv. Elastic Stack [45] je prvním zmiňovaným open-source řešením. Kombinuje tři komponenty: Elasticsearch, Logstash a Kibana. Logstash je pomyslnou první vrstvou systému, podporuje velké množství různých datových zdrojů [46] a jejím cílem je unifikovat takto získaná data a předat k dalšímu zpracování. Samotné zpracování a analýza dat probíhá v rámci Elasticsearch vrstvy a poslední komponenta Kibana se využívá pro tvorbu grafických vizualizací zpracovaných dat. Kromě open-source verze jsou dostupná také řešení SaaS.</p>
<i>Nagios</i>	<p>První verze systému Nagios byla zveřejněna už v roce 2002 a patří mezi nejstarší systémy řešící problematiku monitoringu infrastruktur. Pro monitoring zařízení mohou být využity oba přístupy, tedy agent i agent-less monitoring [47].</p> <p>Nagios existuje ve dvou verzích, open source verzi Nagios Core a zpoplatněné verzi Nagios XI. Bezplatná verze obsahuje základní metody monitoringu prvků infrastruktury a základní systém reportingu, zpoplatněná verze následně nabízí možnosti automatického reportování, rozsáhlejší možnosti konfigurace apod. Ani jedna verze nenabízí režim provozu SaaS. Seznam rozdílů verzí je dostupný zde [48].</p>
<i>ManageEngine OpManager</i>	<p>Pomocí systému je možné vyhodnocovat síťový provoz, ale také jednotlivá zařízení, virtuální stanice, úložiště apod. v reálném čase. Monitoring probíhá v agent-less režimu pro všechna zařízení. A podobně jako předchozí řešení je možné vyhodnocovat chybové stavy a generovat upozornění. Neexistuje bezplatná verze a není možnost SaaS [49].</p>

<i>Prometheus</i>	Systém Prometheus je jedno z hlavních dostupných open-source řešení. Primární určení je ke sledování provozu aplikací a služeb. Systém Prometheus se skládá z několika komponent. Za monitoring a získávání dat v čase zodpovídá Prometheus server. Ten je rozšířen o komponenty realizující vizualizaci dat a upozornění na definované stavy. [50]
<i>Pulseway</i>	Moderní systém s možnostmi vzdáleného monitoringu a správy zařízení v infrastruktuře. Pulseway cílí na snadné použití na straně zákazníka a jednoduchou integraci do stávající infrastruktury. Skrz aplikaci správci získají přístup k provozním datům jednotlivých zařízení a je možné konfigurovat vlastní systém upozornění na kritické stavy a provádět operace vzdálené správy. Lze tvořit také automatická pravidla jako reakci na detekované stavy. [51]
<i>Solar-Winds</i>	Firma Solar-Winds nabízí celou řadu nástrojů sloužících pro práci s infrastrukturou. Jedním z nich může například být Server and Application monitor. Ten je určený pro monitorování infrastruktur, konkrétně jednotlivých zařízení nebo provozovaných aplikací. Nejčastěji s využitím protokolu SNMP nebo WMI. Pro monitoring existují připravené vzory, které je možné využít při konfiguraci, samotná konfigurace celého systému může být složitá z důvodu většího počtu komponent. Bezplatná verze je funkční pouze v rámci 30-ti denního zkušebního období. [52]
<i>WhatsUp Gold</i>	Komplexní monitorovací nástroj schopný sledovat jednotlivé komponenty infrastruktury jako jsou síťová zařízení, servery, aplikace apod. Obdobně jako ostatní řešení využívá protokoly SNMP, WMI, SSH pro získávání dat ze zařízení. Data pak popisují fyzický stav zařízení a jejich provoz. Aplikace obsahuje možnost tvořit grafické vizualizace a vytvářet systém upozornění na události a stavy v infrastruktuře. Řešení je také možné integrovat spolu s řešením Flowmon NPMD/NDR.

Zabbix

Platforma Zabbix je v rámci zmiňovaných možností další čistě open-source řešení. Veškerá funkcionality platformy je dostupná zdarma k implementaci a neexistuje možnost SaaS. Jedinou zpoplatněnou částí platformy je nadstandardní podpora a asistence s implementací, samotná funkcionality není nijak limitována.

Monitoring může být realizován v agent i agent-less režimu. Agent podporuje širokou škálu OS, agent-less režim využívá už dříve zmiňovaných komunikačních protokolů – SNMP, IPMI apod. Součástí řešení je kromě systémů sběru dat také možnost tvorby grafických vizualizací a konfigurace systému upozornění a notifikací. Výhodou je rozsáhlá komunita platformy a dostatek materiálů pro řešení problémů při implementaci [53].

Tab. 3-1 Popis porovnávaných monitorovacích systémů

3.2 Srovnání vybraných řešení

Využitím dostupných informací můžeme rozšířit a aktualizovat tabulku z úvodu této kapitoly.

Nástroj	Licence	Podpora monitorovaného OS	Systém upozornění	Cena – úroveň enterprise, příp. podobné
Datadog IM	Zpoplatněná	Agent - Windows, Mac, Linux/Unix	E-mail, případně nastavitelný kanál, grafická vizualizace	Monitoring - \$ 23 za prvek infrastruktury / měsíc + další služby odděleně
Dynatrace	Zpoplatněná	Agent - Windows, Linux/Unix	E-mail, případně nastavitelný kanál, grafická vizualizace	Základní cena \$ 21 za každých 8 GB RAM na monitorovaném prvku / měsíc
Elastic Stack	Open-source	V závislosti na kolektoru dat	E-mail, případně nastavitelný kanál, grafická vizualizace	Open-source
Nagios	Open-source / zpoplatněná	Agent - Windows, Mac, Linux/Unix	E-mail, případně nastavitelný kanál, grafická vizualizace	Open-source; zpoplatněná licence \$ 3 495, platí se licence na monitorovací systém, ne v režimu za prvek
ManageEngine OpManager	Zpoplatněná	V závislosti na kolektoru dat	E-mail, případně nastavitelný kanál, grafická vizualizace	Pro počet 250 zařízení základní cena \$ 11 545.
Prometheus	Open-source	V závislosti na kolektoru dat	E-mail, případně nastavitelný kanál, grafická vizualizace	Open-source
Pulseway	Zpoplatněná	Agent - Windows, Mac, Linux/Unix	E-mail, případně nastavitelný kanál, grafická vizualizace	V závislosti na počtu zařízení, pro 250 zařízení základní cena \$ 370 / měsíc
Solar-Winds	Zpoplatněná	V závislosti na kolektoru dat	E-mail, případně nastavitelný kanál, grafická vizualizace	V režimu nákupu vlastní licence pro on premise řešení - \$ 2 995 / rok. Po roce je případně nutné za poplatek obnovit nárok na podporu.
WhatsUp Gold	Zpoplatněná	V závislosti na kolektoru dat	E-mail, případně nastavitelný kanál, grafická vizualizace	Ovlivněno počtem zařízení, dostupné nabídky pro 100 zařízení \$ 3 985.
Zabbix	Open-source	Agent - Windows, Mac, Linux/Unix	E-mail, případně nastavitelný kanál, grafická vizualizace	Open-source

Tab. 3-2 Srovnání vybraných monitorovacích systémů

II. PRAKTICKÁ ČÁST

4 POPIS ŘEŠENÉ INFRASTRUKTURY

Kromě teoretického popisu infrastruktur a popisu systémů pro práci s infrastrukturou. Patří mezi další cíle práce praktická implementace monitorovacího řešení na testovací infrastruktuře.

Samotné implementaci předchází praktický popis infrastruktury, možnosti identifikace klíčových prvků a definování scénářů případného výpadku identifikovaných prvků.

4.1 Obecné vlastnosti a rozdělení řešené infrastruktury

S využitím teoretického základu stanoveného v kapitole 1 a jejich podkapitol můžeme řešenou infrastrukturu, pro kterou má být monitorovací systém navrhován, označit jako infrastrukturu hybridní. Jednotlivá zařízení jsou fyzicky provozována v rámci infrastruktury a převážná většina služeb využívá pro svůj provoz lokálně spravovaných serverů a spadá pod lokální správu. Ale jsou využívány i některé externí cloudové služby. V souladu s informacemi z teoretické části práce je nutné říct, že se jedná o infrastrukturu spadající do kategorie vzdělávacích institucí.

4.1.1 Topologické rozdělení infrastruktury

Z topologického hlediska se celková infrastruktura rozprostírá na území více měst, a v oddělených budovách. Technická vybavenost každé budovy se liší na základě potřeb, počtů a typů provozovaných zařízení.

Z hlediska internetové sítě jsou jednotlivé lokality propojeny centrálním směrovačem, který řídí provoz mezi logickými segmenty sítě a odchozí provoz do Internetu. Řešenou infrastrukturu a primární cíl při návrhu implementace v rámci této práce tvoří infrastruktura pouze jedné budovy. Je předpokládáno, že poznatky a závěry stanovené prací budou obecně aplikovatelné na prvky ostatních lokalit a tím dojde k návrhu systému pro pokrytí celé infrastruktury jako celku.

Řešená infrastruktura tedy představuje rozsáhlou infrastrukturu, popsanou v kapitole 1. Pod lokální správu v rámci infrastruktury spadají koncová zařízení uživatelů, jejich požadavky, servery, síťové tiskárny, síťová zařízení – směrovače, access pointy a jiná elektronika. V řešení infrastruktuře není implementován žádný monitorovací systém.

V podkapitole 1.1.2 byl navržen a popsán systém klasifikace prvků rozsáhlé infrastruktury do oddělených kategorií lišících se dle podstaty a typu zařízení. Na základě těchto informací je možné rozdělit i řešenou infrastrukturu.

4.1.2 Popis řešené infrastruktury na základě HW vlastností zařízení

Ve zmiňované kapitole 1.1.2 bylo stanoveno rozdělení HW zařízení od čtyř kategorií: **koncové body, servery, síťová vrstva, ostatní zařízení**. V řešené infrastruktuře se vyskytují zařízení spadající do těchto kategorií v následující podobě:

<p><i>Koncové body</i></p>	<p>V rámci řešené infrastruktury tvoří nejpočetnější skupinu zařízení koncové body, využívané pro osobní potřebu uživatelů. Tato zařízení jsou nejčastěji realizována formou stolních počítačů, případně přenosných laptopů. Pro řešenou infrastrukturu je specifické, že převážná většina koncových bodů fyzicky umístěných v budově, se nachází na snadno dostupných místech. Přístup k těmto zařízením tak potenciálně má velký počet lidí, což rapidně zvyšuje rizika pro infrastrukturu. Menší část zařízení je pak umístěna v rámci kanceláří zaměstnanců. Přístup k těmto zařízením je tedy do určité míry omezen.</p> <p>Celkový počet koncových bodů přítomných v rámci infrastruktury, případně laptopy spadající pod lokální správu. Můžeme počet stanovit odhadem na 750-1000 zařízení. Do budoucna může být předpokládán drobný nárůst počtu zařízení, ale zároveň je nutné zmínit, že v rámci infrastruktury dochází k průběžné obměně zařízení, která tento nárůst reguluje.</p>
<p><i>Servery</i></p>	<p>Další skupinou zařízení provozovanou v rámci infrastruktury je skupina serverů. Do této skupiny jsou v rámci řešené infrastruktury zahrnuta zařízení s cílem provozovat služby pro uživatele, zařízení zajišťující výpočetní výkon k provádění simulací, disková pole – nejčastěji realizovaná formou NAS, případně vytvořené clustery.</p> <p>Zařízení jsou až na výjimky umístěná v dedikované, vhodně vybavené serverovně. Ta je uzamykatelná a přístup do ní je omezen pouze na vybranou skupinu správců. V rámci serverovny jsou zařízení umístěna v uzamykatelných rackových skříních.</p>

	<p>Počet těchto zařízení by se dal celkově stanovit na 20-25 a výrazný nárůst v počtu zařízení není očekáván. V rámci celkové infrastruktury je počet serverových zařízení vyšší a je provozována další serverovna.</p>
<i>Síťová vrstva</i>	<p>Co se síťových zařízení týče, tak jak již bylo zmíněno, centrálním prvkem mezi lokalitami celkové infrastruktury je jeden centrální směrovač. V rámci řešené infrastruktury je pak síťová vrstva realizována primárně formou přepínačů. Struktura síťového zapojení bude popsána v dalších podkapitolách práce. Druhou nejpočetnější skupinou síťových zařízení jsou pak síťové access pointy realizující pokrytí bezdrátovou sítí. Mezi další zařízení pak můžeme zahrnout síťové prvky pro tvorbu izolovaných podsítí v rámci řešené infrastruktury a neřiditelné switche využívané k navýšení počtu přípojných bodů sítě.</p> <p>Hlavní síťová struktura je v rámci řešené infrastruktury realizována desítkami směrovačů a access pointů.</p>
<i>Ostatní zařízení</i>	<p>Mezi ostatní zařízení pak v rámci řešené infrastruktury budou nejčastěji spadat síťové tiskárny, audiovizuální technika – informační kiosky, dataprojektory a jiná zařízení propojená v rámci počítačové sítě – měřicí přístroje, IP kamery apod.</p>

Tab. 4-1 Popis prvků HW vrstvy řešené infrastruktury

4.1.3 Popis řešené infrastruktury na základě SW vlastností zařízení

Stejně jako v teoretické části i při praktickém popisu jsou odděleny HW a SW vlastnosti provozovaných zařízení. Využitím stejných 4 kategorií jako v kapitole 1.1.2 je možné stanovit popis infrastruktury jako:

<i>Operační systémy</i>	<p>V rámci řešené infrastruktury a SW vybavenosti provozovaných zařízení je nejpočetněji zastoupeným operačním systémem systém Windows. Až na výjimky v řádu pár jednotek jsou veškeré koncové body infrastruktury provozovány s využitím tohoto operačního systému. Jedná se tedy o stovky zařízení. V současnosti je většina koncových bodů připojována k systému Active directory a SCCM. Systém SCCM je v rámci infrastruktury používán relativně nově – řešená infrastruktura byla historicky jedna z posledních, která v rámci celkové infrastruktury začala s implementací a využitím těchto systémů. Primární využití systému SCCM je pro hromadné instalace SW vybavení.</p> <p>Koncové body provozované mimo operační systém MS Windows, pak nejčastěji využívají Mac OS, případně některou z linuxových distribucí.</p> <p>Co se serverové části infrastruktury týče, servery a zařízení sloužící jako datová úložiště NAS jsou provozována na odpovídajících operačních systémech. Servery v klasickém smyslu pojetí jsou v řešené infrastruktuře provozovány s využitím virtualizačních platforem. Mezi nejrozšířenější patří virtualizační platforma VMware ESXi (+vSphere), případně open-source alternativa Proxmox. V rámci nadřazené infrastruktury všech lokalit je využívána ve větší míře i virtualizační platforma Hyper-V.</p> <p>Takto tvořené virtuální servery a případné minimum dedikovaných zařízení nejčastěji fungují na bázi Unixových systémů, zejména na základě distribucí CentOS nebo Debian. Celková infrastruktura navíc využívá OS Windows Server.</p>
--------------------------------	---

	<p>Co se síťových zařízení týče, tak převládají zařízení s operačním systémem IOS.</p>
Webové služby	<p>V rámci řešené infrastruktury je provozováno několik webových služeb, často se odlišujících svojí důležitostí.</p> <p>Obecně lze říct, že jedna služba využívající webové rozhraní je kritická pro všechny uživatele napříč všemi lokalitami, další webové služby jsou pak provozovány pro potřeby pouze řešené infrastruktury. Kromě možných například konfiguračních rozhraní se také často jedná o webová rozhraní zařízení provozovaných jako NAS, případně rozhraní hostované cloudové služby Nextcloud.</p> <p>V rámci celkové infrastruktury jsou pak provozovány další systémy využívající webové rozhraní – například firemní web.</p>
Služby a aplikace	<p>Další služby provozované na serverových zařízeních pak v rámci řešené infrastruktury jsou již zmiňované služby NAS zařízení pro ukládání a zálohování dat. V rámci řešené infrastruktury je také provozováno hned několik licenčních služeb poskytující licence k zakoupenému SW vybavení.</p> <p>Nadřazená celková infrastruktura pak zahrnuje i služby a provoz systému SCCM, Active directory a jeho komponenty, systém VOIP, DHCP a DNS servery, SMTP server doplněný o SPAM filtr apod.</p>
Síťová vrstva	<p>Samotná konfigurace síťových zařízení a jejich správa spadá pod nadřazené správcovské oddělení v rámci celkové infrastruktury a není v kompetenci správcovského týmu řešené lokality.</p> <p>Pro síťovou vrstvu jsou definována pravidla pro rozdělení do virtuálních lokálních sítí (VLAN), pravidla příchozí a odchozí komunikace pomocí Firewallu, směrovací pravidla pro infrastrukturu a konfigurace zabezpečení a odolnosti jednotlivých síťových prvků.</p>

Tab. 4-2 Popis prvků SW vrstvy řešené infrastruktury

4.1.4 Popis řešené infrastruktury na základě jejich uživatelů

Stejně jako v teoretických kapitolách, je možné rozdělit i uživatele přistupující k řešené infrastruktuře.

Uživatelé infrastruktury můžeme také dělit do dvou skupin a to na: **klasické uživatele a správce**.

Správcovská struktura infrastruktury má stanovenou jednoduchou hierarchii. Celková infrastruktura napříč všemi lokalitami má jeden centrální správcovský tým o 2-3 členech. Tento tým primárně zodpovídá za provoz a správnou konfiguraci síťové části infrastruktury a za chod serverů a služeb provozovaných mimo řešenou infrastrukturu a centrální správu IT operací. Každá oddělená lokalita pak má svůj vlastní správcovský tým, ten opět čítá 1-2 členy a hierarchicky spadá pod centrální správcovský tým. V kompetencích lokálního správcovského týmu pak je veškerá výpočetní technika provozována v rámci lokality. Tedy všechna zařízení spadající do stanovených kategorií a také uživatelské požadavky, realizace SW vybavenosti, servis apod. Výjimku tvoří síťová vrstva.

Z hlediska kybernetické bezpečnosti neexistuje na žádné úrovni oddělený tým, který by se problematice věnoval. Bezpečnost informací je řešena pouze na úrovni již zmíněných správcovských týmů, kdy centrální tým často jen předá doporučení, případně upozornění na hrozbu nebo problém. Samotná realizace řešení je pak řešena lokálním správcovským týmem.

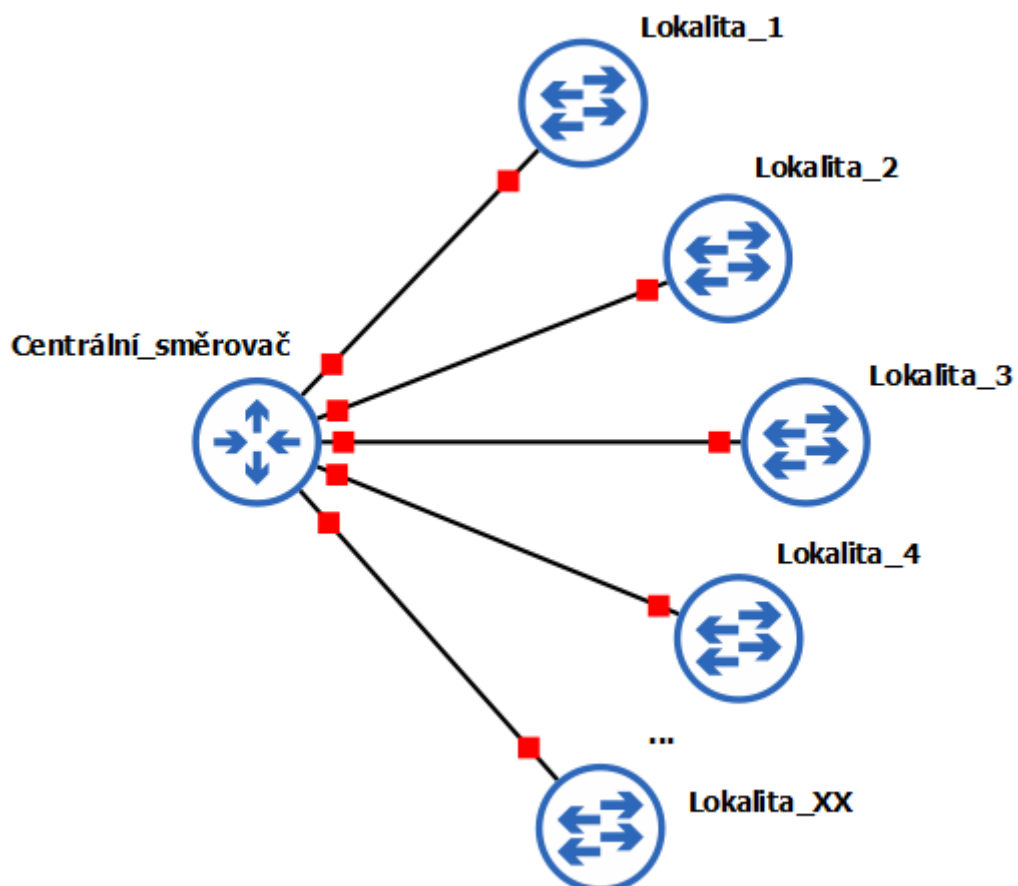
V teoretickém úvodu práce bylo zmíněno, že vzdělávací instituce často patří k nejméně podfinancovaným odvětvím z hlediska rozpočtu na IT oddělení. Z výše uvedeného je jasně patrné, že reálná situace odpovídá tomuto tvrzení. Zmiňované malé správcovské týmy nejsou schopny flexibilně reagovat na nové situace. Často dochází k situacím, kdy je problém vyřešen jen do určité míry a z důvodu časového tlaku se zaměření týmu přesune na jiný nově vzniklý problém. K tomu je nutné připočítat nároky a požadavky uživatelů, a navíc samotnou situaci ohledně kybernetické bezpečnosti. Personální stav IT oddělení, jeho hierarchie, členění činností a stanovení jasných postupů je oblast, ve které se řešená infrastruktura může a zároveň musí zlepšit, pokud chce organizace minimalizovat rizika spojená s provozem.

Druhou skupinou jsou pak klasičtí uživatelé infrastruktury, ti infrastrukturu využívají k pracovní potřebě, spoléhají na funkčnost jednotlivých prvků a dostupnost služeb. Specifické pro řešenou infrastrukturu je možnost rozdělit běžné uživatele do dvou skupin. Jednou skupinou jsou kmenoví zaměstnanci, přibližně 150 lidí. Ti většinou mají dedikovaný osobní

počítač, tedy pevně daný přístupový bod do infrastruktury ve své kanceláři, případně osobní laptop. Vzhledem k tomu, že popisovaná infrastruktura spadá pod vzdělávací instituci, druhou skupinu tvoří studenti. Velice specifické pro tuto skupinu je, že mají přístup k velkému počtu různě umístěných přístupových bodů. Další vlastností této skupiny je velký počet jejich členů, do infrastruktury takto střídavě přichází a odchází stovky uživatelů denně, v horizontu let se pak jedná o tisíce uživatelů. Tato fluktuace, široký přístup ke koncovým bodům infrastruktury a obrovský nepoměr mezi počtem správců a uživatelů, jsou další z důvodů, proč je vhodné v rámci infrastruktury implementovat monitorovací systém.

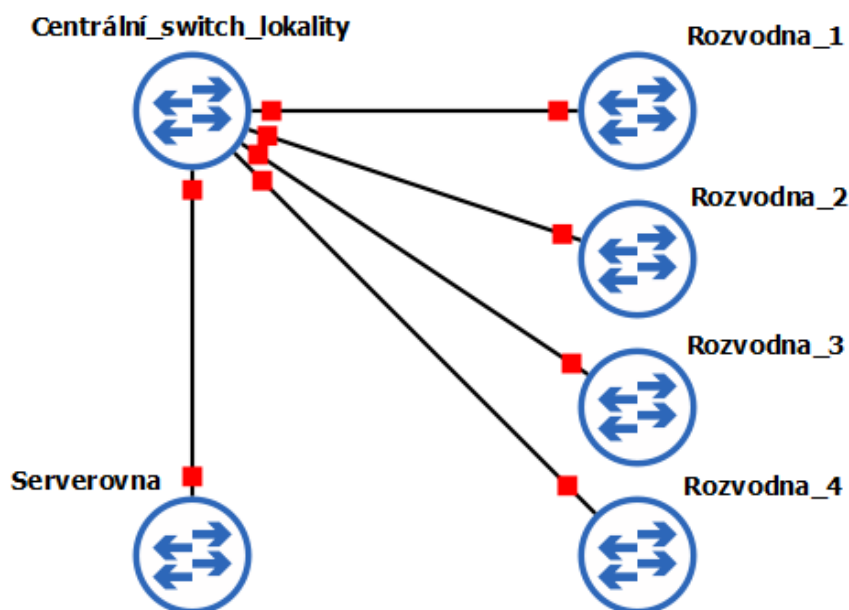
4.2 Síťová struktura řešené infrastruktury

Pro stručný popis řešené infrastruktury můžeme použít zjednodušená schémata síťového zapojení.



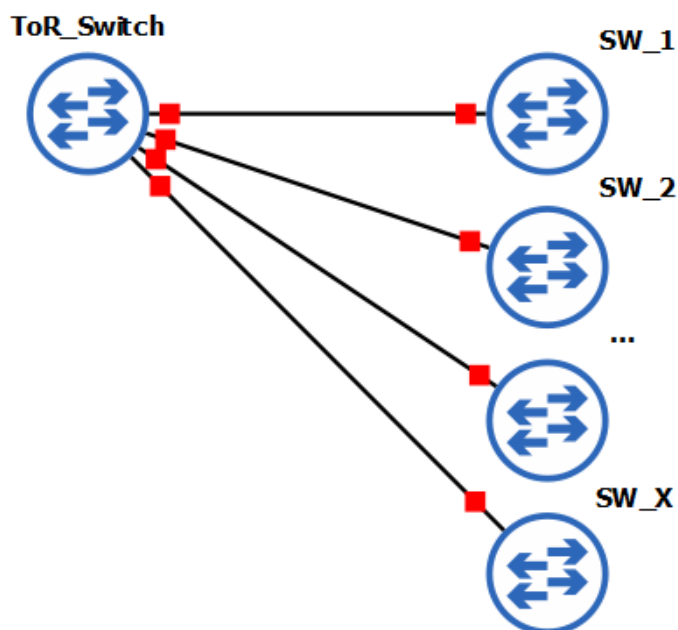
Obr. 4-1 Zjednodušené schéma propojení lokalit prostřednictvím centrálního směrovače
[zdroj vlastní]

V rámci řešené infrastruktury jedné lokality lze zjednodušené síťové schéma představit jako:



Obr. 4-2 Rozdělené řešení infrastruktury dle síťového zapojení
[zdroj vlastní]

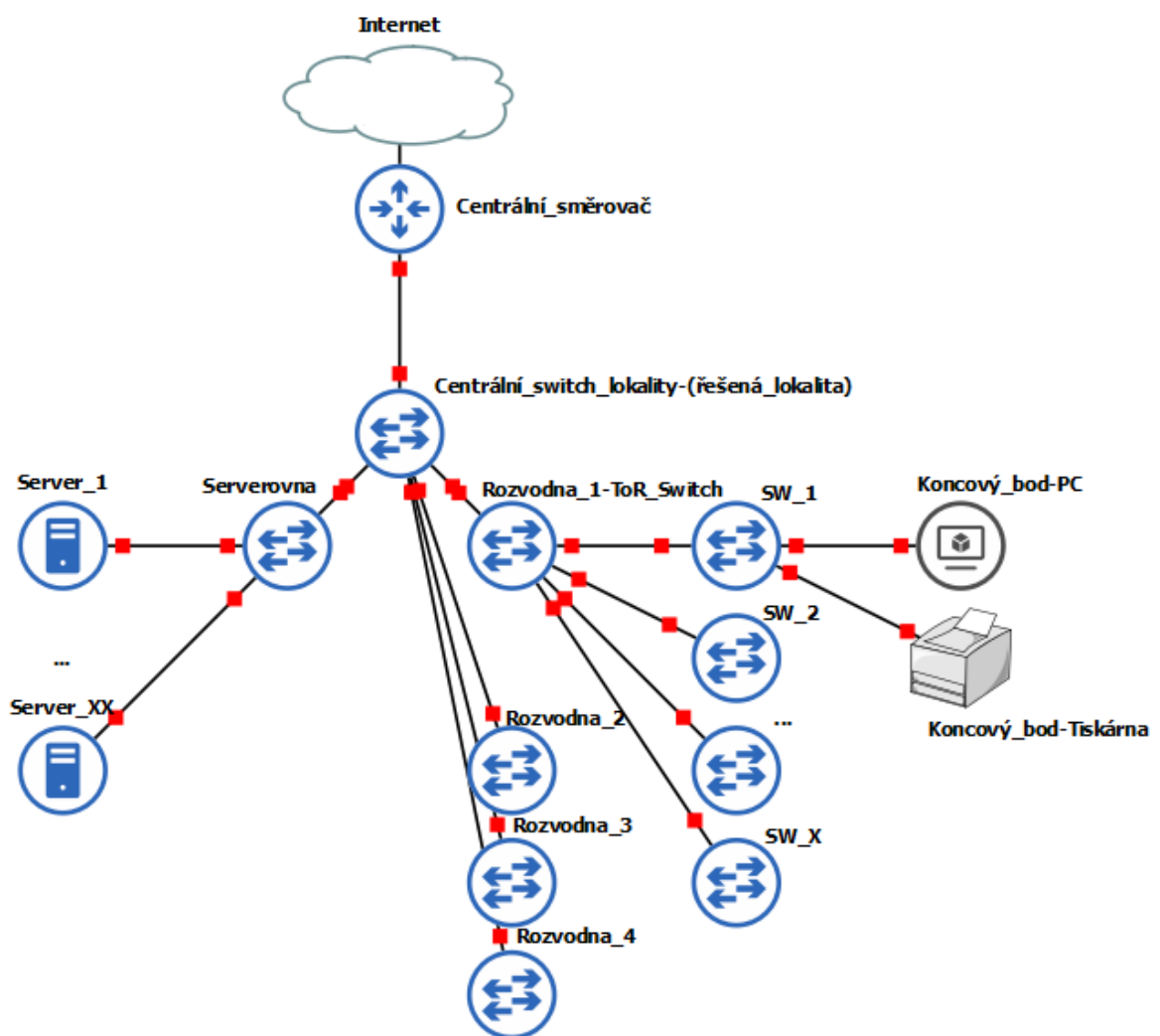
Zjednodušené schéma na Obr. 4-2 ukazuje rozdělení řešené infrastruktury z hlediska síťového zapojení. Infrastruktura disponuje jedním centrálním přepínačem (Switchem), který je optickým vláknem spojen s centrálním směrovačem. Centrální switch lokality následně poskytuje opět formou optických vláken připojení do čtyřech rozvodných místností a samotné serverovny vybudované pro řešenou lokalitu.



Obr. 4-3 Síťové zapojení v rozvodné místnosti [zdroj vlastní]

Obr. 4-3 zobrazuje propojení síťových prvků v rozvodné místnosti. Základním prvkem každé rozvodné místnosti je tzv. Top of Rack Switch (ToR Switch). Takto můžeme označit switch, který je z hlediska síťové hierarchie nejvýše postaveným prvkem v rackové skříni. Zjednodušeně se jedná o switch, který poskytuje konektivitu ostatním zařízením v rackové skříni. Do ToR switche jsou tedy připojeny ostatní switche v rozvodné místnosti. Počet připojených switchů se v rámci lokality pohybuje mezi 5-8 zařízeními. Switche připojené do ToR switche představují pomyslnou poslední vrstvu sítě, jsou přímo spojeny s přípojnými zásuvkami rozmístěnými po budově.

Vzhledem k nárůstu počtu zařízení v infrastruktuře a narůstajícím požadavkům dochází i k případům, kdy i do těchto „koncových“ switchů jsou připojena další zařízení typu switch pro navýšení počtu přípojných zásuvek. V ostatních případech jsou do internetových zásuvek, a tedy do jednotlivých portů switchů, připojena přímo jednotlivá zařízení infrastruktury.



Obr. 4-4 Zjednodušený schématický plán počítačové sítě řešené infrastruktury [zdroj vlastní]

Obr. 4-4 zjednodušeně znázorňuje schématický plán sítě infrastruktury. Je znázorněna různá povaha zařízení připojených do „koncových“ switchů v rozvodné místnosti a oddělený prostor serverovny. Pro další rozvodné místnosti by zapojení bylo takřka totožné, a proto není na plánu znázorněno.

Při implementaci monitorovacího systému je vhodné provést zmapování struktury topologie sítě. Už ze schématického plánu sítě je patrné, jaký je vztah mezi jednotlivými uzly a jaký je očekávaný tok dat.

4.3 Logická síťová struktura řešené infrastruktury

Kromě topologického rozdělení sítě je důležité řešit i logickou strukturu sítě. Tedy jakým způsobem je fyzická topologie rozdělena z hlediska jednotlivých podsítí a jaká je jejich hierarchie.

V rámci řešené infrastruktury je segregace sítě řešena primárně pomocí virtuálních lokálních sítí – VLAN. Tyto VLANy jsou vytvořeny jednak na základě fyzického umístění zařízení, nebo na základě určení zařízení. Budovu řešené infrastruktury lze rozdělit celkem na 5 křídel a pro každou podčást budovy je vytvořena oddělená VLAN. Nově jsou pak vytvořeny VLAN pro serverovnu lokality.

Z hlediska datového toku v rámci infrastruktury pak může dojít primárně ke dvěma situacím. První variantou je, že společně komunikují zařízení v rámci společné VLAN. V tomto případě komunikace odpovídá úrovni L2 modelu OSI. Taková komunikace probíhá čistě v rámci společné VLAN a je obsloužena na úrovni switchů řešené infrastruktury. Pro sledování statistik provozu (NetFlow) L2 komunikace je nutné získávat data z jednotlivých switchů. Druhou variantou pak je komunikace zařízení do jiné VLAN, do Internetu apod. V tomto případě už se nejedná o komunikaci typu L2 a datový tok je řízen nadřazeným centrálním směrovačem. Z hlediska optimalizace datového provozu to není optimální, veškerá komunikace mezi jednotlivými VLAN musí být obsloužena jedním centrálním prvkem ležícím mimo lokalitu, může docházet k přetěžování datových spojů a prodlužuje se celková doba komunikace. Na druhou stranu je pochopitelné, že vzhledem k již zmiňovanému počtu správců, by bylo obtížné zpravovat více směrovačů a konfigurovat další pravidla na desítkách síťových prvků. Pro sledování NetFlow L3 komunikace je postačující získávat data pouze z centrálního směrovače.

4.4 Identifikace kritických prvků řešené infrastruktury

Před implementací monitorovacího systému je tedy vhodné infrastrukturu postupně zmapovat a kategorizovat jednotlivá zařízení, provozovaná v rámci infrastruktury. V rámci předchozích kapitol byla zařízení infrastruktury rozřazena do kategorií a schematicky bylo zmapováno síťové zapojení.

Tyto informace nyní můžou být využité pro identifikaci významných prvků infrastruktury. U takových prvků předpokládáme, že je vhodné na ně zaměřit monitorovací systém.

Problematika identifikace těchto kritických prvků je podobně otevřená jako například již zmiňovaná problematika kategorizace provozovaných zařízení. Společně s členy laboratoře PTLAB a kolegy z univerzity jsme v souvislosti s výzkumnou činností laboratoře řešili právě problematiku selekce kritických prvků. Jmenovitě bych jako autor práce chtěl poděkovat p. Ing. Františku Sedláčkovi, který na jedné ze schůzek navrhl možnost identifikace takových prvků na základě různé míry a typu jejich důležitosti pro infrastrukturu. Navrhované kategorie můžeme shrnout jako: **Prvek kritický pro provoz infrastruktury, ekonomicky významný prvek a informačně významný prvek**. Další pomyslně oddělenou kategorií pak můžou být prvky, které jsou v infrastrukturu významné za účelem provozu služeb.

4.4.1 Prvek kritický pro provoz infrastruktury.

Do kategorie prvků kritických pro provoz infrastruktury spadají taková zařízení, která v případě výpadku omezí samotné fungování infrastruktury. Zjednodušeně můžeme říct, že výpadek prvku kritického pro fungování infrastruktury přímo ovlivní a znemožní plnohodnotné fungování dalších prvků infrastruktury.

V rámci řešené infrastruktury lokality do této kategorie nejčastěji spadají síťová zařízení. Hierarchie síťového zapojení byla stanovena v předchozích oddílech. V případě, že dojde k výpadku některého ze síťových zařízení, vždy dojde k omezení funkčnosti prvků hierarchicky podřízených nefunkčnímu zařízení. Analýza infrastruktury při řešení práce odhalila potenciální nedostatky při jejím návrhu a potenciálně nedostatečnou odolnost některých prvků.

4.4.1.1 Scénáře výpadku síťových zařízení

Scénáře výpadku síťových zařízení v rámci infrastruktury lze rozdělit na několik úrovní v závislosti na důležitosti zařízení. V následující tabulce jsou jednoduše popsány scénáře výpadku zařízení zobrazených na Obr. 4-4 a jsou seřazeny podle vzrůstající míry dopadu na infrastrukturu:

<p>Výpadek koncového switche (v obrázku označeny jako SW_1 ...)</p>	<p>V případě výpadku koncového switche dojde ke ztrátě připojení pro všechna zařízení, která jsou do switche přímo připojena. Nejčastěji se tedy jedná o pracovní stanice uživatel. V případě, že za koncovým switchem, bude umístěn další switch, dojde k nárůstu míry dopadu takového výpadku. Obecně se da říct, že dojde ke ztrátě připojení pro minimálně 20-50 zařízení.</p> <p>Pokud bude koncový switch umístěn v serverovně, může dojít ke ztrátě připojení více serverů, ztrátě dostupnosti služeb, přístupu k datům apod. To je při provozu serverů kritický problém a stav, kterému by mělo být předcházeno vhodnou strukturou sítě a redundancí síťových prvků</p> <p>Telefony systémů VOIP připojené na porty koncového switchu zároveň ztrácí kromě konektivity také zdroj napájení.</p> <p>Výsledkem výpadku koncového switchu je tedy ztráta připojení připojených zařízení.</p>
<p>Výpadek ToR switchu</p>	<p>Hierarchicky nadřazený koncovým prvkům je Top of Rack switch. Ten distribuuje připojení do sítě na jednotlivé koncové switchy.</p> <p>V případě výpadku ToR switchu dochází ke ztrátě připojení pro všechna zařízení v rackové skříni. Scénář je tedy podobný jako v přechodím případě, rozdílem je míra dopadu takového výpadku.</p> <p>Pro switchy a všechna zařízení podřazená ToR switchi dojde k výraznému omezení jejich činnosti. Zařízení ztratí možnost komunikovat do ostatních podsítí a lokalit, stejně</p>

	<p>tak komunikovat do Internetu. Dojde ke ztrátě přístupu ke službám v infrastruktuře a výraznému omezení komunikace zařízení.</p> <p>V případě zapojení pro serverovnu se prolíná charakter koncových a ToR switchů a scénář výpadku je tedy stejný jak v předchozím případě – servery připojené k vypadnutému switchi ztrácí síťovou konektivitu, dochází ke ztrátě dostupnosti služeb a dat.</p>
<p><i>Výpadek centrálního switchu lokality</i></p>	<p>Dalším hierarchickým prvkem síťového zapojení je centrální switch lokality.</p> <p>V případě výpadku centrálního switchu dochází primárně ke ztrátě připojení s centrální lokalitou, centrálním směrovačem a službami provozovanými mimo řešenou infrastrukturu. Komunikace s jinými lokalitami a komunikace do Internetu není možná, provoz lokality je omezen.</p> <p>Výpadek neovlivní provoz ostatních lokalit, dochází pouze ke ztrátě komunikace s postiženou lokalitou.</p> <p>Centrální switch lokality představuje tzv. single point of failure. Tedy prvek jehož selhání ovlivní veškerou podřízenou infrastrukturu lokality.</p>
<p><i>Výpadek centrálního směrovače</i></p>	<p>V případě kompletního výpadku centrálního směrovače v nadřazené infrastruktuře dochází k totálnímu rozpadu síťové komunikace, provozované služby jsou nedostupné, je omezena veškerá možná komunikace a webové služby.</p> <p>Scénář kompletního výpadku centrálního směrovače lze označit jako nejzávažnější možný problém infrastruktury. Hlavním cílem by mělo být vhodně zajistit zařízení proti výpadku. Například s využitím redundance zařízení apod. Hrozbě ztráty tohoto prvku je nutné předcházet.</p>

Tab. 4-3 Scénáře provozního výpadku síťových zařízení řešené infrastruktury

Obecně výpadky síťových zařízení vedou ke ztrátě konektivity v rámci infrastruktury a s vnějším světem. Výpadky se podle charakteru liší mírou svého dopadu, celkově je ale stav síťového výpadku pro infrastrukturu kritický a zamezuje jejímu plnému fungování. V současnosti je kritičnost síťového připojení důležitá i pro realizaci distanční výuky nebo případnou práci zaměstnanců z domova. Zároveň je připojení nezbytné pro správné fungování systémů Active directory a doménového přihlášení, případně systému SCCM. Ztráta připojení k serverům AD může vést k zamezení přihlášení doménovým účtem, ztrátě přístupu k definovaným systémovým politikám apod.

4.4.1.2 Provozní výpadky ostatních zařízení

Pro fungování infrastruktury samozřejmě nejsou kritická pouze zařízení síťové infrastruktury. V řešené infrastruktuře se vyskytují i zařízení jiné povahy, zejména servery, kritické pro provoz infrastruktury.

Podobně jako v předchozím případě můžeme stanovit scénáře výpadku vybraných zařízení s tím rozdílem, že nyní už není možné tabulku brát jako seřazenou dle míry dopadu, míra dopadu jednotlivých zařízení se může lišit v závislosti na okolnostech.

Servery	<p>Provozním výpadkem serverů uvažujeme stav, kdy nedojde k výpadku provozovaného SW na zařízení, ale k fyzickému výpadku samotného serverového zařízení. Výpadek provozně kritického serveru přímo omezí nebo zamezí správnému fungování jiných prvků infrastruktury.</p> <p>Při výpadku zařízení, která slouží jako uzly pro hypervisory virtualizačních technologií, může dojít k výraznému omezení provozovaných virtuálních zařízení, případně až ke ztrátě jejich dostupnosti.</p> <p>Na fyzických zařízeních také může být provozováno množství služeb nebo jiných aplikací a v případě ztráty fyzického zařízení dochází ke ztrátě veškerého provozovaného SW, stejně tak ve zmiňovaném případě omezení provozu virtuálních zařízení.</p> <p>V případě výpadku diskového pole může dojít ke ztrátě dat, nebo ke kaskádovému výpadku navázaných služeb.</p>
----------------	--

	<p>V případě nadřazené infrastruktury by při nejhorším scénáři mohlo dojít ke ztrátě služeb jako Active Directory nebo SCCM. Potenciální výpadky těchto služeb mají stejné následky jako v případě ztráty síťové konektivity, může dojít k zamezení ověření doménových účtů, nedochází k aplikaci GPO. Pomocí systému SCCM nebude možná vzdálená distribuce SW vybavení apod.</p> <p>Mezi další provozní servery můžeme zařadit servery DHCP, nebo DNS, SMTP server pro realizaci mailových služeb, nebo fileserver a printserver. Výpadky těchto serverů opět omezí fungování infrastruktury jako celku, bude docházet k chybám v síťové komunikaci, ztrátě mailových služeb nebo omezení možnosti přístupu k souborům a tisku.</p>
<p><i>Správcovské stanice</i></p>	<p>Správci infrastruktur využívají pro správu infrastruktury dedikované koncové uzly. Primárně v podobě osobních počítačů nebo v podobě virtuálních stanic.</p> <p>V případě ztráty uvedených zařízení dochází k razantnímu omezení rozsahu činnosti správce. Velká část správcovských nástrojů je dostupná pouze z takto dedikovaných zařízení. Správci pak nejsou schopni provádět zásahy a servis infrastruktury, reagovat na změny a pracovní efektivita je značně omezena.</p>
<p><i>Uživatelské stanice, ostatní koncové prvky</i></p>	<p>Výpadky uživatelských stanic, případně ostatních koncových prvků – např. tiskárny, telefony, jsou z provozního hlediska pro infrastrukturu nejméně kritické.</p> <p>To však neznamená, že v rámci infrastruktury nejsou podstatné. Koncové prvky jsou nejpočetnější skupinou zařízení a zároveň představují přímé přístupové body do infrastruktury.</p> <p>V případě výpadku koncového zařízení dochází zejména k omezení pracovní činnosti postihnutého zaměstnance, případně k zamezení práce na zařízení. Horším scénářem je výpadek pracovní stanice členů vyššího managementu a ztráta nezálohovaných dat.</p> <p>Výpadek ostatních koncových prvků – jako tiskárna / telefon zpravidla omezuje spíše uživatelský komfort a ne infrastrukturu.</p>

Tab. 4-4 Scénáře provozního výpadku ostatních zařízení infrastruktury

4.4.2 Prvky ekonomicky významné pro infrastrukturu

Na problematiku identifikace ekonomicky významných prvků lze opět pohlížet z více úhlů pohledu. V infrastrukturách, jejichž primárním cílem je generovat zisk, bude identifikace ekonomicky významných prvků probíhá mírně odlišně. V takové infrastruktuře se budou ekonomicky významné prvky částečně prolínat s kategorií provozně kritických prvků – v případě jejich ztráty by došlo k výpadku části infrastruktury, což povede k ekonomické ztrátě.

V rámci řešené infrastruktury není primárním cílem generovat zisk ve smyslu provozu výrobních linek, uzavírání transakcí apod. Kritériem pro identifikaci ekonomicky významných prvků v rámci řešené infrastruktury je odhadovaná škoda způsobena ztrátou zařízení. Základním předpokladem je, že zařízení, nebo jeho komponenta bude trvale vyřazena z provozu.

Obecně může ke ztrátě zařízení dojít vlivem opotřebení a stáří zařízení. Další možností může být včasné neodhalení vznikající poruchy – například kaskádová porucha diskového pole. Postupně vzniká více nepoužitelných sektorů, dochází k postupnému přetěžování ostatních disků, což může vést k postupnému selhání a kompletní ztrátě integrity diskového pole. Dalším případem může být dlouhodobé přetížení zařízení, výpadek chlazení – trvalé poškození chipů a komponent. Posledním případem může být úmyslné zničení při kybernetickém útoku.

Pro stanovení ekonomických dopadů můžeme použít kategorie stanovené při identifikaci provozně kritických prvků.

<i>Sít'ová zařízení</i>	Při ztrátě síťových zařízení vznikne infrastruktura odhadovaná škoda cca 80–100 tis. Kč za zařízení. Samozřejmě se cena může pohybovat na základě aktuálních podmínek trhu.
<i>Servery</i>	<p>V případě ztráty některého ze serverů nebo datových polí vznikne kromě zmiňovaných provozních ztrát a komplikací, také ztráta finanční. Cena serverů v rámci infrastruktury se pohybuje v řádech stovek tisíců, některá zařízení cenou mohou dosahovat i řádu milionů.</p> <p>Vzhledem k omezenému rozpočtu na IT infrastrukturu a vysoké ceně zařízení, může být ztráta těchto zařízení pro infrastrukturu kritická. K situaci navíc bude nutné přidat ekonomické dopady spojené se ztrátou dat apod., potenciální finanční náročnost tohoto problému byla představena v teoretické části práce.</p>
<i>Ostatní koncové body</i>	<p>U ostatních prvků infrastruktury lze obecně předpokládat, že finanční ztráty a nutná cena na obnovu zařízení nebude dosahovat stejných cifer jako v předchozích případech.</p> <p>Samozřejmě i v kategorii uživatelských stanic existují výjimky dosahující cenou řády vyšších desítek tisíc, dále je nutné uvažovat opět potenciální ztráty spojené se ztrátou dat z pracovních stanic.</p> <p>Za předpokladu, že nedojde ke ztrátě izolovaného stroje, ale dojde k hromadnému poškození pracovních stanic, hrozí, že náklady na obnovu budou v řádech milionů a ekonomické dopady pro infrastrukturu potenciálně budou horší než v předchozích dvou případech.</p>

Tab. 4-5 Popis identifikovaných ekonomicky významných prvků

4.4.3 Prvky informačně významné pro infrastrukturu

Posledním kritériem pro identifikaci kritických prvků může být informační významnost prvku infrastruktury.

Informační významnost můžeme opět klasifikovat ve dvou různých oblastech. Je nutné oddělit významnost/citlivost informací a dat, které se v rámci prvků infrastruktury pohybují a zároveň i datový tok v rámci infrastruktury.

Z hlediska významnosti informací spadají do kategorie v rámci řešené infrastruktury primárně servery a pracovní stanice uživatelů.

V rámci řešené infrastruktury existuje server, který na základě digitální identity uživatelů synchronizuje uživatelské účty. V případě narušení bezpečnosti takového serveru může dojít k úniku osobních dat uživatelů, přístupových údajů a tím narušení integrity celkové infrastruktury.

Datová úložiště v rámci infrastruktury mohou a jsou používána pro zálohování pracovních výsledků výzkumných týmů, sdílení materiálů, na serverech dochází k provádění simulací apod. Každá kompromitace a ztráta takových dat může být pro infrastrukturu a její uživatele zdrojem komplikací, vézt ke ztrátě pracovních výsledků apod.

V rámci nadřazené infrastruktury jsou také provozovány tzv. informačně významné systémy. Pro ty obzvláště platí nutnost velmi zodpovědné práce s daty uživatel a případná ztráta osobních údajů představuje pro uživatele infrastruktury obrovský problém. Zároveň se jedná z hlediska GDPR i o vážný problém organizace.

Co se osobních stanic týká, záleží citlivost dostupných informací na povaze a určení konkrétních zařízení. V případě, že by napadené zařízení náleželo zaměstnanci vyššího managementu nebo některého z organizačních oddělení, může opět dojít ke ztrátě vysoce citlivých dat. Tato data mohou opět spadat pod GDPR, může se jednat o finanční rozvahy, interní dokumenty, strategické plány, informace o výplatách zaměstnanců apod.

U dalších pracovních stanic opět může dojít ke ztrátě významných pracovních výsledků. Pracovní stanice může být propojena s citlivou laboratorní technikou, případně s prostředím, které může být zdraví nebezpečné. Získání přístupu k datům, případně ovládacím prvkům může vyústit v kritický problém, který může přinést i ekonomické dopady.

Jako další informačně významné uzly mohou být označeny již zmiňované správcovské stanice. Skrz ně by útočník mohl získat přístup k administrativním nástrojům infrastruktury. To může vést ke vzniku dalších škod a případných ztrát dat v infrastruktuře.

Z hlediska informační významnosti z pohledu datového toku jsou opět významná síťová zařízení infrastruktury. Podobně, jak byla síťová zařízení seřazena z hlediska problematiky jejich výpadků, je možné síťová zařízení seřadit na základě vzrůstajícího datového toku od koncových switchů směrem k centrálnímu směrovači. Při práci s informační významností síťových prvků se identifikují prvky, které je vhodné sledovat z hlediska síťového provozu, který tyto prvky musí obsloužit. V případě, že útočník bude schopný získat administrátorský přístup k některému ze síťových zařízení, může docházet k zachytávání síťové komunikace infrastruktury.

Největší dopad z hlediska možného úniku informací infrastruktury by opět byl centrální switch lokality, případně samotný centrální směrovač kompletní infrastruktury. Další oblastí pro potenciální odposlech komunikace je bezdrátová síť v rámci lokality.

4.4.4 Významná zařízení infrastruktury

Do kategorie významných zařízení v rámci řešené infrastruktury pak zahrnujeme zařízení, která provozují významné služby nebo aplikace, které jsou v rámci infrastruktury využívány. Výpadek těchto zařízení nutně nevede k vyřazení dalších prvků, spíše dochází ke snížení uživatelského komfortu, ztrátě přístupu k uloženým datům, některé aplikace mohou přestat fungovat.

Zjednodušeně tedy můžeme říct, že takto významná zařízení jsou potřebná pro umožnění vykonávání pracovní činnosti. V rámci řešené infrastruktury můžeme zařadit systémy využívané pro elektronickou podporu výuky, lokální verzovací systém, lokálně provozované cloudy pro potřeby uživatelů. Další významné systémy pak jednoznačně tvoří licenční servery. Na jejich funkčnosti závisí možnost využívat zakoupené SW aplikace v rámci infrastruktury.

Už z povahy zařízení je patrné, že popisované kategorie zařízení a jejich význam pro infrastrukturu se vzájemně prolínají. Zařízení může být významné pro uživatele infrastruktury, protože provozuje důležité služby – např. licenční server, ale zároveň může spadat do kategorie informačně kritických prvků. V případě cizího přístupu k zařízení může dojít k odcizení licenčních informací apod.

Před samotnou implementací monitorovacího systému je tedy vhodné obdobným způsobem provést analýzu infrastruktury, pro kterou má být monitorovací systém tvořen. Je žádoucí

takto stanovit prvky, které jsou pro infrastrukturu významné a na takové prvky primárně zaměřit úsilí při požadavcích a následné implementaci monitorovacího systému. Zároveň je vhodné stanovit síťové schéma infrastruktury, stanovit předpokládaný datový tok, ověřit konfiguraci sítě. Pro monitorovací systém je podstatné, aby monitorované prvky mohly v rámci sítě komunikovat s řídicím serverem. Z hlediska optimalizace datového toku je naopak důležité, aby monitorovací systém byl navržen tak, aby generoval minimální síťový provoz v rámci infrastruktury a zatěžoval minimum síťových prvků.

5 NÁVRH IMPLEMENTACE MONITOROVACÍHO SYSTÉMU

Předchozí kapitola popisuje infrastrukturu, pro kterou má být implementován monitorovací systém. Základem pro návrh a volbu řešení bylo zmapování infrastruktury, identifikace jednotlivých prvků a stanovení hierarchie a důležitosti jednotlivých zařízení.

Dalším krokem nutným pro návrh monitorovacího systému je identifikace požadavků na monitorovací systém, stanovení cílů a přínosů. V další řadě je nutné uvědomit si, jaké prvky se v infrastruktuře nacházejí a jakým způsobem je chceme monitorovat. Jinými slovy, jaké komunikační protokoly musí být s monitorovacím systémem kompatibilní, případně jaká zařízení budou monitorována.

5.1 Požadavky na navrhovaný monitorovací systém

Cílem práce je navrhnout systém monitoringu pro řešenou infrastrukturu. Jeho účelem by mělo být získávat data o provozním stavu zařízení, získávat informace z logů zařízení a mít možnost zpracovat získaná data pomocí vytvořených pravidel. Pravidla by měla být realizovatelná tak, ať jsou schopna odhalit potenciální problém z hlediska provozu zařízení, nebo kybernetické bezpečnosti. V kapitole 2 byly teoreticky popsány přístupy k samotnému monitoringu, možný charakter dat apod. V následující kapitole 3 byla zmíněna některá dostupná řešení, která je možné použít pro monitoring IT infrastruktur.

Při volbě řešení pro implementaci v rámci řešené infrastruktury byly podstatné 3 hlavní požadavky – **škálovatelnost, open-source a kompatibilita**:

<i>Open-source</i>	<p>V předchozích kapitolách byl zmiňován omezený rozpočet pro provoz IT infrastruktury. Ať už v rámci řešené infrastruktury jedné lokality, nebo celkové infrastruktury instituce.</p> <p>Z přehledu dostupných řešení je patrné, že pořizovací cena systémů z pravidla bývá vysoká. Implementované řešení musí být zvoleno ze systémů, které jsou dostupné v režimu open-source, s možností komerčního nasazení. Faktem je, že open-source systémy mohou být náročnější při implementaci a provozu. I následná údržba systému více spoléhá na schopnosti správců infrastruktury. Požadavky na finanční omezení zde převažují nad potenciálními komplikacemi při implementaci.</p>
---------------------------	--

<i>Škálovatelnost</i>	<p>Druhým požadavkem na implementovatelné řešení je jeho škálovatelnost. Z hlediska řešené infrastruktury bylo zmíněno, že se do budoucna dá očekávat další nárůst v počtu připojených zařízení. Z toho důvodu je nutno, aby navržené řešení bylo do budoucna rozšiřitelné.</p> <p>Zároveň lze předpokládat, že v případě implementace řešení na základě této práce, bude dalším cílem rozšířit monitorovací systém do dalších lokalit infrastruktury. To opět vyžaduje, aby navrhovaný systém byl modifikovatelný a rozšiřitelný.</p>
<i>Kompatibilita</i>	<p>Posledním z hlavních požadavků je nutná kompatibilita se systémy infrastruktury. Tato vlastnost je nutná pro jakékoliv navrhované řešení. V rámci řešené infrastruktury musí navrhované řešení být kompatibilní se systémy na bázi OS Windows a Unix/Linux. Dalšími zařízení, ze kterých v rámci řešené infrastruktury mají být získávána data jsou síťová zařízení využívající komunikační protokoly SNMP, případně virtualizační platformy VMware nebo Hyper-V. U těch lze předpokládat potřebu využít opět komunikační protokol SNMP, potenciální přímou kompatibilitu s monitorovacím systémem a u vybraných zařízení možnost využít rozhraní IPMI.</p>

Tab. 5-1 Souhrn požadavků na návrh řešení

5.2 Volba řešení pro implementaci

Při rešeršní přípravě k práci byla porovnána vybraná řešení monitorovacích systémů (Kapitola 3). Na základě stanovených požadavků z předchozí podkapitoly 5.1 zůstaly pro možnost volby celkem 4 možnosti: **Elastic Stack**, **Nagios Core**, **Prometheus** a **Zabbix**. Ostatní řešení jsou zpoplatněná, a proto nejsou vhodná pro řešenou infrastrukturu

Po dalším srovnání výše uvedených možností, byl pro návrh systému a implementaci v rámci testovací infrastruktury zvolen monitorovací systém Zabbix.

Zabbix je plně bezplatnou možností mezi monitorovacími systémy a oproti konkurenčním řešením nabízí, i přes tuto skutečnost, velice komplexní řešení monitoringu, které není nijak uměle omezeno.

Na rozdíl od ostatních řešení Zabbix nabízí možnost konfigurace systému s využitím prostředí webového rozhraní a konfiguraci není nutné vytvářet editováním konfiguračních souborů. Zároveň Zabbix poskytuje rozsáhlé možnosti způsobů monitoringu. Formou volně dostupného agenta⁷ plně pokrývá možnosti agent monitoringu pro následující platformy [54]:

- Linux/Unix
- Windows – desktop i server (min. v XP)
- Mac OS X
- HP-UX
- Solaris: 9 - 11
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD

Pro zařízení mimo uvedené platformy, např. síťová zařízení, pak Zabbix široce pokrývá možnosti agent-less monitoringu. Je možné využít protokolu SNMP, rozhraní IPMI u serverových zařízení, přímou kompatibilitu se systémem VMware, protokoly SSH a Telnet, pro operační systémy Windows lze přes Zabbix agenta využít dotazy WMI.

Kromě četných způsobů získání dat nabízí Zabbix zároveň integrované možnosti jejich zpracování. Lze tvořit grafické vizualizace získaných dat, systém také umožňuje vytvářet vlastní pravidla pro tvorbu upozornění na vzniklý stav zařízení a infrastruktury. Následná upozornění je možné předávat správcům nejen prostřednictvím systému Zabbix, ale také některým z podporovaných komunikačních kanálů (Např. SMS, e-mail, Slack, Discord apod.).

Z hlediska nastavení monitorovacího systému je situace značně usnadněna přehledným webovým rozhraním a konfigurace jednotlivých kroků není náročná. Další silnou stránkou systému Zabbix v oblasti konfigurace je velmi kvalitně zpracovaná dokumentace a aktivní komunita uživatelů. Tým podpory systému Zabbix je obecně považován za velice aktivní i v případě využívání verze bez zaplacené podpory. Na svých stránkách Zabbix BLOG [55] pravidelně zveřejňují články, ve kterých popisují možnosti práce se systémem Zabbix, scénáře použití a novinky v rámci platformy.

Silným aspektem systému Zabbix je tedy jeho ucelenost. Veškeré nástroje pro monitoring zařízení jsou zahrnuty v rámci jedné platformy, je dostupné webové rozhraní, existují možnosti grafických vizualizací, je podporována tvorba upozornění, a existuje celá řada způsobů získání dat. Samotná konfigurace je relativně snadná.

⁷ Existují 2 verze Zabbix agenta, popisovaná kompatibilita je pokryta jejich kombinací, obě verze jsou plně funkční se systémem Zabbix

5.3 Možnosti integrace systému Zabbix pro řešenou infrastrukturu

Součástí návrhu monitorovacího systému pro řešenou infrastrukturu je představení možností jeho integrace do stávajícího stavu infrastruktury. Přístupů k integraci může být více a v rámci této kapitoly bude doporučen nejvhodnější postup integrace, jehož cílem je použít systém Zabbix dle platných doporučení a s ohledem na budoucí udržitelnost.

5.3.1.1 Hlavní komponenty systému Zabbix

Monitorovací systém Zabbix se skládá z několika hlavních SW komponent. Kritické pro úspěšné zprovoznění systému jsou: **Zabbix server, webové rozhraní a databáze pro ukládání dat.**

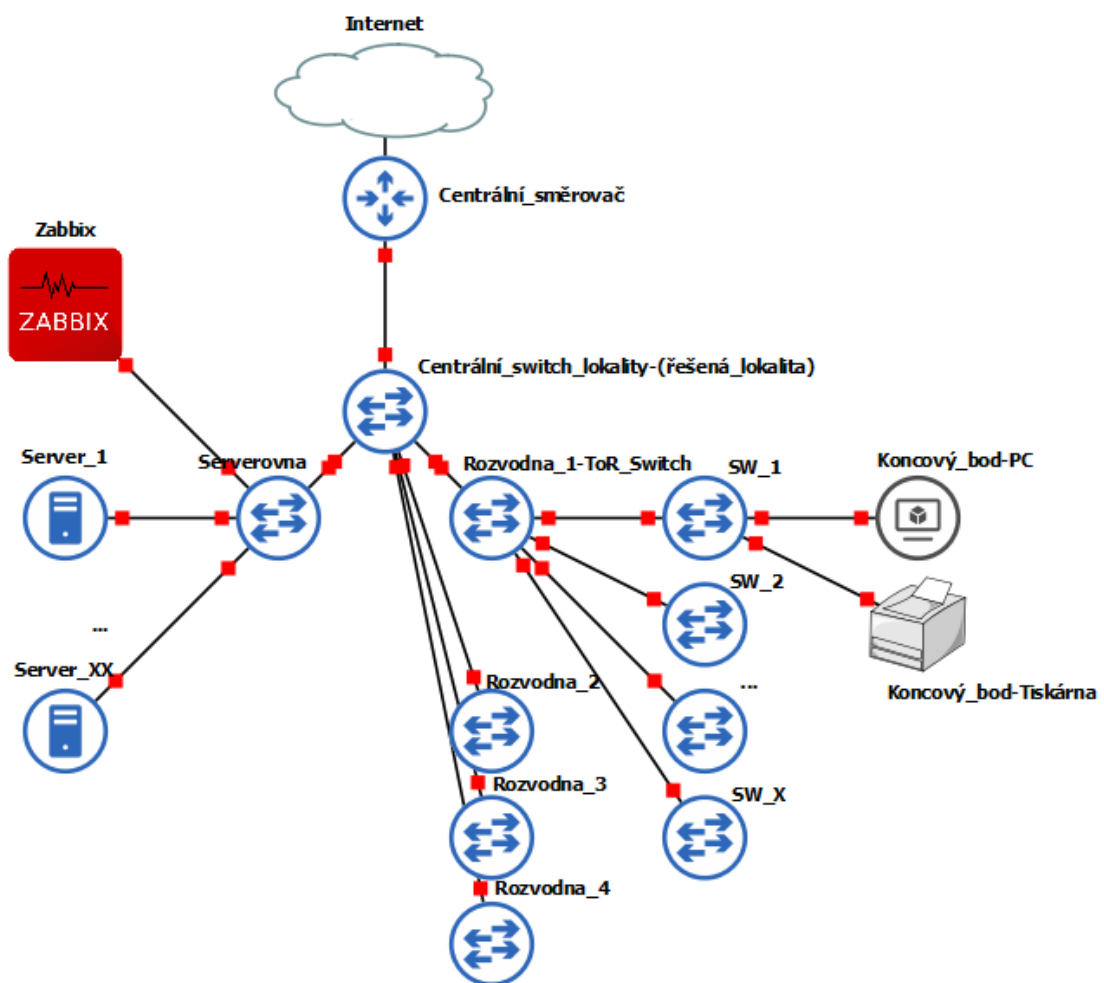
Funkce jednotlivých komponent lze jednoduše shrnout:

Zabbix server	<p>Zabbix server je hlavní back-endová komponenta monitorovacího systému. Server realizuje sběr informací z monitorovaných prvků a následné zpracování a ukládání získaných dat. Při zpracování dat je server zodpovědný za vyhodnocování nastavených pravidel, odesílání upozornění a přípravu dat pro grafické vizualizace.</p> <p>Server také řídí ukládání dat a konfigurace systému do poskytnuté databáze.</p> <p>Limitací platformy Zabbix je nemožnost provozovat Zabbix server na platformě Windows [56].</p>
Webové rozhraní	<p>Druhou komponentou platformy je již zmiňované webové rozhraní. Jedná se o front-end prostředí celého systému. Pomocí webového rozhraní lze plně konfigurovat proces monitoringu infrastruktury, procházet získaná data a grafické vizualizace.</p> <p>Webové rozhraní je napsáno v jazyce PHP a jeho provoz je tedy limitovaný pouze nutností kompatibilního webserveru. Nejčastějším přístupem je instalace webového rozhraní na stejném zařízení jako Zabbix server [57].</p>

Databáze	<p>Poslední komponentou systému je odpovídající databázové úložiště. Databáze je využívána pro ukládání dat získaných v rámci monitoringu a zároveň pro uložení konfigurace monitorovacího systému.</p> <p>Kompletní seznam podporovaných databázových serverů je opět dostupný v dokumentaci, nejvíce doporučované databázové servery pro využití se systémem Zabbix jsou: MySQL a PostgreSQL [58].</p>
-----------------	--

Tab. 5-2 Popis komponent monitorovacího systému Zabbix

Nejjednodušším řešením integrace do řešené infrastruktury tedy je vyhradit potřebný výpočetní výkon a provést instalaci výše uvedených komponent a následně vytvořit funkční instanci systému Zabbix:



Obr. 5-1 Prvotní návrh implementace monitorovacího serveru do infrastruktury [zdroj vlastní]

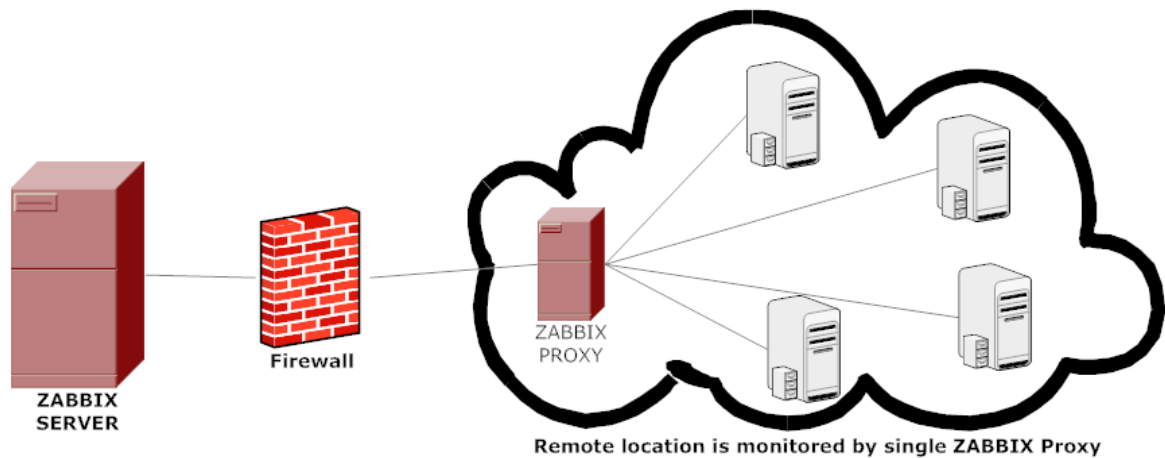
Řešení znázorněné na Obr. 5-1 je implementačně nejjednodušší. Existuje jedna instance serveru, databáze a webového rozhraní. Na server se postupně připojí jednotlivé prvky řešené infrastruktury a bude docházet ke sběru dat.

Na druhou stranu s sebou tato metoda implementace přináší hned několik problémů. V první řadě je nutné uvažovat nad vytížením samotného Zabbix serveru při obsluze jednotlivých požadavků. Víme, že v infrastruktuře budou monitorovány stovky zařízení, případné rozšíření na celou infrastrukturu instituce zvedne tento počet řádově na tisíce zařízení. Server následně musí současně obsluhovat síťovou komunikaci s jednotlivými prvky, datovou režii při práci s databází a samotné zpracování dat v rámci vytvořených pravidel a vizualizací. Tímto způsobem může dojít k postupnému přetěžování serveru, neúplnému zpracování jednotlivých požadavků, ztrátě dat apod.

Druhým problémem této implementace je vzniklý síťový provoz v rámci infrastruktury. Zabbix server bude muset mít přístup ke všem prvkům infrastruktury. Víme, že infrastruktura je dělená na jednotlivé podsítě a směrování mezi nimi provádí centrální směrovač. Bude tedy nutné umožnit komunikaci mezi všemi prvky podsítí a serverem Zabbixu na požadovaných síťových protokolech. Zároveň komunikace prvků bude vytvářet zátěž na centrálním směrovači. Problém bude opět pouze umocňován postupným rozšiřováním na další prvky infrastruktury.

Z těchto důvodů nelze tento přístup k integraci označit za vhodný. Řešením výše uvedených problémů je využití další použitelné SW komponenty – tzv. Zabbix proxy.

Využití Zabbix proxy není pro úspěšné zprovoznění systému nutné, je však velmi výhodné. Proxy lze nejjednodušeji popsat jako oddělený kolektor dat z monitorovaných prvků. Podobně jako server potřebuje každá instance proxy své databázové úložiště. Činnost proxy pak částečně odpovídá Zabbix serveru, proxy také zodpovídá za komunikaci s monitorovanými prvky a řídí unifikaci a korektní ukládání získaných dat. Rozdílem je, že získaná data jsou lokálně ukládána v databázích jednotlivých proxy a následně už v korektním tvaru předávána Zabbix serveru. Zabbix server takto získává předpřipravená data pro vyhodnocení. Hlavním přínosem použití proxy je distribuce zátěže mezi více prvky, kdy server zodpovídá primárně za zpracování získaných dat a není přetěžován obsluhou komunikace s prvky infrastruktury.

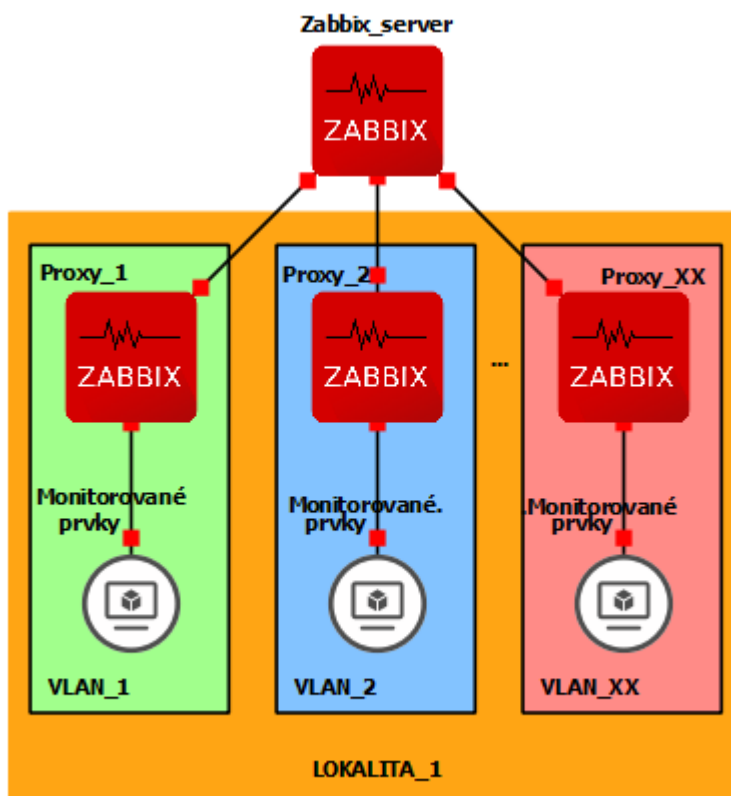


Obr. 5-2 Schéma využití Zabbix proxy [59]

Mezi hlavní způsoby využití proxy patří právě monitorování oddělených podsítí, případně monitorování oddělených lokalit infrastruktury. Také jak je z Obr. 5-2 patrné, dojde také k usnadnění konfigurace pravidel síťového provozu. Umístěním proxy do stejné podsítě jako monitorované prvky dojde k eliminaci většiny zátěže na centrální směrovač – proxy a monitorované prvky komunikují v rámci L2 vrstvy modelu OSI a provoz vzniká pouze lokálně. Pro Zabbix server následně musí být viditelné pouze jednotlivé proxy a v rámci sítě je nutné povolit pouze tuto komunikaci. Nevýhodou tohoto řešení je nutnost instalace a údržby více instancí proxy + databáze.

5.3.1.2 Navrhovaný přístup k nasazení systému Zabbix pro řešenou infrastrukturu

Na základě znalostí struktury infrastruktury získané předchozí analýzou a vlastnostmi systému Zabbix je možné stanovit nejlepší způsob implementace systému pro řešenou infrastrukturu:



Obr. 5-3 Princip doporučené implementace systému Zabbix pro infrastrukturu [zdroj vlastní]

Obr. 5-3 schematicky zobrazuje optimální rozmístění jednotlivých komponent monitorovacího systému. Víme, že řešená lokalita je rozdělena na virtuální podsítě, které z pravidla čítají desítky zařízení, síťová zařízení se také nacházejí v oddělené podsíti. Nejlepším přístupem k zabezpečení monitoringu infrastruktury je instalace centrální instance Zabbix serveru + webového rozhraní + databáze. A následně v rámci každé virtuální sítě vytvořit jednu instanci Zabbix proxy + databáze. Prvky nacházející se v rámci jednotlivých podsítí jsou monitorovány příslušnou proxy, která předává data pro zpracování do hlavního serveru.

Tímto způsobem je zajištěna minimalizace odchozího síťového provozu infrastruktury, většina komunikace probíhá lokálně mezi prvky a příslušnou proxy. Konfigurace FW hlavního serveru musí obsahovat pouze komunikaci s jednotlivými proxy, samotný server neprovádí

monitoring koncových prvků. Jediné prvky, které centrální server může sledovat jsou jednotlivé proxy, ovšem i to není nutné – jednotlivé proxy můžou být nakonfigurovány tak, aby sledovaly samy sebe a pouze předávala data na hlavní server.

Konfigurace systému probíhá prostřednictvím centrálního serveru a jeho webové rozhraní, jednotlivé proxy si v časových intervalech načítají potřebnou konfiguraci. V případě výpadku některé z proxy nedochází ke ztrátě již získaných dat, ta jsou primárně ukládána v hlavní databázi serveru.

Při nasazování monitorovacího systému může vzniknout požadavek na zvýšenou odolnost samotného Zabbix serveru. Nejčastěji v kritických infrastrukturách není možné, aby docházelo k výpadkům hlavního serveru. Proto je možné centrální server instalovat jako tzv. high availability cluster.

V tomto režimu dojde k instalaci několika instancí Zabbix serveru. Při instalaci jsou jednotlivé instance serveru konfigurovány jako uzly clusteru. Následně existuje jeden aktivní server a X uzlů připravených k použití. Instance serverů spolu sdílí společnou databázi a konfigurační rozhraní zůstává stejné. Nastavení jednotlivých proxy pak musí zahrnovat adresy všech uzlů clusteru. V případě výpadku aktivního serveru dochází k aktivaci některého z připravených uzlů. High availability cluster řeší pouze replikaci a tím případný výpadek jen u Zabbix serveru, ostatní komponenty jako DB, web rozhraní nebo proxy jsou stále náchylné k výpadku.

Pokud bude požadavek replikovat všechny komponenty, je lepší zvolit řešení třetích stran určená pro tvorbu clusterů a vytvořit vlastní high availability cluster pro jednotlivé komponenty monitorovacího systému.

Distribuováním operace sledování jednotlivých prvků na oddělené proxy je zároveň zajištěna rozšiřitelnost celého řešení. V případě vzniku další podsítě lze pouze přidat další proxy a navázat k ní nové prvky. Stejně tak systém může být postupně rozšířen v ostatních lokalitách infrastruktury. Zátěž na výpočetní výkon je rozdělena mezi jednotlivé proxy a získaná data jsou sjednocena v rámci centrálního serveru kde jsou zpracována, nedochází tedy k tříštění řešení.

5.4 Instalace systému Zabbix v testovací infrastruktuře

V předchozích oddílech kapitoly byl popsán proces selekce řešení a následného návrhu struktury monitorovacího systému pro řešenou infrastrukturu. Dalšími cíli práce je provést implementaci a zkušební provoz v rámci testovací infrastruktury. Následující kapitola zároveň popíše možné scénáře použití monitorovacího systému tak, aby čtenáři práce byli po přečtení schopni uchopit problematiku monitoringu pro vlastní infrastrukturu.

Poslední část kapitoly popisující integraci systému Zabbix je ukázkou instalace systému v testovací infrastruktuře. Proces instalace následně může být použit při finální implementaci řešení do infrastruktury.

Jak již bylo popsáno, pro zprovoznění systému Zabbix budou nutné následující komponenty: Zabbix server, webové rozhraní, Zabbix proxy a jejich příslušný počet databázových uložišť. V rámci demonstrační instalace bude z důvodu omezení pracovního prostoru instalována pouze jedna proxy a jedna instance Zabbix serveru.

5.4.1 Způsoby instalace

Instalace je limitována nutností provozovat Zabbix server na kompatibilní platformě, navrhované řešení zároveň předpokládá, že jednotlivé komponenty budou instalovány na stejném zařízení. Tedy v rámci jednoho zařízení instance Zabbix server, webové rozhraní a databáze, na druhém zařízení pak Zabbix proxy a její databáze.

Platforma Zabbix nabízí několik způsobů, jak přistoupit k procesu instalace serveru [60]:

<i>Instalace z repozitářů</i>	První možností instalace je využití balíčků z repozitářů hlavních linuxových distribucí. Přidáním repozitáře platformy Zabbix je možné prostřednictvím balíčkovacího systému provést kompletní instalaci a konfiguraci jednotlivých komponent z terminálu systému.
<i>Instalace s využitím kontejnerové izolace</i>	Další možností instalace je využití tzv. Docker images. Každou komponentu platformy je možné provozovat jako izolovaný kontejner. Zjednodušeně lze říct, že jednotlivé komponenty jsou provozovány v rámci izolovaného virtuálního prostředí jako tzv. aplikační virtualizace. Nedochozí k virtualizaci HW prostředků, ale pouze SW prostředí pro běh aplikace = kontejner.

<i>Virtuální zaří- zení</i>	Platforma Zabbix také nabízí možnost využít předchystané virtuální zařízení pro spuštění v rámci většiny virtualizačních platforem. Zároveň je také dostupný instalační soubor systému ve formátu .iso. Tento způsob instalace zahrnuje předinstalované a předkonfigurované nástroje - je doporučován spíše pro testování, ne pro finální nasazení.
<i>Kompilace zdrojů</i>	V neposlední řadě mají uživatelé možnost stáhnout zdrojové soubory. S využitím překladače kompilují a instalují jednotlivé komponenty monitorovacího systému Zabbix. Z hlediska složitosti instalace je tato možnost nejnáročnější.

Tab. 5-3 Souhrn metod instalace systému Zabbix

Pro instalaci v rámci testovací infrastruktury, a tedy i jako doporučení pro finální implementaci byla zvolena instalace s využitím kontejnerové izolace jednotlivých komponent.

Instalace je snadná z hlediska konfigurace jednotlivých komponent a jednoduše replikovatelná. Komponenty jsou provozovány v izolovaném prostředí, takže nedochází k vzájemnému ovlivňování s ostatním provozovaným SW na zařízení. Kontejnerová virtualizace také podporuje lepší udržitelnost systému, virtuální prostředí je uzpůsobené provozu komponenty a nehrozí, že by např. aktualizací systému došlo k odstranění potřebných nástrojů a znehodnocení konfigurace. Jednotlivé kontejnery jsou také snadno zálohovatelné a v případě potřeby přenositelné na jiná zařízení.

Pro testovací účely a provoz monitorovacího systému bylo poskytnuto několik zařízení, pro provoz instance Zabbix serveru, proxy a jejich komponent byly vyhraněny dva linuxové stroje s OS Rocky Linux 8⁸ [61].

Pro správu virtuálních kontejnerů na poskytnutých zařízeních byl použit SW Podman [62]. Správce kontejnerů Podman funguje až na drobné odlišnosti stejně jako známé řešení – Docker [63]. Hlavním rozdílem je, že Podman nativně nevyžaduje spouštění kontejnerů s root oprávněními, oba systémy jsou z hlediska použití plně kompatibilní.

⁸ Rocky Linux je volně přístupná distribuce, která vznikla po oznámení ukončení vývoje platformy CentOS a je plnohodnotným pokračováním tohoto systému. Za vývojem stojí z převážné většiny původní tým z CentOS.

5.4.2 Instalace Zabbix serveru a jeho komponent

Při instalaci jednotlivých komponent systému Zabbix je využita nejaktuálnější LTS verze systému, dostupná v době tvorby práce – verze 6.0 LTS.

Vzhledem k využití kontejnerového řešení můžeme instalaci snadno rozdělit do několika postupných kroků:

1. Vytvoření virtuálního prostoru pro provoz komponent – tzv *pod*:

```
podman pod create --name Zabbix -p 10051:10051 -p 3306:3306 -p 80:8080
```

Pod si lze představit jako virtuální síť do které budou postupně „připojeny“ ostatní kontejnery. V rámci podu probíhá nastavení vlastností pro všechny zahrnuté kontejnery. V našem případě jsou nastaveny parametry:

--name Zabbix	Název podu
-p 10051:10051	Síťové porty, které budou dosažitelné ze sítě infrastruktury
-p 3306:3306	
-p 80:8080	

Tzv. propagace síťových portů funguje následovně: *port_hosta:port_kontejneru*, výše uvedené nastavení tedy zabezpečí, že příchozí komunikace serveru na portech 10051, 3306 a 80 bude přeměrována do izolovaného prostředí kontejnerů. Pro odchozí komunikaci kontejnerů platí situace naopak. Bez zpropagování portů by s jednotlivými komponentami nebylo možné komunikovat ze zbytku infrastruktury. Jednotlivé komponenty by byly schopny komunikovat pouze v rámci izolovaného podu.

Port 10051 je využíváný komunikačním protokolem Zabbixu, pomocí tohoto portu probíhá monitorování jednotlivých zařízení a komunikace mezi Zabbix serverem a Zabbix proxy.

Port 3306 je pak nativním portem pro MySQL databáze a je zpropagován **pouze pro testovací účely** – pro případnou kontrolu dat v databázi s využitím externích nástrojů. V případě provozu instance databáze na jiném zařízení je port nutné otevřít.

Port 80 je použitý pro zpřístupnění webového rozhraní systému Zabbix z portu 8080.

2. Instalace databázového serveru

Databázový server může být volen z některého z dostupných řešení, obecným doporučením je, volit takové řešení, se kterým již správci infrastruktury mají zkušenosti. Z tohoto důvodu je využitý databázový server MySQL.

```
podman run --name mysql-server -t \
    -e MYSQL_DATABASE="Zabbix" \
    -e MYSQL_USER="Zabbix" \
    -e MYSQL_PASSWORD="*****" \
    -e MYSQL_ROOT_PASSWORD="*****" \
    -v ./mysql:/var/lib/mysql:Z \
    --restart=always \
    --pod=Zabbix \
    -d mysql:8.0 \
    --character-set-server=utf8 \
    --collation-server=utf8_bin \
    --default-authentication-plugin=mysql_native_password
```

Uživatelské parametry:

--name mysql-server	Název kontejneru
-e MYSQL_DATABASE	Nastavení názvu databáze
-e MYSQL_USER	Vytvoření MySQL uživatele databáze
-e MYSQL_PASSWORD	Nastavení hesla vytvořeného uživatele
-e MYSQL_ROOT_PASSWORD	Nastavení root hesla pro operace s DB
-v ./mysql:/var/lib/mysql:Z \	Podobně jako je možné propagovat síťové porty, dochází v tomto případě k propojení datového adresáře databáze z kontejneru, do vnějšího adresářového systému serveru → ./mysql Při spouštění kontejneru je nutné, aby adresář ./mysql byl prázdný
--pod=Zabbix	Přiřazení kontejneru do již vytvořeného podu Zabbix

Ostatní parametry souvisí s verzí a nastavením DB serveru dle dokumentace [64].

3. Instalace komponenty *Zabbix server*:

Na základě zvoleného DB serveru je nutné zvolit odpovídající image pro Zabbix server – ve vztahu k předchozí konfiguraci je nutné zvolit image využívající MySQL.

```
podman run --name Zabbix-server-mysql -t \
    -e DB_SERVER_HOST="127.0.0.1" \
    -e MYSQL_DATABASE="Zabbix" \
    -e MYSQL_USER="Zabbix" \
    -e MYSQL_PASSWORD="*****" \
    -e MYSQL_ROOT_PASSWORD="*****" \
    -e ZBX_HOSTNAME="zabbix_server_MAIN"
    --restart=always \
    --pod=Zabbix \
    -d docker.io/Zabbix/zabbix-server-mysql:latest
```

Parametry:

--name Zabbix-server-mysql	Název kontejneru
-e DB_SERVER_HOST	Nastavení adresy, na které běží databázový server. Vzhledem k provozu databáze na stejném fyzickém zařízení můžeme použít výše uvedenou adresu localhost, komunikační port je defaultně 3306
-e MYSQL_DATABASE	Název databáze, kterou jsme vytvořili v předchozím kroku
-e MYSQL_USER	Uživatel databáze, opět dle předchozího kroku
-e MYSQL_PASSWORD	Uživatelské heslo dle předchozího kroku
-e MYSQL_ROOT_PASSWORD	Správcovské heslo dle předchozího kroku
-e ZBX_HOSTNAME	Nastavení hostname pro instanci serveru – nutné pro komunikaci s agentem.
--pod=Zabbix	Přiřazení kontejneru do již vytvořeného podu Zabbix
-d	Podobně jako u repozitářových systémů jsou image jednotlivých kontejnerů dostupné on-line. V našem případě požadujeme z repozitářů dockeru.io poslední verzi Zabbix serveru s podporou MySQL.

4. Instalace *webového rozhraní*

Pomyslnou poslední komponentou je webové rozhraní pro konfiguraci.

```
podman run --name Zabbix-web-mysql -t \
    -e ZBX_SERVER_HOST="127.0.0.1" \
    -e DB_SERVER_HOST="127.0.0.1" \
    -e MYSQL_DATABASE="Zabbix" \
    -e MYSQL_USER="Zabbix" \
    -e MYSQL_PASSWORD="*****" \
    -e MYSQL_ROOT_PASSWORD="*****" \
    --restart=always \
    --pod=Zabbix \
    -d docker.io/Zabbix/zabbix-web-nginx-mysql:latest
```

Parametry jsou z většiny totožné jako v předchozím kroku, rozdílné parametry jsou:

--name Zabbix-web-mysql	Název kontejneru
-e ZBX_SERVER_HOST	Nastavení adresy, na které běží instance Zabbix serveru, opět díky provozu na stejném zařízení a v rámci jednoho podu lze využít adresu localhost.
-d	Opět volíme image dostupný z repozitářů docker.io. Opět je nutné zvolit verzi podporující MySQL a zvolit webový server. V tomto případě byl zvolen webový server Nginx, alternativou je Apache.

5. Instalace Zabbix agenta

Posledním a volitelným krokem je instalace Zabbix agenta na zařízení. Takto lze docílit, že Zabbix server bude schopný monitorovat zařízení, které jej provozuje.

```
podman run --name Zabbix-agent \
  -e ZBX_SERVER_HOST="127.0.0.1" \
  -e ZBX_HOSTNAME="zabbix_server_MAIN" \
  --restart=always \
  --pod=Zabbix \
  -d docker.io/zabbixmultiarch/zabbix-agent2:latest
```

Parametry jsou opět velmi podobné s předchozími komponentami, rozdíly:

--name Zabbix-agent	Název kontejneru
-e ZBX_HOSTNAME	Parametr, který nastavuje, pod jakým názvem figuruje instance Zabbix serveru, tento název je nastavitelný pomocí webového rozhraní a zároveň byl nastaven při instalaci serveru. Nastavený hostname při konfiguraci kontejneru se musí shodovat se skutečným hostname instance serveru.
-d	Z repozitářů tentokrát využíváme image Zabbix agenta v modernější verzi 2.

Výsledkem takto provedené instalace by mělo být úspěšné spuštění jednotlivých komponent uvnitř vytvořeného podu:

Zabbix pod group		Running	Create container in pod		
Container	Owner	CPU	Memory	State	
> mysql-server docker.io/library/mysql:8.0 --character-set-server=utf8 --collation-server=utf8_bin --...	system	6.68%	11.1 / 252 GiB	running	
> zabbix-agent docker.io/zabbixmultiarch/zabbix-agent2:latest /usr/sbin/zabbix_agent2 --foreground -c...	system	0.28%	0.0244 / 252 GiB	running	
> zabbix-java-gateway docker.io/zabbix/zabbix-java-gateway:latest /usr/sbin/zabbix_java_gateway	system	0.09%	0.209 / 252 GiB	running	
> zabbix-server-mysql docker.io/zabbix/zabbix-server-mysql:latest /usr/sbin/zabbix_server --foreground -c...	system	4.83%	0.0336 / 252 GiB	running	
> zabbix-web-mysql docker.io/zabbix/zabbix-web-nginx-mysql:latest	system	0.03%	0.164 / 252 GiB	running	

Obr. 5-4 Přehled spuštěných komponent systému Zabbix [zdroj vlastní]

Zároveň by na adrese použitého serveru mělo být dostupné webové rozhraní nainstalovaného systému:

Obr. 5-5 Přihlašovací okno webového rozhraní Zabbix [zdroj vlastní]

Defaultní přístup do systému je U: Admin a P: Zabbix

Výše uvedený způsob popisuje kompletní proces instalace potřebných komponent a může sloužit jako návod při nasazení systému Zabbix do infrastruktury.

5.4.3 Instalace Zabbix proxy a jejích komponent

Navrhovaná struktura monitorovacího systému počítá s využitím Zabbix proxy pro monitoring jednotlivých zařízení v oddělených podsítích. Samotný proces instalace proxy je velmi podobný jako při instalování instance serveru:

1. Tvorba *podu*

Podobně jako v předchozím případě, na dalším testovacím zařízení je vytvořen pod pro sjednocení kontejnerů:

```
podman pod create --name zabbix_proxy -p 10051:10051 -p 3306:3306
```

Proxy nevyužívá webové rozhraní, port 80 proto není potřebný, port 3306 je propagován ze stejných důvodů jako v předchozím případě.

2. Instalace *databázového serveru*

Postup instalace je totožný jako při instalaci databáze pro klasický Zabbix server, jsou použity stejné parametry. Je vhodné použít jiné uživatelské jméno a hesla.

```
podman run --name mysql-server -t \  
-e MYSQL_DATABASE="zabbix_proxy" \  
-e MYSQL_USER="zabbix_proxy" \  
-e MYSQL_PASSWORD="*****" \  
-e MYSQL_ROOT_PASSWORD="*****" \  
-v ./mysql:/var/lib/mysql:Z \  
--restart=always \  
--pod=zabbix_proxy \  
-d mysql:8.0 \  
--character-set-server=utf8 \  
--collation-server=utf8_bin \  
--default-authentication-plugin=mysql_native_password
```

3. Instalace instance *proxy*

Instalace proxy probíhá velmi podobně jako při instalaci Zabbix serveru, ale je využít jiný image z repozitářů:

```
podman run --name zabbix_proxy_U5 -t \  
    -e DB_SERVER_HOST="127.0.0.1" \  
    -e MYSQL_DATABASE="zabbix_proxy" \  
    -e MYSQL_USER="zabbix_proxy" \  
    -e MYSQL_PASSWORD="*****" \  
    -e MYSQL_ROOT_PASSWORD="*****" \  
    -e ZBX_HOSTNAME="zabbix_proxy_U5" \  
    -e ZBX_SERVER_HOST="*.*.*.*" \  
    --restart=always \  
    --pod=zabbix_proxy \  
    -d docker.io/Zabbix/zabbix-proxy-mysql:latest
```

Novým parametrem instalace je:

`-e ZBX_SERVER_HOST`

IP adresa na které se nachází instance hlavního Zabbix serveru. Komunikační port je opět defaultně 10051.

4. Instalace *Zabbix agenta*

Stejně jako v předchozím případě i zde je vhodné, aby zařízení provozující proxy bylo současně monitorováno. V následující konfiguraci je agent nastavený tak, že komunikuje s proxy na stejném zařízení. Zjednodušeně tedy proxy monitoruje sama sebe a získaná data jsou následně předána na hlavní server:

```
podman run --name Zabbix-agent \  
    -e ZBX_SERVER_HOST="127.0.0.1" \  
    -e ZBX_HOSTNAME="zabbix_proxy_U5" \  
    --restart=always \  
    --pod=zabbix_proxy \  
    -d docker.io/zabbixmultiarch/zabbix-agent2:latest
```

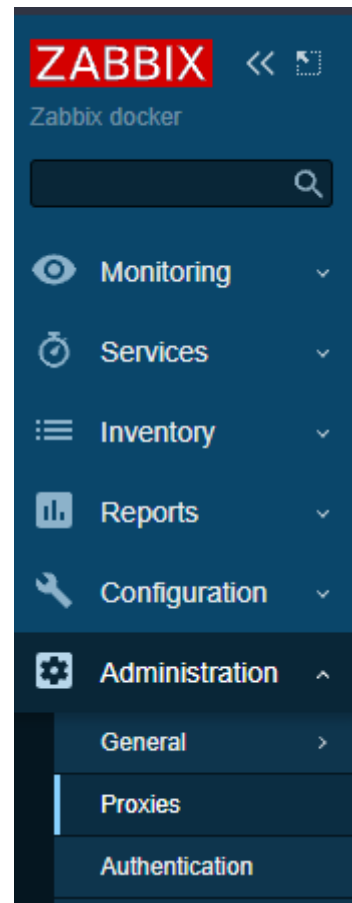
Vzhledem k provozu na stejném zařízení a v rámci jednoho podu je adresa proxy použita jako localhost.

5.4.4 Registrace proxy v systému Zabbix

Aby byla proxy použitelná pro monitorování zařízení je nejprve nutné ji zaregistrovat v rámci systému Zabbix. Tak bude zajištěna komunikace a výměna dat mezi hlavním serverem Zabbix a proxy.

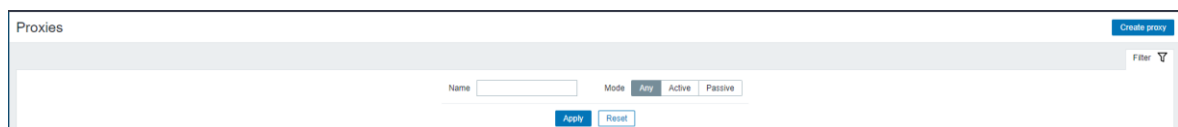
Po přihlášení do webového rozhraní je nutné otevřít záložku:

Administration > Proxies



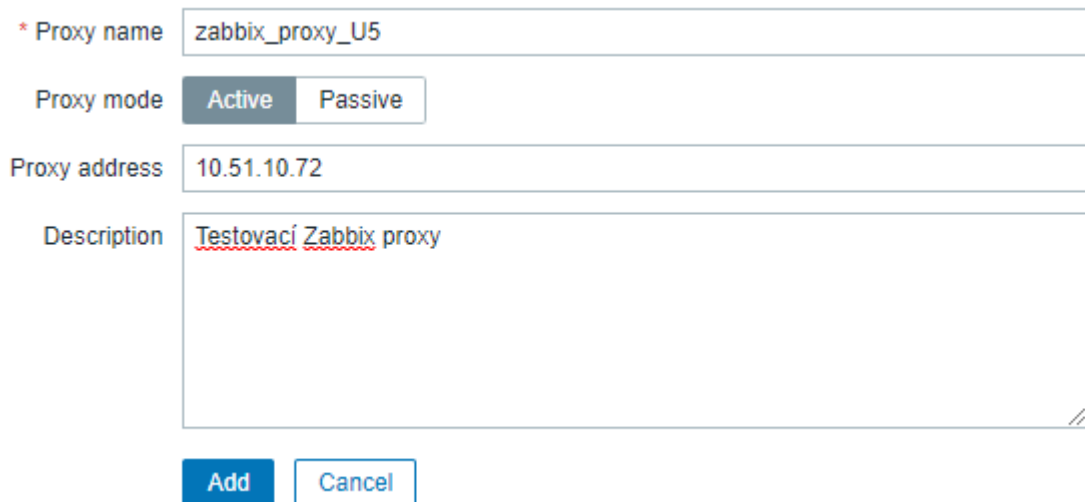
Obr. 5-6 Registrace proxy
krok č.1 [zdroj vlastní]

Dalším krokem je registrace nové proxy: **Create proxy** v pravém horním rohu aplikace:



Obr. 5-7 Registrace proxy krok č. 2 [zdroj vlastní]

Je provedena konfigurace dle nastavení proxy při její instalaci:



* Proxy name: zabbix_proxy_U5

Proxy mode: Active (selected) / Passive

Proxy address: 10.51.10.72

Description: Testovací Zabbix proxy

Buttons: Add, Cancel

Obr. 5-8 Registrace proxy krok č. 3 [zdroj vlastní]

Po chvíli od potvrzení registrace by výsledný stav měl indikovat probíhající komunikaci s proxy:

<input type="checkbox"/>	Name ▲	Mode	Encryption	Compression	Last seen (age)
<input type="checkbox"/>	zabbix_proxy_U5	Active	None	On	5s

Obr. 5-9 Registrace proxy – potvrzení probíhající komunikace [zdroj vlastní]

Při produkčním nasazení je žádoucí konfigurovat šifrování komunikace proxy – server.

Využitím výše uvedených postupů je možné plně implementovat monitorovací řešení Zabbix v rámci řešené infrastruktury a dodržet navržený postup integrace pomocí jednotlivých zařízení proxy.

Jediná nevýhoda kontejnerové izolace je nemožnost zpětné změny síťového nastavení vytvořených podů. Při požadavku na změnu konfigurace sítě musí být pod smazán a znovu vytvořen. Tato operace je spojena se smazáním všech kontejnerů v rámci podu. Je tedy potřeba kontejnery zálohovat, smazat, vytvořit pod s novým nastavením a znovu provést instalaci zálohovaných kontejnerů.

Tomuto problému je částečně předcházeno využitím proxy. U podu serveru je nutný pouze primární port pro komunikaci s proxy. Vzhledem k tomu, že proxy odesílají získaná data na server, může při nutnosti změny konfigurace proxy docházet k jejich mazání a opětovnému vytvoření. Smazání proxy neovlivní data již uložené na hlavním serveru.

6 SCÉNÁŘE POUŽITÍ MONITOROVACÍHO SYSTÉMU ZABBIX

Předchozí kapitoly se zabývaly problematikou selekce a návrhu struktury monitorovacího systému pro řešenou infrastrukturu. Byla stanovena doporučení pro správnou integraci systému Zabbix do infrastruktury. Následně byla provedena ukázková instalace v testovací infrastruktuře. Takto byl stanoven možný postup instalace, který je využitelný při finální implementaci řešení.

V rámci této kapitoly budou popsány možné scénáře použití a konfigurace monitorovacího systému. Čtenáři práce by po přečtení měli získat znalosti o možnostech a způsobech integrace systému Zabbix do jejich infrastruktury a zároveň získat přehled o jeho základním použití. To jim může pomoci uchopit problematiku monitoringu a pomoci při práci s dokumentací systému Zabbix.

Ukázkové konfigurace v rámci kapitoly jsou vytvořeny na základě informací dostupných v aktuální dokumentaci platformy Zabbix – zdroj [65].

6.1 Možnosti využití Zabbix agenta pro monitoring zařízení

Lze předpokládat, že při nasazení monitorovacího systému na všechny prvky infrastruktury, bude nejčastěji využívaným způsobem monitoring pomocí Zabbix agenta. Minimálně v rámci řešené infrastruktury by taková situace platila. Nejpočetnější skupinu tvoří zařízení s OS Windows, z hlediska serverů pak OS Linux a jeho variace.

Proto budou v první řadě popsány možnosti využití Zabbix agenta pro získání dat z infrastruktury a při procesu budou zároveň vysvětleny základní principy monitoringu pomocí platformy Zabbix.

6.1.1 Instalace agenta na sledované zařízení

Prvním nutným krokem při využití Zabbix agenta je jeho instalace na sledovaném zařízení a prvotní konfigurace.

Vzhledem k rozložení OS v rámci řešení infrastruktury bude popsána ukázková instalace agenta na zařízení platformy Windows a platformy Linux.

Stejně jako v předchozím případě by bylo možné instalovat Zabbix agent formou kontejneru. Takové řešení ale není vhodné pro instalace na běžná zařízení a je jednodušší využít dostupné aplikace agenta.

6.1.1.1 Aktivní vs pasivní agent

Před samotnou ukázkou instalace je nutné vysvětlit režimy fungování Zabbix agenta. Agent může operovat ve dvou režimech – aktivním a pasivním.

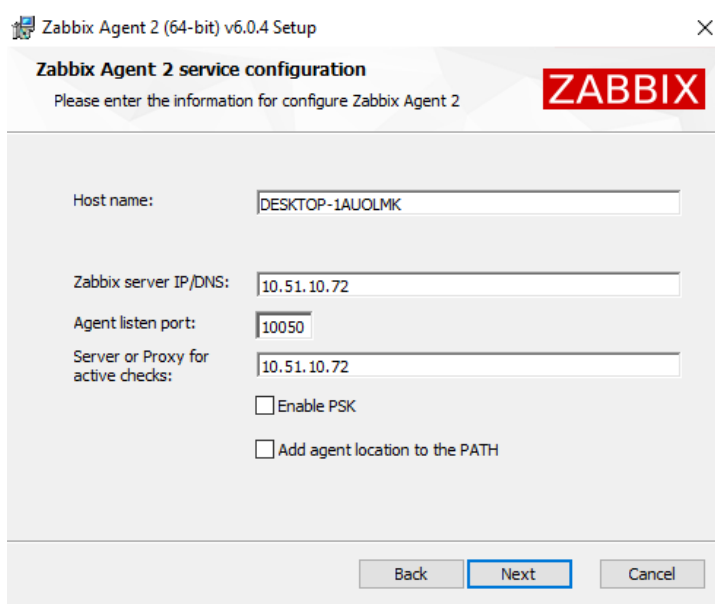
Běžnější je využití v pasivním režimu. V tomto režimu probíhá získání dat následovně: Server/proxy otevře spojení s monitorovaným zařízením a zažádá o požadované hodnoty dle nastavení. Agent jako odpověď vrátí požadovaná data a spojení se uzavírá.

Druhý způsob využití je aktivní režim. V takovém případě spojení iniciuje zařízení s nainstalovaným agentem. První proběhne dotaz na server, jaká data jsou požadována. Následně dojde k lokálnímu vyhodnocení požadavku a po získání všech výsledků agent opět otevře spojení a odešle data na server.

Agent může být konfigurován tak, aby byl schopný využívat oba typy režimu komunikace. Pro většinu monitoringu je možné využívat pasivní režim. Ale existují případy, které budou popsány v dalších částech, kdy získání dat musí probíhat v režimu aktivním. Zejména se jedná o nutnost lokálního získání a parsování dat ve sledovaném zařízení.

6.1.1.2 Instalace na Windows zařízení

Instalace agenta na Windows zařízení probíhá prostřednictvím .msi balíčku. Ten je zároveň uzpůsoben pro instalaci z příkazové řádky – možné využít například systém SCCM nebo GPO politiku pro hromadnou instalaci v infrastruktuře.



Obr. 6-1 Konfigurace instalace Zabbix agenta pro OS Windows

[zdroj vlastní]

Při instalaci je nutné nastavit parametry instalace:

Host name	Získán automaticky dle nastavení názvu zařízení.
Zabbix server IP/DNS	Adresa zařízení, které provádí monitoring zařízení v pasivním režimu. V našem případě zadáváme IP instalované proxy. V případě řešené infrastruktury by to vždy byla adresa proxy pro příslušnou VLAN.
Agent listen port	Defaultní hodnota 10050 – port na kterém agent očekává komunikaci.
Server or Proxy for active checks	Adresa zařízení, které poskytuje informace pro aktivní monitoring. Opět zadáváme adresu instalované proxy. Případně proxy pro příslušnou VLAN.

Pro testovací účely není nastaveno šifrování komunikace – PSK, při finální implementaci je vhodné, aby komunikace probíhala šifrovaně.

Celková konfigurace agenta je dostupná formou konfiguračního souboru – defaultní cesta:

“C:\Program Files\Zabbix Agent 2\zabbix_agent2.conf“

6.1.1.3 Instalace pro zařízení s OS Linux

Při instalaci na zařízení s OS Linux je nejjednodušší využít repozitář platformy Zabbix, pro ukázkovou instalaci je využito zařízení s OS Ubuntu 20.04:

```
wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu20.04_all.deb
dpkg -i zabbix-release_6.0-1+ubuntu20.04_all.deb
apt update
apt install zabbix-agent2
```

Po instalaci agenta je nutné provést jeho konfiguraci – podobně jako na systémech Windows. Konfigurační soubor agenta se nachází v:

/etc/Zabbix/zabbix_agent2.conf

Otevřením v libovolném textovém editoru je nutné manuálně nastavit stejné parametry jako v předchozím případě – hostname a komunikační port jsou opět nastaveny defaultně.

Nastavení adresy pro pasivní kontroly, opět využita adresa testovací proxy:

```
### Option: Server
#   List of comma delimited
#   Incoming connections w
#   If IPv6 support is ena
#   and ':::/0' will allow
#   '0.0.0.0/0' can be use
#   Example: Server=127.0.
#
# Mandatory: yes, if StartAgen
# Default:
# Server=
Server=127.0.0.1
```

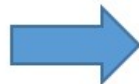


```
### Option: Server
#   List of comma delimited
#   Incoming connections w
#   If IPv6 support is ena
#   and ':::/0' will allow
#   '0.0.0.0/0' can be use
#   Example: Server=127.0.
#
# Mandatory: yes, if StartAgen
# Default:
# Server=
Server=10.51.10.72
```

Obr. 6-2 Konfigurace Zabbix agenta pro OS Linux – adresa pro pasivní kontroly [zdroj vlastní]

Stejně tak adresu zařízení pro aktivní kontroly:

```
### Option: ServerActive
#   List of comma delimited
#   If port is not specifie
#   Cluster nodes need be
#   IPv6 addresses must be
#   If port is not specifie
#   If this parameter is ne
#   Example for multiple se
#       ServerActive=127.0.
#   Example for HA:
#       ServerActive=zabbix
#   Example for HA with tw
#       ServerActive=zabbix
#
# Mandatory: no
# Default:
# ServerActive=
ServerActive=127.0.0.1
```



```
### Option: ServerActive
#   List of comma delimit
#   If port is not specifi
#   Cluster nodes need
#   IPv6 addresses must
#   If port is not specifi
#   If this parameter
#   Example for multip
#       ServerActi
#   Example for HA:
#       ServerActi
#   Example for HA wit
#       ServerActi
#
# Mandatory: no
# Default:
# ServerActive=
ServerActive=10.51.10.72
```

Obr. 6-3 Konfigurace Zabbix agenta pro OS Linux – adresa pro aktivní kontroly [zdroj vlastní]

Po uložení změn je nutné restartovat službu Zabbix agenta:

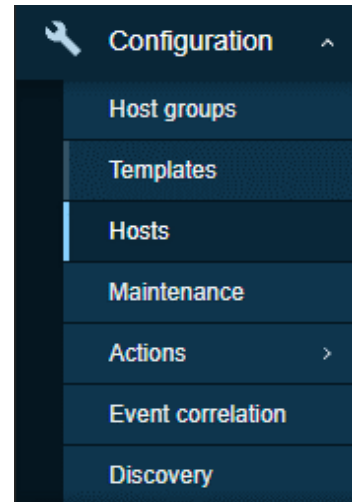
```
service zabbix-agent2 restart
```

6.1.2 Registrace monitorovaného zařízení v systému Zabbix

Stejně jako v případě proxy je nutné sledovaná zařízení registrovat v rámci systému Zabbix.

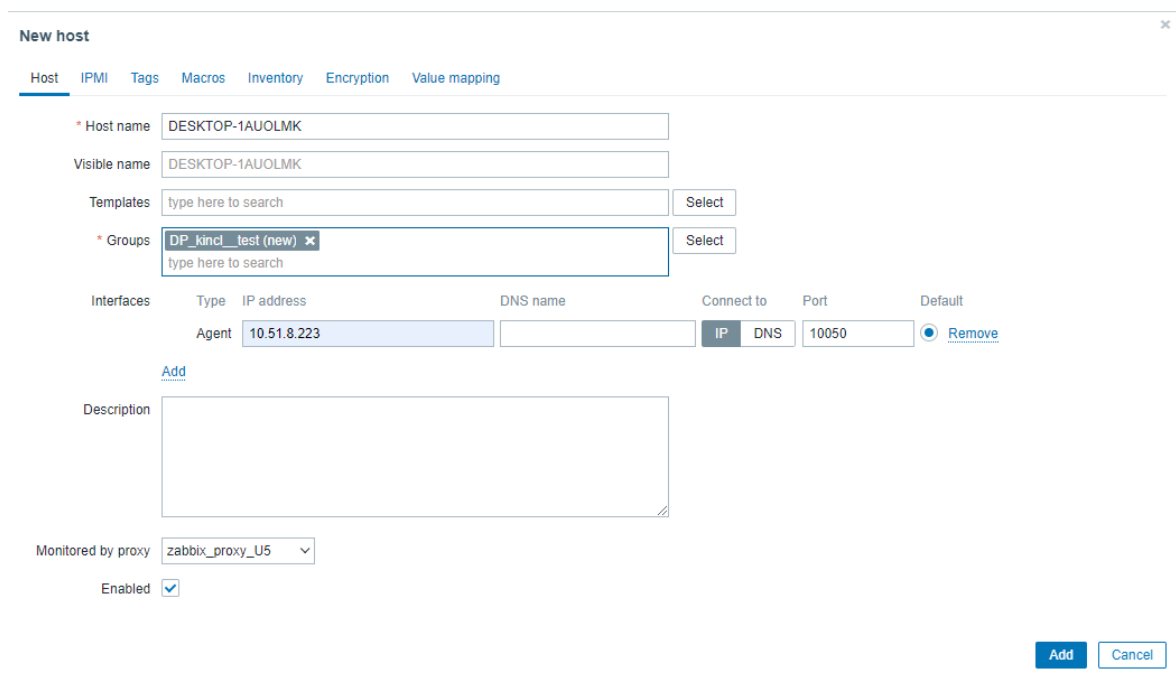
Pomocí webového rozhraní je nutné otevřít záložku:

Configuration>Hosts



Obr. 6-4 Registrace monitorovaného zařízení krok č. 1 [zdroj vlastní]

Následně opět v pravém horním rohu – **Create host:**

A screenshot of the 'New host' form in the Zabbix web interface. The form has tabs for Host, IPMI, Tags, Macros, Inventory, Encryption, and Value mapping. The 'Host' tab is active. Fields include: Host name (DESKTOP-1AUOLMK), Visible name (DESKTOP-1AUOLMK), Templates (search field), Groups (DP_kinc1_test (new) selected), Interfaces table with columns Type, IP address, DNS name, Connect to, Port, and Default. The table has one row for 'Agent' with IP address 10.51.8.223, Connect to IP and DNS, Port 10050, and Default set to Remove. There is an 'Add' link below the table. A Description text area is empty. Monitored by proxy is set to zabbix_proxy_U5. The Enabled checkbox is checked. 'Add' and 'Cancel' buttons are at the bottom right.

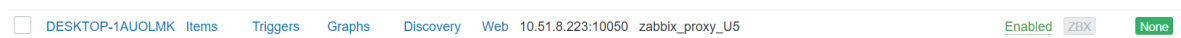
Obr. 6-5 Registrace monitorovaného zařízení krok č. 2 [zdroj vlastní]

Hostname se musí shodovat s hostname sledovaného zařízení, v rámci nastavení Groups je možné zařízení přiřadit do skupiny (Groups) – pro testovací účely je zadáním nového názvu vytvořena skupina DP_kincl_test.

Nastavení interface následně je zvoleno jako *agent*, je nutné vložit adresu sledovaného zařízení, port je defaultní.

Nutné určit, že host je monitorovaný prostřednictvím dříve registrované proxy. Následně je možné potvrdit registraci hosta.

Do přehledu hostů je přidán záznam o registrovaném zařízení:



Obr. 6-6 Výsledek registrace zařízení [zdroj vlastní]

Ikona statusu komunikace – *ZBX* je zatím nezvýrazněna – dostupnost hosta je neznámá. Spojení se aktivuje až po nastavení pravidel monitoringu.

6.1.2.1 Automatická registrace zařízení

Výše uvedený scénář registrace je použitelný pouze v případě, že cílem je monitorovat pouze několik zařízení. V případě, že je nutné pokrýt stovky zařízení v rámci infrastruktury, byl by tento proces manuální registrace zařízení nezvladatelný.

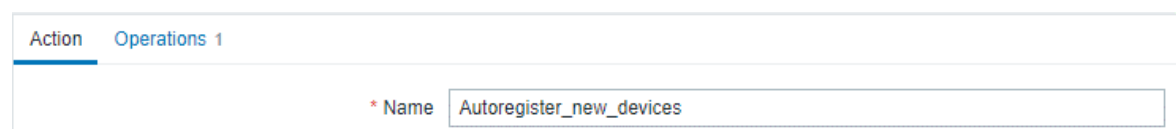
Řešením je využití toho, že agenty na zařízeních lze nastavit jako aktivní. Jak již bylo řečeno, v této konfiguraci agent navazuje spojení se server a na základě této komunikace může dojít k automatické detekci a registraci nových zařízení.

Pro nastavení opět využijeme záložku:

Configuration > Actions > Autoregistration actions

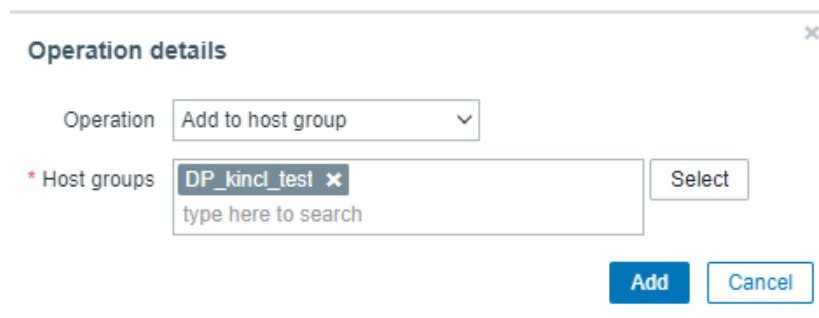
Zde vytvoříme novou akci – opět pravý horní roh.

V dialogovém okně je nutné nastavit název akce:



Obr. 6-7 Konfigurace automatické registrace zařízení krok č. 1 [zdroj vlastní]

a v záložce **Operations** požadovanou činnost:



Operation details

Operation Add to host group

* Host groups DP_kincl_test x type here to search Select

Add Cancel

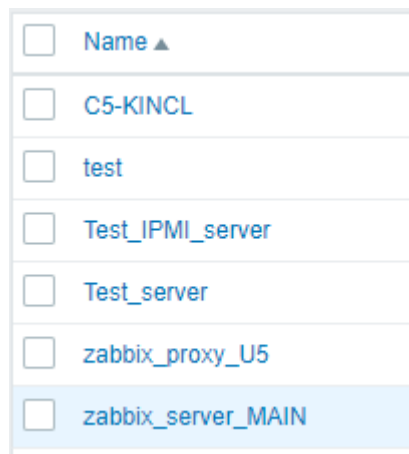
Obr. 6-8 Konfigurace automatické registrace zařízení krok č. 2 [zdroj vlastní]

Podmínky autoregistrace není nutné nastavit. Po přidání operace vložení do námi vytvořené skupiny a vytvoření celé akce, budou všechna neznámá zařízení s aktivním agentem automaticky přidána do zadané skupiny a automaticky registrována.

6.2 Získávání dat ze sledovaných zařízení

Potom co jsou jednotlivá zařízení registrovaná v systému Zabbix, budou viditelná v rámci přehledu registrovaných hostů ve webovém rozhraní:

Configuration > Hosts



<input type="checkbox"/>	Name ▲
<input type="checkbox"/>	C5-KINCL
<input type="checkbox"/>	test
<input type="checkbox"/>	Test_IPMI_server
<input type="checkbox"/>	Test_server
<input type="checkbox"/>	zabbix_proxy_U5
<input type="checkbox"/>	zabbix_server_MAIN

Obr. 6-9 Přehled registrovaných hostů v testovací infrastruktuře

Po registraci zařízení je možné začít tvořit požadavky pro získávání dat. Požadavek na získání dat je označen jako **Item** a každý item souvisí s procesem získání požadované hodnoty. Pro konfiguraci jednotlivých požadavků je nutné u zařízení, pro která má být vytvořen požadavek, otevřít záložku **Items**:



Obr. 6-10 Tvorba dotazu pro sběr dat z testovacího zařízení krok č. 1 [zdroj vlastní]

Takto je otevřena konfigurace požadavků pro zvolené zařízení a je možné konfigurovat jednotlivé operace.

Nový požadavek je vytvořen kliknutím na **Create item** v pravém horním rohu. Tím je otevřeno dialogové okno, ve kterém je prováděna konfigurace požadavku a jeho následné přidání do systému Zabbix.

V rámci demonstrace principu použití je předpokládáno, že požadovaná informace má vyjadřovat aktuální dostupnost sledovaného zařízení.

Zařízení bylo do systému registrováno jako zařízení využívající Zabbix agenta pro získávání informací. Pro platformu Zabbix existuje celá řada definovaných dotazů – tzv. klíčů, které slouží k získávání dat prostřednictvím agenta. Kompletní seznam je dostupný v dokumentaci [66].

Pro sledování dostupnosti lze použít definovaný klíč **agent.ping**. Tento dotaz provede ověření dostupnosti zařízení. V případě úspěšného odpovědi vrátí 1, v případě neúspěchu 0.

Konfiguraci dotazu je možné nastavit následovně:

* Name

Type

* Key

Type of information

Units

* Update interval

Custom intervals

Type	Interval	Period	Action
Flexible Scheduling	50s	1-7,00:00-24:00	Remove

[Add](#)

* History storage period

* Trend storage period

Value mapping

updates host inventory field

Description

Enabled

Obr. 6-11 Konfigurace dotazu na dostupnost sledovaného zařízení [zdroj vlastní]

Je nutné nastavit libovolný název pro dotaz, zvolit typ dotazu – v tomto případě pasivní režim Zabbix agenta a vybrat ze seznamu odpovídající klíč.

Po registraci itemu začne systém Zabbix sledovat dostupnost zařízení – vzhledem k použití proxy, je možné že proces získávání dat bude spuštěn s časovou prodlevou, proxy musí nejprve získat informace k vlastní konfiguraci a spustit monitoring zařízení, defaultně by tato prodleva neměla být delší než 1 h.

Obdobným způsobem je nutné pro všechna zařízení konfigurovat sérii dotazů pro získání požadovaných dat. Podobně jako při registraci nových zařízení je takový scénář realizovatelný jen při velmi malém počtu zařízení. Pro každé zařízení můžou být nastaveny desítky dotazů a při velké počtu zařízení by konfigurace monitoringu nebyla realizovatelná.

Řešením tohoto problému je využití tzv. Templates (Vzorů) v systému Zabbix.

6.2.1 Využití a tvorba templates v systému Zabbix

Template v systému Zabbix představuje pomyslné sjednocení Itemů do skupiny. Při jeho tvorbě jsou nejdříve definovány jednotlivé dotazy, stejně jako v předchozím případě. Rozdíl je, že takto vytvořený Template je následně možné aplikovat na libovolný počet registrovaných zařízení.

Přínosem je, že konfiguraci dotazů je nutné provést pouze při tvorbě vzoru. Po jeho nasazení na jednotlivá zařízení systém Zabbix replikuje tyto dotazy pro jednotlivá zařízení automaticky. Díky tomu je možné zabezpečit monitoring velkého počtu zařízení a zajistit snadnou možnost změny konfigurace na všech zařízeních pro která je Template použitý.

Kromě již zmiňovaných předností systému Zabbix, je další silnou stránkou systému existence desítek integrovaných vzorů přímo v rámci platformy. Tyto vzory jsou volně dostupné a často obsahují předpřipravenou konfiguraci pro konkrétní typy zařízení a operačních systémů. Jsou přednastaveny jednotlivé dotazy, definovány kritické stavy a příslušná upozornění, předchystané grafy. I s minimální znalostí systému je tedy možné využitím existujících vzorů zajistit monitoring infrastruktury.

Protože i dostupné Templates jsou pro uživatele plně modifikovatelné, budou v rámci práce popsány další jednoduché scénáře konfigurace, se kterými se uživatelé mohou setkat.

<input type="checkbox"/>	VMware Hypervisor	Hosts	Items 26	Triggers 4	Graphs	Dashboards	Discovery 2	Web
<input type="checkbox"/>	VMWare SD-WAN VeloCloud by HTTP	Hosts	Items 7	Triggers 5	Graphs	Dashboards	Discovery 5	Web
<input type="checkbox"/>	Website certificate by Zabbix agent 2	Hosts	Items 13	Triggers 3	Graphs	Dashboards	Discovery	Web
<input type="checkbox"/>	WildFly Domain by JMX	Hosts	Items 5	Triggers 2	Graphs	Dashboards	Discovery 2	Web
<input type="checkbox"/>	WildFly Server by JMX	Hosts	Items 17	Triggers 5	Graphs 1	Dashboards	Discovery 4	Web
<input type="checkbox"/>	Windows by Zabbix agent	Hosts	Items 32	Triggers 12	Graphs 5	Dashboards 2	Discovery 4	Web

Obr. 6-12 Ukázka dostupných Templates v systému Zabbix [zdroj vlastní]

6.2.2 Tvorba dynamických pravidel pro získání dat

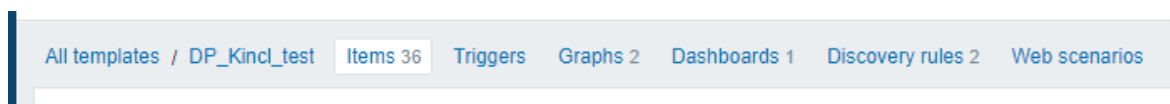
Další limitací, při tvorbě dotazů pro získání dat, je nutnost znalosti konfigurace koncového zařízení pro některé typy dotazů.

Následující ukázka předpokládá, že je cílem na koncových zařízeních v infrastruktuře monitorovat obsazenost připojených souborových systémů.

Při konfiguraci klasického dotazu na vlastnosti souborového systému je nutné znát jeho název. To samo o sobě představuje značný problém. V první řadě, není jasné, jaké souborové systémy mohou být ke koncovým zařízením připojeny. PC s OS Windows nejčastěji jednotlivé disky označují postupnými písmeny abecedy, linuxové systémy pak mají slovní názvy. V rámci dotazu tedy není možné přesně specifikovat dotazy na vlastnosti disku C, vlastnosti disku D apod. U některých zařízení tyto disky nemusí být přítomny, u jiných naopak může být disků přítomno více a absencí dotazu nedojde ke sledování všech disků.

Řešením problému je tvorba tzv. dynamických pravidel. V rámci testovacího template, vytvořeného pro monitorování zařízení Windows, bude demonstrován způsob konfigurace dynamického dotazu.

Na záložce **Configuration>Templates** je zvolena záložka **Items** u vzoru, který je modifikován, tomto případě je zvolen template vytvořený pro účely demonstrace. Takto je otevřena konfigurace samotného vzoru.



Obr. 6-13 Konfigurace dynamických pravidel pro získání dat krok č. 1 [zdroj vlastní]

Dle horní záložky zobrazené na obrázku Obr. 6-13 je patrné, že v rámci testovacího template je zahrnuto 36 různých typů dotazů pro sběr dat. Pro ukázkou dynamických pravidel jsou dále důležitá tzv. **Discovery rules**.

V tomto scénáři je představena konfigurace dynamických prvků pro monitoring připojených souborových systémů. Základem pro tvorbu dynamických prvků je tvorba tzv. master item. Ten slouží jako základ, pro další pravidla a zpracování dat.

Proces tvorby Itemu je stejný jako při předchozím příkladu, pro získání základních informací je provedena následující konfigurace:

* Name

Type

* Key

Type of information

* Update interval

Custom intervals

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	Remove

[Add](#)

History storage period Storage period

Trends storage period Do not keep trends Storage period

Host inventory field

Description

Enabled

Obr. 6-14 Konfigurace master itemu pro monitoring souborových systémů [zdroj vlastní]

Návratová hodnota klíče **vfs.fs.get** je soubor JSON, který obsahuje informace o připojených souborových systémech:

```
[
  {
    "fsname": "C:",
    "fstype": "NTFS",
    "fslabel": "",
    "fsdrivetype": "fixed",
    "bytes": {
      "total": 509783953408,
      "free": 37576810496,
      "used": 472207142912,
      "pfree": 7.371124619516184,
      "pused": 92.62887538048382
    }
  },
  {
    "fsname": "D:",
    "fstype": "FAT32",
    "fslabel": "ROCKY-8-5-X",
    "fsdrivetype": "removable",
    "bytes": {
      "total": 30747394048,
      "free": 19885424640,
      "used": 10861969408,
      "pfree": 64.67352845888892,
      "pused": 35.32647154111107
    }
  }
]
```

Obr. 6-15 Ukázka návratové hodnoty klíče **vfs.fs.get** ve formátu JSON [zdroj vlastní]

JSON zobrazený na Obr. 6-15 indikuje připojení dvou disků do systému – C a D, kdy disk D je odnímatelný a jedná se o zařízení USB.

Nyní je nutné vytvořit pravidla, která provedou zpracování souboru JSON a extrahují jednotlivé hodnoty.

Pro tento účel je nutné vytvořit již zmiňované **Discovery rule**. Při vytváření pravidla je konfigurace následující:

The screenshot shows a configuration form for a Discovery rule. The fields are as follows:

- Name:** Discovery rule for Filesystems
- Type:** Dependent item (dropdown menu)
- Key:** fs.mountpoint.discovery
- Master item:** DP_Kincl_test: Get filesystem (with a 'Select' button)
- Sources period:** 0
- Description:** (empty text area)
- Enabled:**

Obr. 6-16 Konfigurace discovery rule pro monitoring připojených souborových systémů [zdroj vlastní]

Je nutné, aby pravidlo bylo konfigurováno jako závislý prvek, nadřazený (Master) item je pak dotaz vytvořený v předchozím kroku, tím dojde k předání výsledku dotazu pro další práci v rámci tvořeného Discovery rule. Hodnota klíče je v tomto případě uživatelsky nastavitelná, pro přehlednost je vhodné pojmenovat klíč jasným způsobem.

Současně s touto konfigurací, je nutné konfigurovat příslušná makra – záložka LLD macros:

LLD macros	LLD macro	JSONPath
	{#FSDTYPE}	\$.fsdrivetype
	{#FSNAME}	\$.fsname
	{#FSTYPE}	\$.fstype

Obr. 6-17 Nutná konfigurace maker pro identifikaci připojených souborových systémů [zdroj vlastní]

Při tvorbě Discovery pravidel si lze makra představit jako způsob tvorby zástupných hodnot. Na pravé straně jsou klíče ze získaného souboru JSON a na levé straně je název makra, pod kterým budou dostupné hodnoty těchto klíčů při zpracovávání jednotlivých hodnot.

Posledním krokem spojeným s konfigurací Discovery pravidla je tvorba prototypů itemů pro získání dat – záložka **Item prototypes**.

Vytváření prototypu spustíme stejným způsobem jako při vytváření klasického itemu. Při samotné konfiguraci je ale nutné navázat na předchozí kroky.

Následující dotaz slouží k získání informací o volném místě na připojených souborových systémech:

The screenshot shows the configuration form for an item prototype. The fields are as follows:

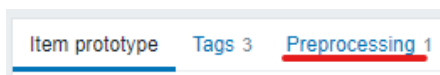
- Name:** Free disk space of {#FSNAME}
- Type:** Dependent item (dropdown)
- Key:** free[{#FSNAME}] (with a Select button)
- Type of information:** Numeric (unsigned) (dropdown)
- Master item:** DP_Kincl_test: Get filesystem (with a Select button)
- Units:** B
- History storage period:** Storage period 90d (with a Do not keep history button)
- Trend storage period:** Storage period 365d (with a Do not keep trends button)
- Value mapping:** type here to search (with a Select button)
- Description:** (empty text area)
- Create enabled:**
- Discover:**

Obr. 6-18 Konfigurace prototypu itemu – zjištění volného místa na připojených souborových systémech
[zdroj vlastní]

V názvu prototypu je nutné použít zástupné makro pro název připojeného disku – pravidla budou replikována pro všechny identifikované souborové systémy. Opět se jedná o tzv. Závislý (Dependant) item a nadřazeným prvek je stejný jako v předchozím případě.

Klíč dotazu je závislý na klíčích, které jsou použity pro identifikaci jednotlivých hodnot v souboru JSON. V tomto případě nás zajímá počet volných bytů. Klíč je tedy **free** a opět je použito zástupné makro pro název disku, aby došlo k extrakci hodnoty pro příslušný souborový systém.

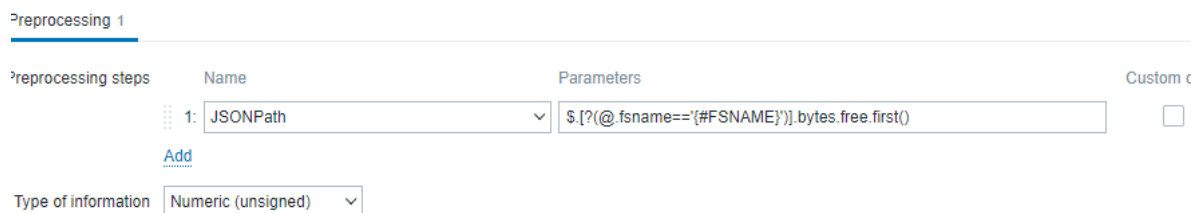
Aby takovýto dotaz fungoval je nutné skrz horní lištu nastavit **Preprocessing** dat:



Obr. 6-19 Nastavení preprocessingu dat

[zdroj vlastní]

Na záložce preprocessingu je nutné konfigurovat způsob práce se hodnotou JSON:



Obr. 6-20 Konfigurace zpracování hodnoty JSON [zdroj vlastní]

Je využitý způsob JSONPath a na pravé straně je nastaveno pravidlo pro extrakci hodnoty ze zpracovávaného JSONu. Opět je nutné využít definovaného makra, které zajistí, že se dotazy vyhodnotí postupně pro korektně identifikované disky.

Návratovou hodnotou výše uvedeného pravidla je počet volných bytů na disku a tato hodnota je předána a uložena pod klíčem definovaným v rámci předchozího kroku.

Výsledkem takto provázaných dynamických pravidel a následně vytvořených prototypů je, že při aplikaci vzoru na zařízení, jsou nejprve získány informace o všech připojených souborových systémech a pro všechny (i nově připojené) souborové systémy jsou dynamicky vytvářena jednotlivá pravidla.

Name ▲	Last check	Last value
% Free disk space of C: ?	40s	7.3687 %
% Free disk space of D: ?	40s	64.6735 %
% Used disk space of C: ?	40s	92.6313 %
% Used disk space of D: ?	40s	35.3265 %
Free disk space of C:	40s	34.98 GB
Free disk space of D:	40s	18.52 GB
Total disk space of C: ?	40s	474.77 GB
Total disk space of D: ?	40s	28.64 GB
Used disk space of C:	40s	439.79 GB
Used disk space of D:	40s	10.12 GB

Obr. 6-21 Ukázka vygenerovaných dotazů pro sledované disky C a D na testovacím zařízení [zdroj vlastní]

Podobným způsobem lze konfigurovat dynamická pravidla pro síťová rozhraní a další vyměnitelná zařízení. V rámci předdefinovaných vzorů jsou dynamická pravidla také obsažena. A celý postup je detailněji popsán v dokumentaci systému – výše uvedená konfigurace je pouze demonstrativní.

Pomocí dynamických dotazů je možné řešit monitoring automaticky registrovaných zařízení o předem neznámé konfiguraci. U více specifických zařízení infrastruktury – např. serverů, lze předpokládat, že monitoring bude možné zajistit běžnými dotazy – konfigurace serverů a podobných zařízení je většinou známá.

6.2.3 Zpracování logů pomocí systému Zabbix

Kromě dotazů na klasické provozní metriky provozovaných systémů, je možné vytvořit dotazy s cílem zpracování logů dostupných v rámci systému.

Konfigurace opět probíhá pomocí dotazu pro Zabbix agenta. Tentokrát je ale nutné využít agenta v aktivním režimu, protože agent nejprve lokálně zpracuje požadovaný log a na server odesílá až získaný výsledek.

V rámci linuxových zařízení probíhá monitoring pomocí klíče **log[]**. Ten je nutné konfigurovat dle dokumentace, je nutné zadat cestu k logu a regulární výraz, který identifikuje požadovanou část logu.

Klíč **log[]** je možné využít také pro sledování logů provozovaných aplikací v rámci systémů, je ovšem nutné zajistit příslušná oprávnění pro Zabbix agenta – min. právo čtení příslušného logu.

V případě zařízení Windows je možné využít dedikovaný klíč pro sledování systémových logů – **eventlog[]**. Hlavním rozdílem oproti klíči **log[]** je, že v tomto případě je možné využít číselné kódy označující zaznamenané události v systému Windows. Podmínkou je, aby sledovaný LOG byl v systému zaznamenáván – je možné vzdáleně nastavit pomocí GPO.

Parent items [DP_Kincl_test](#)

* Name

Type

* Key

Type of information

* Update interval

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible	<input type="text" value="Scheduling"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>
			Remove
Add			

Obr. 6-22 Konfigurace záznamu události z eventlogu – neúspěšné přihlášení [zdroj vlastní]

Konfigurace zobrazená na Obr. 6-22 slouží ke zpracování eventlogu z kategorie Security a zaznamenává logy události s ID 4625, jedná o operaci neúspěšného pokusu o přihlášení k systému Windows. Podobným způsobem probíhá zpracování i pro další systémové události s využitím příslušných ID.

6.3 Monitoring zařízení nepodporujících Zabbix agent

Metody monitoringu zařízení nemusí nutně využívat Zabbix agenta, v některých případech to nemusí být možné. Pro řešenou infrastrukturu se situace týká hlavně síťových zařízení a virtualizačních hypervisorů.

Možnosti, jak konfigurovat jednotlivé způsoby monitoringu jsou detailně popsány v dokumentaci systému. Princip konfigurace zůstává takřka stejný jako v předchozím případě. Zařízení je nejprve nutné do systému registrovat. Na rozdíl od případu agent monitoringu je tentokrát definováno rozhraní jiného komunikačního protokolu, například IPMI:

The screenshot shows the Zabbix host registration interface. The form includes the following fields and options:

- * Host name:** Test_IPMI_server
- Visible name:** Test_IPMI_server
- Templates:** type here to search (with a Select button)
- * Groups:** IMPI monitored devices (with a Select button)
- Interfaces:** A table with columns: Type, IP address, DNS name, Connect to, Port. One interface is defined: Type: IPMI, IP address: 10.5.8.93, Connect to: IP, DNS, Port: 623.
- Description:** Test device for impi monitoring
- monitored by proxy:** zabbix_proxy_U5
- Enabled:**

Obr. 6-23 Registrace zařízení s využitím rozhraní IPMI [zdroj vlastní]

Změnou je v případě IPMI protokolu využití portu 623, v závislosti na nastavení IPMI rozhraní na zařízení je dále nutné na záložce IPMI v horní liště definovat vlastnosti pro IPMI připojení:

The screenshot shows the configuration page for the IPMI interface in Zabbix. The page has a navigation bar with tabs: Host, IPMI (selected), Tags, Macros, Inventory, Encryption, Value mapping. The configuration options are:

- Authentication algorithm:** A dropdown menu with options: Default, None, MD2, MD5, Straight, OEM, RMCP+ (selected).
- Privilege level:** A dropdown menu with options: Callback, User, Operator, Admin (selected), OEM.
- Username:** jkincl
- Password:** [Redacted]

Obr. 6-24 Konfigurace vlastností pro IPMI připojení
[zdroj vlastní]

Zároveň je nutné zajistit, aby využitá proxy byla schopna zpracovávat IPMI dotazy. V prvé řadě je v rámci nastavení podu pro provoz kontejnerů zpřístupnit port 623 a v konfiguraci proxy povolit spuštění procesy pro zpracování IPMI komunikace.

V případě, že je nutné změnit konfiguraci stávající proxy, je nejjednodušší existující pod smazat a vytvořit znovu s novým nastavením – včetně znovuvytvoření jednotlivých kontejnerů. Vzhledem k tomu, že proxy odesílá data na hlavní server, tak ani v případě odstranění proxy a její databáze nedojde ke ztrátě dat. Pokud bude proxy spuštěna se stejným nastavením hostname, není nutné ji znovu registrovat.

Druhou možností je tvorba dedikované proxy pro zpracování IPMI dotazů.

V obou případech je při tvorbě kontejneru proxy nutné přidat další uživatelský parametr:

-e ZBX_IPMIPOLLERS=3

Přidáním výše uvedeného parametru dojde při spouštění kontejneru proxy k nastavení konfigurace a vytvoření třech procesů pro zpracování IPMI komunikace. Počet těchto procesů je nastavitelný v rozsahu 0-1000.

Obdobným způsobem lze proxy nastavit i pro další typy kombinačních protokolů, například SNMP. Kompletní seznam uživatelských parametrů je dostupný v dokumentaci kontejneru proxy [67], vysvětlení všech parametrů pak v dokumentaci Zabbix proxy [59].

Pro IPMI zařízení je následně možné vytvořit dynamický dotaz a načítat hodnoty z IPMI rozhraní:

<input type="checkbox"/>	<u>Test_IPMI_server</u>	<u>IPMI value for sensor 02-CPU 1</u>	34s	40
<input type="checkbox"/>	<u>Test_IPMI_server</u>	<u>IPMI value for sensor 03-CPU 2</u>	34s	40
<input type="checkbox"/>	<u>Test_IPMI_server</u>	<u>IPMI value for sensor 06-P1 DIMM 1-6</u>	34s	25
<input type="checkbox"/>	<u>Test_IPMI_server</u>	<u>IPMI value for sensor 07-P1 DIMM 7-12</u>	34s	25
<input type="checkbox"/>	<u>Test_IPMI_server</u>	<u>IPMI value for sensor 08-P2 DIMM 1-6</u>	34s	28
<input type="checkbox"/>	<u>Test_IPMI_server</u>	<u>IPMI value for sensor 09-P2 DIMM 7-12</u>	34s	26

Obr. 6-25 Ukázka hodnot z testovacího zařízení získaných pomocí IPMI rozhraní [zdroj vlastní]

Podobným způsobem probíhá monitoring zařízení pomocí protokolu SNMP – při registraci zařízení je definováno rozhraní, verze komunikačního protokolu SNMP a tzv. SNMP community – lze si představit jako sdílené heslo pro ověření komunikace.

Dotazy pro získávání dat ze zařízení jsou konfigurovány podobným způsobem jako v ostatních případech, pro identifikaci hodnot se využívají tzv. OID – číselné identifikátory jednotlivých hodnot, které jsou dostupné skrz protokol SNMP.

Pro zařízení CISCO například:

OID = iso.1.3.6.1.2.1.1.3.0

Identifikátor poskytující informace o celkové době od spuštění (uptime) zařízení.

Pro identifikaci dostupných OID na sledovaném zařízení je možné využít některý z dostupných nástrojů, například: **snmpwalk** [68].

Zároveň je možné využít již zmiňované templates systému Zabbix, často existují vzory přímo nastavené pro konkrétní síťová zařízení:



Obr. 6-26 Ukázka dostupných vzorů využívajících protokol SNMP [zdroj vlastní]

6.3.1 Další využití monitorovacího systému

Při využití systému Zabbix nemusí nutně docházet k monitorování konkrétních zařízení, je možné například sledovat dostupnost webových stránek, vyhodnocovat korektnost odpovědi, response time apod.

Konfigurace vždy musí proběhnout jako dotaz z některého ze sledovaných zařízení, pro sledování – prostřednictvím záložky web.

Zde dojde k vytvoření takzvaného scénáře a v rámci něj k definování jednotlivých kroků:

* Steps	Name	Timeout	URL	Required	Status codes	Action
1:	site availability	15s	https://moodle.utb.cz/login/index.php		200	Remove
	Add					

Obr. 6-27 Ukázka sledování dostupnosti webové služby [zdroj vlastní]

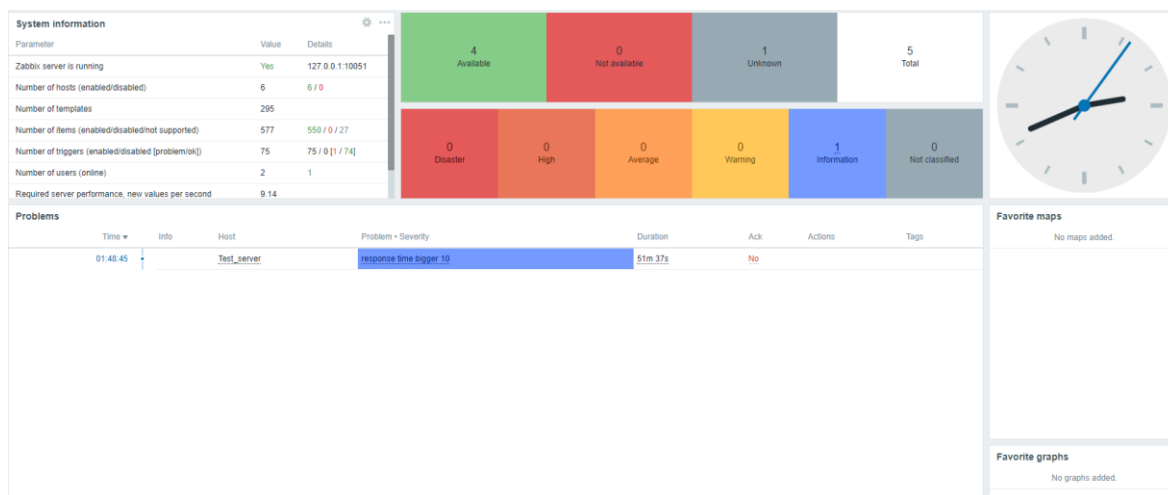
Pravidlo sleduje dostupnost přihlašovací stránky Moodle UTB – v případě HTTP odpovědi 200 (OK) je stránka vyhodnocena jako dostupná. V rámci dotazu jsou automaticky zahrnuty informace o době odpovědi apod.

Další možnosti využití systému Zabbix jsou opět popsány v dokumentaci.

6.4 Grafické vizualizace v systému Zabbix

Jednou z možností, jak dále zpracovávat získaná data a předávat je týmu správců, je tvořit v rámci systému Zabbix grafické vizualizace.

System Zabbix už při instalaci obsahuje některé předdefinované panely. Hlavním panelem je v záložce **Monitoring > Dashboard > All dashboards > Global view**. Tento panel lze označit jako hlavní panel systému:



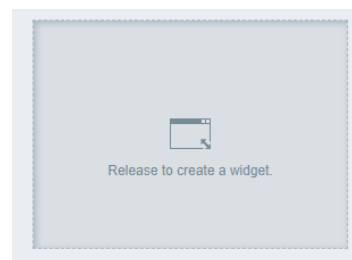
Obr. 6-28 Hlavní panel systému Zabbix [zdroj vlastní]

V rámci panelu jsou umístěny základní informace o monitorovacím systému jako: počet nastavených pravidel, stav monitorovacího serveru, počty připojených hostů a jejich stav. Jednotlivé bloky poskytující informace se nazývají widgety. Tím nejdůležitějším na hlavním panelu je pro správce přehled problémů detekovaných ve sledované infrastruktuře.

Uživatelé mají možnost vytvářet vlastní panely, nebo editovat ty existující. Velikost a uspořádání widgetů v rámci panelu závisí čistě na preferencích uživatele.

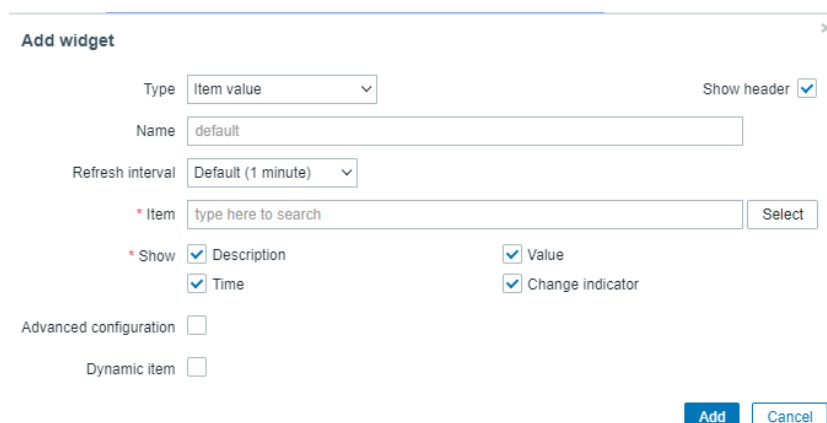
Pro ukázkou konfigurace widgetu je předpokládán scénář, kdy je požadováno na panel přidat widget zobrazující informace o době odezvy sledované stránky z předchozího příkladu.

Je nutné spustit editaci panelu, poté, umístěním myši nad volnou plochu panelu, je možné zatáhnout oblast, která bude představovat nový widget:



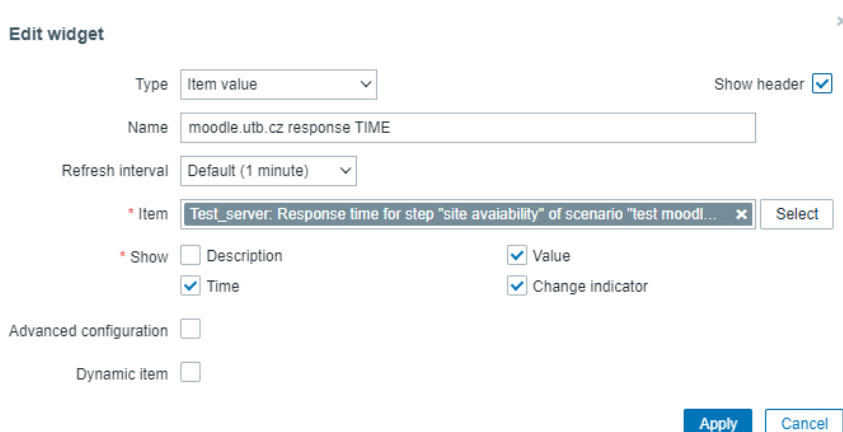
Obr. 6-29 Volba oblasti pro widget
[zdroj vlastní]

Po zvolení velikosti oblasti dojde k otevření konfigurace widgetu:



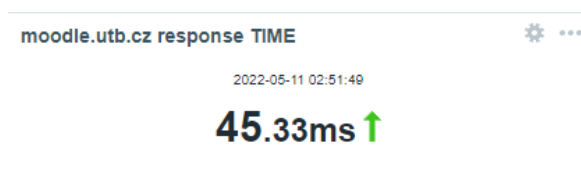
Obr. 6-30 Dialogové okno konfigurace widgetu [zdroj vlastní]

V tomto případě je cílem zobrazit hodnotu itemu, ze zařízení provádějící monitoring webové stránky *moodle.utb.cz*:



Obr. 6-31 Konfigurace pro zobrazení sledované hodnoty odezvy webu moodle.utb.cz [zdroj vlastní]

Výsledný widget bude v rámci panelu vizualizace vypadat následovně:



Obr. 6-32 Grafická vizualizace sledované hodnoty [zdroj vlastní]

Tímto způsobem je možné tvořit panely pro jednotlivé typy zařízení a oddělené týmy správců. Grafické vizualizace slouží jako rychlý způsob předání informací správcovskému týmu.

V případě velkého počtu sledovaných zařízení je možné při konfiguraci jednotlivých panelů narazit na stejná omezení jako při tvorbě jednotlivých dotazů a registraci zařízení. Manuální tvorba by byla příliš časově náročná. Tento problém lze opět vyřešit konfigurací grafické vizualizace v rámci template. Jednotlivé panely jsou nadefinovány již při procesu tvorby vzoru. Následným aplikováním vzoru na koncová zařízení dojde k vytvoření grafické vizualizace pro každé zařízení zvlášť s využitím hodnot získaných ze zařízení.

Jako příklad je uvedena možná podoba grafické vizualizace vytvořené v rámci testovacího template pro Windows zařízení. Vizualizace obsahuje základní provozní data systému:



Obr. 6-33 Grafická vizualizace vytvořená pro testovací zařízení [zdroj vlastní]

Obr. 6-33 zobrazuje generovanou vizualizaci, z té je pro správce možné rychle získat informace o době provozu systému, vytížení procesoru, míře využití paměti RAM. Přehledně je také zobrazeno využití připojených souborových systémů, informace o vybraných síťových portech a základní informace o zařízení a instalovaném agentu systému Zabbix.

7 MOŽNOSTI DETEKCE PROVOZNÍCH VÝPADKŮ A KYBERNETICKÝCH ÚTOKŮ

Jedním z hlavních cílů implementace monitorovacího systému by měla být možnost identifikovat problémové stavy na zařízeních v infrastruktuře. Prakticky vzato se jedná o metody zpracování a vyhodnocení získaných dat.

Základem pro zpracování dat a identifikaci problémů v systému Zabbix jsou tzv. triggers, odpovídajícím českým termínem by mohl být např. spouštěče. Pro zpracování dat je nutné konfigurovat tyto triggers - stejně jako v případě ostatních prvků je lze předdefinovat v rámci template a dostupné vzory obsahují také předpřipravené triggerery. Možnosti konfigurace jsou detailně popsány v dokumentaci systému.

Činnost triggers v systému Zabbix lze vysvětlit následovně: Trigger je vždy vytvořen ve vztahu k některé ze sledovaných hodnot získaných ze zařízení. Trigger obsahuje definovanou podmínku, která je aplikovaná na sledovanou hodnotu. Takto dochází k rozlišení mezi dvěma možnými stavy: Stav **OK** a stav **PROBLEM**.

Například podmínka:

last(/Test_server/web.test.time[test moodle avaiability,site avaiability,resp])>0.100

Sleduje již zmiňovanou dobu odezvy webové stránky Moodle. Konkrétně pro každou nově příchozí hodnotu dojde k vyhodnocení, jestli doba odpovědi byla větší než 100 ms (0.1 s).

V případě, že doba odpovědi byla například 40 ms, podmínka neplatí → trigger je ve stavu **OK** a indikuje, že provozovaný systém je dle nastavených pravidel v pořádku.

V momentě, kdy systém obdrží odpověď po době delší 100ms, podmínka nabude platnosti a stav triggeru se změní na **PROBLEM**.

Změna stavu triggeru vytváří tzv. **action** (akce): dojde k zobrazení informace o problému na hlavním panelu systému (případně v dalších panelech) a zároveň při využití externích komunikačních kanálů (například Slack/E-mail/SMS), je do kanálu při vzniku action odeslána informace o vzniku problémového stavu. Takto správci mohou rychle obdržet upozornění a na vzniklý problém reagovat.

Trigger zůstává ve stavu **PROBLEM** až do vyřešení situace. Při vyřešení situace (doba odezvy se vrátí pod 100ms) se trigger vrací do stavu **OK**. Změna stavu opět vytváří action, problém už není zobrazen na hlavním panelu a do případných komunikačních kanálů je předána zpráva o zániku problému.

Zpracování dat je tedy podmíněno pouze systémem podmínek, které budou pro infrastrukturu nadefinované. Správcovský tým může ve vztahu k získávaným datům definovat libovolné množství různě složitých podmínek. A na základě takto vytvořených podmínek následně dochází k identifikaci problémových stavů v infrastruktuře. Problémové stavy v infrastruktuře mohou být způsobeny provozním výpadkem zařízení anebo mohou souviset s potenciálním kybernetickým útokem. Obecně můžeme všechny problémové stavy označit jako incidenty. Problematika identifikace a klasifikace původu incidentu je opět závislá pouze na nastavených podmínkách.

Využití definovaných podmínek pro detekci incidentů v infrastruktuře je silnou stránkou systému Zabbix. Podmínky lze nastavit pro všechna sledovaná data, takto lze zaznamenat libovolný incident. Na druhou stranu, slabiny systému jsou nutnost tyto podmínky definovat, udržovat jednotlivé podmínky aktuální a reagovat na nově vznikající hrozby. To vše je dodatečně vznikající zátěž na správcovský tým. Dalším problémem pak je složitost rozlišení provozního výpadku a kybernetické hrozby.

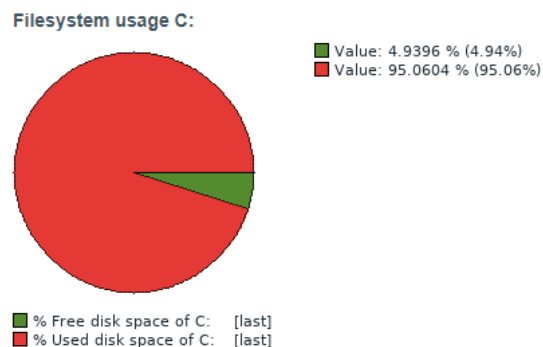
S využitím testovací infrastruktury bylo vytvořeno několik scénářů, na kterých bude výše uvedená problematika blíže vysvětlena s cílem objasnit problém klasifikace povahy incidentů a jejich provázanost.

7.1 Vyhodnocování provozních výpadků

I přes to, že se případy provozních výpadků a případných bezpečnostních incidentů často úzce prolínají, přece jen existují informace o sledovaných systémech, které lze vyhodnocovat z pohledu problematiky provozu.

Nejjednodušším příkladem může být sledování stavu obsazenosti disků na zařízeních v infrastruktuře. Nežádoucím stavem v tomto případě je, aby došlo k vyčerpání diskového prostoru. Takový stav může vést k narušení provozu zařízení, ztráty možnosti přihlášení, deaktivace služeb apod.

Ze zařízení v rámci testované infrastruktury jsou získávány informace o zaplněnosti systémového disku:



Obr. 7-1 Grafické zobrazení zaplněnosti disku
[zdroj vlastní]

Cílem nastaveného pravidla je bude upozornit správce na nedostatek místa. Možná podmínka:

last(/C5-KINCL/pused[C:])>= 90

proměnná **pused** vyjadřuje v procentech míru zaplnění disku – upozornění vzniká v případě, že je zaplněno 90 a více procent.

Po identifikaci problému je na hlavním panelu je dostupné upozornění:

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration
00:05:58	Warning		PROBLEM		C5-KINCL	Less than 10% space disk remaining	2m 18s

Obr. 7-2 Zobrazení problému na hlavním panelu [zdroj vlastní]

Podobným způsobem lze adresovat jakékoliv další parametry související s provozem zařízení. Možné příklady můžou být:

- Vysoká zátěž procesoru
- Vysoké teploty
- Dlouhý system uptime
- Málo dostupné paměti RAM

Pomocí pravidel lze zajistit, že se správcovský tým včas dozví o provozním problému a bude schopný podniknout vhodné kroky řešení tak, aby nedošlo k ovlivnění provozu sledovaného zařízení.

System Zabbix při tvorbě pravidel nabízí také možnost definovat tzv. **predikční pravidla**. Ta využívají historii získaných dat a následnou regresi k určení budoucího stavu sledovaného zařízení.

Příklad:

timeleft(/C5-KINCL/pfree[C:],1h,0)<2h

Výše uvedená podmínka nabude platnosti v případě, že doba do kompletního zaplnění disku bude méně než 2 hodiny. Pro vyhodnocení je použita proměnná *pfree* – volný prostor na disku v % a aproximace je prováděna na základě hodnot z poslední hodiny (1h), 0 označuje stav, který má být vyhodnocen, tedy 0 % volných.

Podobně je možné pomocí funkce **forecast** aproximovat nikoliv dobu do dosažení stavu ale hodnotu sledovaného parametru zařízení v čase. Například kolik % disku bude volných za 7 dní na základě historického vývoje.

7.2 Identifikace bezpečnostních incidentů

Problematika vyhodnocování incidentů v infrastruktuře ve vztahu k bezpečnostním hrozbám je určitě složitější než při identifikaci provozních výpadků. Problémem je vzájemná provázanost incidentů v infrastruktuře a nejasnost jejich původu.

Nejjednodušší opět bude vysvětlit problematiku na příkladech z testovací infrastruktury. Z testovacího zařízení jsou získávány informace o neúspěšném pokusu o přihlášení. Každým pokusem o špatné přihlášení je v logu vytvořen záznam a ten je následně odeslán na monitorovací server:

Source	Severity	Event ID	Value
Microsoft-Windows-Security-Auditing	Failure Audit	4625	Nezdařilo se přihlášení účtu. Předmět: ID zabezpečení: NT AUTHORITY\SYSTEM Název účtu: C5-KINCL\$ Doména účtu: UTB ID přihlášení: 0x3E7 Typ přihlášení: 2 Účet, pro který se nezdařilo přihlášení: ID zabezpečení: NULL SID Název účtu: j_kincl

Obr. 7-3 Uložený záznam při neúspěšném pokusu o přihlášení do zařízení [zdroj vlastní]

Obr. zobrazuje část záznamu o neúspěšném pokusu o přihlášení k systému. V rámci detekce probíhajícího útoku bruteforce = snaha o uhodnutí a prolomení hesla k systému, by mohla být nastavena kontrolní podmínka např:

$$\text{count}(/C5-KINCL/eventlog[Security,,,4625,,all],1m)\geq 5$$

Tedy úplně jednoduše, pokud dojde k zachycení 5 a více neúspěšných pokusů o přihlášení během poslední minuty – je vyhodnocen bezpečnostní incident a může se jednat o probíhající bruteforce útok na zařízení.

Zároveň se ale může pouze jednat o uživatele, kterému se bohužel několikrát nepodařilo úspěšně přihlásit. Zde se projevuje složitost klasifikace incidentu – jedná se o útok, provozní výpadek, nebo chybu uživatele?

Podobná situace může platit například při zaznamenání vysoké vytiženosti procesoru po určitý čas – například:

avg(/C5-KINCL/system.cpu.util[all,system,avg1],1h)>=80

Incident bude zaznamenán v případě, že za poslední hodinu bylo průměrné vytižení procesoru 80 % a více.

Opět vzniká problém s klasifikací incidentu – zařízení mohlo být infikováno škodlivým SW a například byla spuštěna těžba kryptoměny, nebo je zařízení zrovna využíváno pro výpočetní operace v rámci infrastruktury.

Stejná situace platí při sledování zátěže síťového rozhraní – bude zaznamenána velká průměrná zátěž nebo velký počet příchozích packetů. Dojde k zaznamenání incidentu, opět se může jednat o DOS útok na zařízení, nebo dochází ke stahování velkého objemu dat.

Při sledování odezvy webových služeb opět v případě DOS útoku zaznamenáme incident – doba odezvy razantně vzroste nad nastavenou hodnotu. Stejná situace ale může být způsobena provozními problémy zařízení – např. zmiňovaný nedostatek operační paměti, vlivem provozního problému dochází ke zpomalení odezvy webových služeb.

Zde se projevuje vzájemná provázanost jednotlivých incidentů v infrastruktuře a míra úspěšnosti detekce jednotlivých stavů závisí na soustavě nastavených podmínek a jejich komplexitě a vzájemné propojenosti.

Hlavním a velmi podstatným přínosem systému Zabbix je možnost definovat libovolná pravidla pro detekci incidentů v infrastruktuře, nebo identifikaci možných zranitelností (např.: sledování dostupných síťových portů na zařízeních). Z hlediska klasifikace incidentů je nutný dohled správce infrastruktury, ten po obdržení upozornění na detekovaný incident začne vyšetřovat situaci a na základě dalších informací bude schopný rozhodnout, jestli se jedná o probíhající útok, nebo o problém související s provozem zařízení, chybu uživatele apod.

Stále je podstatné, že tým správců je na incident včas upozorněn a je schopný zahájit potřebné kroky pro vyřešení situace. Takto je schopný zabránit provozním výpádkům prvků infrastruktury a zabránit omezení provozu infrastruktury. Z hlediska kybernetických hrozeb

je správcovský tým schopný včas identifikovat vznikající problém a včasným řešením situace zabránit vzniku škod v infrastruktuře.

Jediná limitace detekce incidentů je již několikrát zmiňovaná nutnost definování vhodných pravidel a udržování jejich aktuálnosti. Zároveň některé bezpečnostní hrozby by bylo možné detekovat pouze s použitím komplexních podmínek, které by správcovský tým opět musel udržovat. To v případě nedostatečně početného/financovaného správcovského týmu může být problém.

Částečným řešením problémů s klasifikací incidentů může být porovnávání získaných dat s historickými daty, vždy na odpovídajícím časovém úseku. Takto mohou být jednoduše odhaleny anomálie v provozu infrastruktury.

7.3 Rozšíření možné implementace s využitím OSSIM AlienVault

Právě kvůli zmiňovaným limitacím systému Zabbix a možné složitosti klasifikace bezpečnostních incidentů, případně údržby systému, je navrhovaná implementace monitorovacího systému rozšířena přidáním nástroje AlienVault [69].

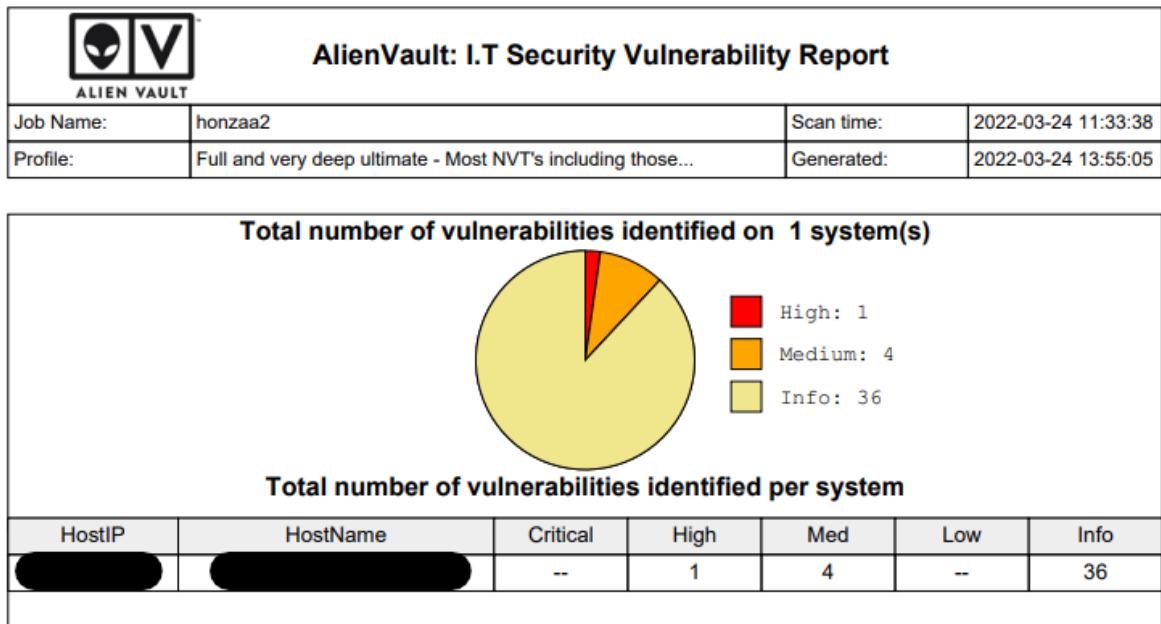
Nástroj AlienVault je open-source SIEM systém, který v případě integrace do infrastruktury může správcovskému týmu pomoci v oblasti detekce a automatické klasifikace bezpečnostních incidentů.

Podobně jako Zabbix i systém AlienVault disponuje aplikací agenta (OTX Endpoint Security), která je určena pro instalaci na koncová zařízení v infrastruktuře. Činnost agenta následně spočívá v analýze bezpečnostních událostí na zařízeních a jejich klasifikaci. Za tímto účelem je využívána tzv. Open threat Exchange (OTX), zjednodušeně si ji lze představit jako komunitně tvořenou databázi, která obsahuje indikátory bezpečnostních hrozeb, identifikátory škodlivých souborů a informace o nově vznikajících zranitelnostech. Díky otevřenosti platformy a spolupráci více než 100 000 ověřených přispěvatelů, je zajištěna stálá aktuálnost bezpečnostní platformy.

Činnost agenta je řízena prostřednictvím webového rozhraní systému, kdy správce infrastruktury zadá požadavek o provedení analýzy zařízení. Agent prověřuje jednotlivá zařízení a vyhledává známky napadení zařízení nebo zranitelnosti v konfiguraci.

Výsledky jsou zobrazeny ve webovém rozhraní systému, nebo je možné využít systém pro vygenerování PDF reportu s výsledky analýzy zařízení.

Report následně obsahuje přehled výsledků analýzy zvolených zařízení (v rámci testovací infrastruktury demonstrováno na 1 zařízení) rozdělený podle závažnosti:



Obr. 7-4 Souhrn výsledků pro zařízení analyzované systémem AlienVault [zdroj vlastní]

A pro každý identifikovaný problém jsou zahrnuty informace o jeho závažnosti, detailní popis, jehož součástí je i vysvětlení možného dopadu a možném způsobu řešení situace:

```

Risk: High
Application: https
Port: 443
Protocol: tcp
Script ID: 11127

CVSS Base Vector:
  AV:N/AC:L/Au:N/C:P/I:P/A:P

Summary:
  It was possible to kill the web server by
  sending an invalid request with a too long header (From, If-Modified-Since, Referer or Content-Type)

Impact:
  An attacker may exploit this vulnerability to make your web server
  crash continually or even execute arbitrary code on the target system.

Solution:
  Upgrade your software or protect it with a filtering reverse proxy.

CVSS Base Score:
  7.5
    
```

Obr. 7-5 Přehled informací o zjištěném problému v reportu AlienVault [zdroj vlastní]

Integrací platformy AlienVault do infrastruktury může správcovský tým zajistit kvalitnější identifikaci bezpečnostních hrozeb. Formou reportů je možné získat přehledné informace o identifikovaných problémech, způsobu jejich řešení.

Díky tomu bude správcovský tým schopen zavčas řešit bezpečnostní nedostatky a tím předcházet potenciálním útokům na infrastrukturu. Další výhodou využití platformy je odlehčení správcovskému týmu z pohledu konfigurace podmínek k identifikaci bezpečnostních incidentů. Rozšíření řešení o platformu AlienVault vhodně doplňuje některé limitace systému Zabbix, hlavně v oblasti klasifikace podstaty incidentů. Kombinací těchto nástrojů (např. po identifikaci incidentu systémem Zabbix si správce v rámci vyšetřování vyžádá analýzu zařízení ze systému AlienVault) vzniká pro správce komplexní nástroj pro správu jejich infrastruktury a je zajištěna určitá míra automatizace jejich činnosti.

ZÁVĚR

V práci byly představeny aktuální problémy související se spolehlivým a bezpečným provozem rozsáhlých infrastruktur. V reakci na neustále se zhoršující situaci v oblasti kybernetické kriminality a zmiňovaná omezení související s provozem infrastruktur, nejčastěji v podobě omezeného rozpočtu pro provoz IT oddělení nebo omezeného počtu správců, byl v práci navržen a popsán možný postup implementace monitorovacího systému pro infrastrukturu.

Na základě porovnání dostupných řešení a zadaných požadavků na realizaci byl implementován monitorovací systém Zabbix. S využitím testovací infrastruktury práce úspěšně představuje možné scénáře použití systému při monitoringu různých typů připojených zařízení. Zároveň formou těchto scénářů práce může pro čtenáře sloužit jako vodítko při vlastní realizaci monitorovacích systémů, stejně tak jako návod při instalaci systému a jeho komponent.

V rámci testovací infrastruktury byly také ověřeny a popsány možnosti detekce incidentů v infrastruktuře a jejich souvislost s provozními výpadky a potenciálními kybernetickými útoky. Vzhledem k popsaným omezením platformy Zabbix práce navrhuje rozšíření řešení o systém OSSIM AlienVault pro identifikaci a klasifikaci bezpečnostních incidentů.

Výstupem práce je postup, který popisuje kombinaci zmiňovaných nástrojů. Takto pro správce infrastruktur vzniká návod, jak vytvořit a implementovat komplexní nástroj, použitelný pro zabezpečení provozního a bezpečnostního monitoringu infrastruktury. Samotné využití těchto nástrojů vede k usnadnění činnosti administrátorského týmu a zkvalitnění jeho služeb.

Díky obecné aplikovatelnosti navrženého postupu na různorodé infrastruktury má práce velký potenciál přispět při zabezpečení dalších počítačových infrastruktur a tím přispět k obecné bezpečnostní situaci kybernetického prostoru.

Dalším důležitým přínosem práce je upozornění na často nedostačený stav zabezpečení stávajících infrastruktur, a hlavně na důležitý problém související s podfinancováním a nedostatkem lidských zdrojů v IT odděleních pečujících o infrastruktury. Upozorněním na tuto problematiku se práce snaží zdůraznit nutnost věnovat se kybernetické bezpečnosti, a tedy opět přispět k navýšení bezpečnosti.

Také byl znázorněn postup identifikace kritických prvků infrastruktury a byla představena kritéria jejich identifikace. Pro řešenou infrastrukturu také bylo detekováno několik potenciálních nedostatků. Identifikace těchto nedostatků může posloužit jako základ pro další práci s infrastrukturou, případně jako vodítko a inspirace při návrhu a revitalizaci dalších infrastruktur.

V neposlední řadě práce naplnila cíl rozšířit expertízu Laboratoře penetračního testování PTLAB získáním nových poznatků, které budou využitelné při další činnosti laboratoře.

Mezi další potenciální budoucí zaměření práce patří využití navrženého systému pro tvorbu izolovaných polygonů pro bezpečnou analýzu a testování zařízení během probíhajících kybernetických útoků. Následným cílem bude na získaných datech ze zařízení odhalit korelaci mezi získanými daty a typem testovaného útoku. Tyto informace by následně mohly být využitelné při návrhu bezpečnostních pravidel s pomocí kterých by docházelo ke spolehlivější identifikaci probíhajících útoků a kritických stavů infrastruktury v reálném čase. Finálním zaměřením takto tvořeného systému bude snaha o automatizaci managementu infrastruktury a jejích obranných mechanismů.

SEZNAM POUŽITÉ LITERATURY

- [1] C. Morris, „14 million US businesses are at risk of a hacker threat,“ 2017. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html>
- [2] S. Morgan, „Cybercrime magazine,“ 2020. [Online]. [cit. 2022-05-15]. Dostupné z: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- [3] SonicWall Inc., „2022 SONICWALL CYBER THREAT REPORT,“ 2022. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf>
- [4] NÚKIB, „NÚKIB vydal Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací,“ 2022. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.nukib.cz/cs/infoservis/hrozby/1823-nukib-vydal-varovani-v-souvislosti-s-ekonomickymi-sankcemi-spojnymi-s-ruskou-federaci/>
- [5] C. Bing a S. Kelly, „Cyber attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed,“ Reuters, 8 Květen 2021. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/>
- [6] NÚKIB, „FN v Brně Bohunicích dnes nahlásila NÚKIBu kybernetický bezpečnostní incident,“ 2020. [Online]. [cit. 2022-05-15]. Dostupné z: <https://web.archive.org/web/20200812092544/https://nukib.cz/cs/informacni-servis/aktuality/1417-fn-v-brne-bohunicich-dnes-nahlasila-nukibu-kyberneticky-bezpecnostni-incident/>
- [7] INTERPOL, „CYBERCRIME: COVID-19 IMPACT,“ 2020. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf>

- [8] H. Teymurlouei a V. Harris, „Effective Methods to Monitor IT Infrastructure Security for Small Business,“ v *International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2019
- [9] „Penetration testing laboratory,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://ptlab.fai.utb.cz/>
- [10] „Fakulta aplikované informatiky UTB ve Zlíně,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://fai.utb.cz/>
- [11] Gartner, „Gartner Glossary,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.gartner.com/en/information-technology/glossary/it-infrastructure>
- [12] IBM, „Why IT infrastructure is important,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.ibm.com/topics/infrastructure>
- [13] R. Hat, „What is IT infrastructure?,“ 2019. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.redhat.com/en/topics/cloud-computing/what-is-it-infrastructure>
- [14] atatus, „IT infrastructure,“ 2021. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.atatus.com/glossary/it-infrastructure/>
- [15] E. University, „What is IT infrastructure ?,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.ecpi.edu/blog/what-is-it-infrastructure>
- [16] S. One, „Cyber Attacks on Small Businesses Increase,“ 2021. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.solveone.com/pages/cyber-attacks-on-small-businesses-increasing-in-2021/>
- [17] Hiscox, „Hiscox Cyber Readiness Report,“ 2019. [Online]. [cit. 2022-05-15]. Dostupné z: <https://web.archive.org/web/20210410015222/https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf>
- [18] J. Galvin, „60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself,“ [Online]. [cit. 2022-05-15]

- [19] CORO, „The Biggest Cyber Security Threats Coming in 2022,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://go.coro.net/cyberthreats2022>
- [20] NÚKIB, „Hrozba kybernetických útoků na nemocnice a jiné významné cíle ČR,“ 2020. [Online]. [cit. 2022-05-15]. Dostupné z: <https://nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/>
- [21] NÚKIB, „NÚKIB a Ministerstvo zdravotnictví vydaly doporučení ke snížení kybernetických hrozeb pro zdravotnická zařízení,“ 2022. [Online]. [cit. 2022-05-15]. Dostupné z: <https://nukib.cz/cs/infoservis/aktuality/1815-nukib-a-ministerstvo-zdravotnictvi-vydaly-doporuceni-ke-snizeni-kybernetickych-hrozeb-pro-zdravotnicka-zarizeni/>
- [22] SOPHOS, „The State of Ransomware 2021,“ 2021. [Online]. [cit. 2022-05-15]. Dostupné z: <https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf>
- [23] F. b. o. investigation, „Internet crime report 2021,“ 2021. [Online]. [cit. 2022-05-15]. Dostupné z: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
- [24] COVEWARE, „Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority,“ 2021. [Online]. [cit. 2022-05-15]
- [25] ESET, „Co je phishing ?,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.eset.com/cz/phishing/>
- [26] Verizon, „2021 Data Breach Investigation Report,“ 2021. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.verizon.com/business/resources/reports/dbir/>
- [27] IBM, „How much does a data breach cost?,“ 2021. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.ibm.com/security/data-breach>
- [28] CISCO, „What Is an Exploit ?,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html>

- [29] OWASP, „SQL Injection,“ [Online]. [cit. 2022-05-15].
Dostupné z: https://owasp.org/www-community/attacks/SQL_Injection
- [30] OWASP, „Cross Site Scripting (XSS),“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://owasp.org/www-community/attacks/xss/>
- [31] Kaspersky, „What is DNS Cache Poisoning and DNS Spoofing ?,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.kaspersky.com/resource-center/definitions/dns>
- [32] D. Gupta, „Cybersecurity Awareness Month: Predicting the Deadliest Cyber Attacks in 2022,“ LoginRadius, 2021. [Online]. [cit. 2022-05-15]
- [33] C. Marinelli, „What is infrastructure monitoring and why is it mission-critical in the new normal?,“ Dynatrace, 2021. [Online]. [cit. 2022-05-15]
- [34] techopedia, „Security Information Management,“ 2015. [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.techopedia.com/definition/4098/security-information-management>
- [35] techopedia, „Security Event Management,“ 2015. [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.techopedia.com/definition/25763/security-event-management>
- [36] techopedia, „What’s the difference between SEM, SIM and SIEM?,“ 2022. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.techopedia.com/7/31201/security/whats-the-difference-between-sem-sim-and-siem>
- [37] C. So-In, „A Survey of Network Traffic Monitoring and Analysis Tools,“ 2006. [Online]. [cit. 2022-05-15].
Dostupné z: https://www.researchgate.net/publication/241752391_A_Survey_of_Network_Traffic_Monitoring_and_Analysis_Tools
- [38] T. Clavel, „What Is NetFlow? How NetFlow Works and Why to Use It,“ 2021. [Online]. [cit. 2022-05-15]. Dostupné z: <https://blog.gigamon.com/2018/01/08/what-is-netflow/>

- [39] J. Hernantes, G. Gallardo a N. Serrano, „IT Infrastructure-Monitoring Tools,“ *IEEE Software*, sv. 32, pp. 88 - 93, 2015.
- [40] TrustRadius, „IT Infrastructure Monitoring Tools,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.trustradius.com/it-infrastructure-monitoring>
- [41] E. Qadah, „15 Best IT Infrastructure Monitoring Tools & Software [2022 Comparison],“ sematext, 2022. [Online]. [cit. 2022-05-15]. Dostupné z: <https://sematext.com/blog/infrastructure-monitoring-tools/>
- [42] M. Wilson, „Best IT Infrastructure Monitoring Tools and Software,“ pcwldd, 2022. [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.pcwldd.com/best-infrastructure-monitoring-tools-and-software>
- [43] Datadog, „Datadog infrastructure monitoring,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.datadoghq.com/product/>
- [44] Dynatrace, „Dynatrace,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.dynatrace.com/>
- [45] elastic, „The Elastic Stack,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.elastic.co/elastic-stack/>
- [46] elastic, „Logstash Reference [8.1] » Input plugins,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.elastic.co/guide/en/logstash/current/input-plugins.html>
- [47] Nagios, „The Nagios IT Management Software Suite,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.nagios.com/products/>
- [48] Nagios, „Nagios // Core feature comparision,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://assets.nagios.com/handouts/nagiosxi/Nagios-XI-vs-Nagios-Core-Feature-Comparison.pdf>
- [49] ManageEngine, „ManageEngine OpManager, the trusted network monitoring software,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://www.manageengine.com/network-monitoring/>
- [50] Prometheus, „What is Prometheus?,“ [Online]. [cit. 2022-05-15]. Dostupné z: <https://prometheus.io/docs/introduction/overview/>

- [51] Pulseway, „Real-time IT management software,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.pulseway.com/it-management-software>
- [52] SolarWinds, „Server & Application Monitor,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.solarwinds.com/server-application-monitor>
- [53] Zabbix, „Explore Zabbix features,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.zabbix.com/features>
- [54] Zabbix, „Zabbix documentation - Agent,“ 2022. [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.zabbix.com/documentation/current/it/manual/concepts/agent>
- [55] Zabbix, „Zabbix BLOG,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://blog.zabbix.com/>
- [56] Zabbix, „Zabbix documentation - Server,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.zabbix.com/documentation/current/en/manual/concepts/server>
- [57] Zabbix, „Zabbix documentation - Web interface installation,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.zabbix.com/documentation/current/en/manual/installation/frontend>
- [58] Zabbix, „Zabbix documentation - Requirements,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.zabbix.com/documentation/current/en/manual/installation/requirements#database-management-system>
- [59] Zabbix, „Zabbix documentation - Proxy,“ 2022. [Online]. [cit. 2022-05-15].
Dostupné z: https://www.zabbix.com/documentation/current/en/manual/appendix/config/zabbix_proxy
- [60] Zabbix, „Zabbix documentation - Getting Zabbix,“ [Online]. [cit. 2022-05-15].
Dostupné z: https://www.zabbix.com/documentation/current/en/manual/installation/getting_zabbix

- [61] Rocky Enterprise Software Foundation, „Rocky Linux,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://rockylinux.org/>
- [62] Containers organization - Github, „Podman,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://podman.io/getting-started/>
- [63] Docker Inc., „Docker,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.docker.com/>
- [64] docker, „dockerhub - mysql,“ [Online]. [cit. 2022-05-15].
Dostupné z: https://hub.docker.com/_/mysql
- [65] Zabbix, „Zabbix Manual,“ 2001-2022. [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.zabbix.com/documentation/current/en/manual>
- [66] Zabbix, „Zabbix agent - item keys,“ 2022. [Online]. [cit. 2022-05-15].
Dostupné z: https://www.zabbix.com/documentation/current/en/manual/config/items/itemtypes/zabbix_agent
- [67] Zabbix, „Dockerhub - Zabbix proxy mysql,“ 2022. [Online]. [cit. 2022-05-15].
Dostupné z: <https://hub.docker.com/r/zabbix/zabbix-proxy-mysql>
- [68] die.net, „Linux man page - snmpwalk,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://linux.die.net/man/1/snmpwalk>
- [69] Alienvault Inc., „AlienVault,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://otx.alienvault.com/>
- [70] Kaspersky, „What is the Deep and Dark Web?,“ [Online]. [cit. 2022-05-15].
Dostupné z: <https://www.kaspersky.com/resource-center/threats/deep-web>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2FA	<i>Two factor authentication</i>	HW	<i>Hardware</i>
AD	<i>Active directory</i>	ID	<i>Identifier</i>
AP	<i>Access point</i>	IEEE	<i>Institute of Electrical and Electronics Engineers</i>
BEC	<i>Business email compromise</i>	INTERPOL	<i>International Criminal Police Organization</i>
CSCI	<i>Computational Science & Computational Intelligence</i>	IOS	<i>Internetwork Operating System</i>
CVE	<i>Common Vulnerabilities and Exposures</i>	IP	<i>Internet Protocol</i>
DB	<i>Database</i>	IPMI	<i>Intelligent Platform Management Interface</i>
DDOS	<i>Distributed Denial-of-Service</i>	IT	<i>Information Technology</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>	JSON	<i>JavaScript Object Notation</i>
DNS	<i>Domain Name System</i>	L2	<i>OSI model - Data link layer</i>
DOS	<i>Denial-of-Service</i>	L3	<i>OSI model – Network layer</i>
ECPI	<i>East Coast Polytechnic Institute</i>	LTS	<i>Long-term Support</i>
ESXi	<i>Elastic Sky X Integrated</i>	NAS	<i>Network-attached storage</i>
FBI	<i>Federal Bureau of Investigation</i>	NDR	<i>Network Detection and Response</i>
FN	<i>Fakultní nemocnice</i>	NPMD	<i>Network performance monitoring and diagnostic</i>
FW	<i>Firewall</i>	NÚKIB	<i>Národní úřad pro kybernetickou a informační bezpečnost</i>
GB	<i>Gigabyte</i>	OID	<i>Object Identifier</i>
GDPR	<i>General Data Protection Regulation</i>	OTX	<i>Open Threat Exchange</i>
GPO	<i>Group Policy Object</i>	OWASP	<i>Open Web Application Security Project</i>
HTTP	<i>Hypertext Transfer Protocol</i>	PC	<i>Personal Computer</i>

PDF	<i>Portable Document Format</i>	SSH	<i>Secure Socket Shell</i>
PHP	<i>Hypertext Pre-processor</i>	SW	<i>Software / Switch</i>
PSK	<i>Pre-Shared Key</i>	ToR	<i>Top-of-Rack</i>
PTLAB	<i>Penetration Testing Laboratory</i>	USA	<i>United States of America</i>
RAM	<i>Random Acces Memory</i>	USB	<i>universal serial bus</i>
SaaS	<i>Software as a service</i>	OS	<i>Operating System</i>
SCCM	<i>System Center Configuration Manager</i>	OSI	<i>Open Systems Interconnection</i>
SEM	<i>Security Event Manager</i>	OSSIM	<i>Open-Source Security Information Management</i>
SIEM	<i>Security Information and Event Manager</i>	USD	<i>United States dollar</i>
SIM	<i>Security Information Manager</i>	UTB	<i>Univerzita Tomáše Bati</i>
SMS	<i>Short Message Service</i>	VLAN	<i>Virtual Local Area Network</i>
SMTP	<i>Simple Mail Transfer Protocol</i>	VM	<i>Virtual Machine</i>
SNMP	<i>Simple Network Management Protocol</i>	VOIP	<i>Voice over IP</i>
SPAM	<i>Irrelevant or unsolicited messages sent over the internet</i>	WMI	<i>Windows Management Instrumentation</i>
SQL	<i>Structured Query Language</i>	XSS	<i>Cross-site Scripting</i>

SEZNAM OBRÁZKŮ

Obr. 0-1 Procentuální podíl výskytu klíčového slova COVID-19 z celkového počtu nahlášených incidentů [7].....	11
Obr. 1-1 Navržená struktura pro primární dělení prvků infrastruktur	17
Obr. 1-2 Navržené rozdělení kategorie HW zařízení	18
Obr. 1-3 Navržené rozdělení kategorie SW infrastruktury	19
Obr. 1-4 Navržené rozdělení osob s přístupem k infrastruktuře	20
Obr. 1-5 Schéma navrhovaného způsobu dělení infrastruktur	21
Obr. 1-6 Porovnání počtu útoků na střední firmy v letech 2019 – 2022 [19].....	23
Obr. 1-7 Procentuální nárůst počtu útoků na jednotlivá odvětví průmyslu Q1 2020 – Q4 2021 [19]	23
Obr. 1-8 Grafické znázornění procesu zabezpečování infrastruktury z publikace na CSCI 2019 [8].....	30
Obr. 2-1 Schéma procesu monitorování infrastruktury	31
Obr. 3-1 Tabulka řešení srovnávaných v článku zabývajícím se problematikou monitoringu infrastruktur [39].....	37
Obr. 4-1 Zjednodušené schéma propojení lokalit prostřednictvím centrálního směrovače	50
Obr. 4-2 Rozdělené řešení infrastruktury dle síťového zapojení	51
Obr. 4-3 Síťové zapojení v rozvodné místnosti	51
Obr. 4-4 Zjednodušený schématický plán počítačové sítě řešené infrastruktury	52
Obr. 5-1 Prvotní návrh implementace monitorovacího serveru do infrastruktury	68
Obr. 5-2 Schéma využití Zabbix proxy [59].....	70
Obr. 5-3 Princip doporučené implementace systému Zabbix pro infrastrukturu	71
Obr. 5-4 Přehled spuštěných komponent systému Zabbix	80
Obr. 5-5 Přihlašovací okno webového rozhraní Zabbix	80
Obr. 5-6 Registrace proxy krok č.1	83
Obr. 5-7 Registrace proxy krok č. 2	83
Obr. 5-8 Registrace proxy krok č. 3	84
Obr. 5-9 Registrace proxy – potvrzení probíhající komunikace	84
Obr. 6-1 Konfigurace instalace Zabbix agenta pro OS Windows	86
Obr. 6-2 Konfigurace Zabbix agenta pro OS Linux – adresa pro pasivní kontroly ..	88
Obr. 6-3 Konfigurace Zabbix agenta pro OS Linux – adresa pro aktivní kontroly ...	88

Obr. 6-4 Registrace monitorovaného zařízení krok č. 1	89
Obr. 6-5 Registrace monitorovaného zařízení krok č. 2	89
Obr. 6-6 Výsledek registrace zařízení	90
Obr. 6-7 Konfigurace automatické registrace zařízení krok č. 1	90
Obr. 6-8 Konfigurace automatické registrace zařízení krok č. 2	91
Obr. 6-9 Přehled registrovaných hostů v testovací infrastruktuře	91
Obr. 6-10 Tvorba dotazu pro sběr dat z testovacího	92
Obr. 6-11 Konfigurace dotazu na dostupnost sledovaného zařízení	93
Obr. 6-12 Ukázka dostupných Templates v systému Zabbix	94
Obr. 6-13 Konfigurace dynamických pravidel pro získání dat krok č. 1	95
Obr. 6-14 Konfigurace master itemu pro monitoring souborových systémů	96
Obr. 6-15 Ukázka návratové hodnoty klíče vfs.fs.get ve formátu JSON	96
Obr. 6-16 Konfigurace discovery rule pro monitoring připojených souborových systémů	97
Obr. 6-17 Nutná konfigurace maker pro identifikaci připojených souborových systémů	97
Obr. 6-18 Konfigurace prototypu itemu – zjištění volného místa na připojených souborových systémech	98
Obr. 6-19 Nastavení preprocessingu dat	99
Obr. 6-20 Konfigurace zpracování hodnoty JSON	99
Obr. 6-21 Ukázka vygenerovaných dotazů pro sledované disky C a D na testovacím zařízení	100
Obr. 6-22 Konfigurace záznamu události z eventlogu – neúspěšné přihlášení	101
Obr. 6-23 Registrace zařízení s využitím rozhraní IPMI	102
Obr. 6-24 Konfigurace vlastností pro IPMI připojení	102
Obr. 6-25 Ukázka hodnot z testovacího zařízení získaných pomocí IPMI rozhraní	103
Obr. 6-26 Ukázka dostupných vzorů využívajících protokol SNMP	104
Obr. 6-27 Ukázka sledování dostupnosti webové služby	104
Obr. 6-28 Hlavní panel systému Zabbix	105
Obr. 6-29 Volba oblasti pro widget	105
Obr. 6-30 Dialogové okno konfigurace widgetu	106

Obr. 6-31 Konfigurace pro zobrazení sledované hodnoty odezvy webu moodle.utb.cz	106
Obr. 6-32 Grafická vizualizace sledované hodnoty	106
Obr. 6-33 Grafická vizualizace vytvořená pro testovací zařízení	107
Obr. 7-1 Grafické zobrazení zaplněnosti disku	110
Obr. 7-2 Zobrazení problému na hlavním panelu	110
Obr. 7-3 Uložený záznam při neúspěšném pokusu o přihlášení do zařízení	112
Obr. 7-4 Souhrn výsledků pro zařízení analyzované systémem AlienVault	115
Obr. 7-5 Přehled informací o zjištěném problému v reportu AlienVault	115

SEZNAM TABULEK

Tab. 1-1 Klasifikace infrastruktur dle způsobu provozu	15
Tab. 1-2 Rozdělení prvků infrastruktur do kategorií podle literatury.....	16
Tab. 1-3 Popis kategorií HW vrstvy infrastruktury	19
Tab. 1-4 Popis kategorií SW vrstvy infrastruktury	20
Tab. 1-5 Popis rolí osob s přístupem k infrastruktuře.....	21
Tab. 1-6 Aktuální typy hrozeb pro infrastruktury.....	27
Tab. 1-7 Doporučení pro zabezpečení infrastruktury	30
Tab. 2-1 Možné typy sledovaných dat při provozním monitoringu	32
Tab. 2-2 Agent vs agent-less monitoring.....	35
Tab. 3-1 Popis porovnávaných monitorovacích systémů	41
Tab. 3-2 Srovnání vybraných monitorovacích systémů	42
Tab. 4-1 Popis prvků HW vrstvy řešené infrastruktury	46
Tab. 4-2 Popis prvků SW vrstvy řešené infrastruktury	48
Tab. 4-3 Scénáře provozního výpadku síťových zařízení řešené infrastruktury	56
Tab. 4-4 Scénáře provozního výpadku ostatních zařízení infrastruktury	58
Tab. 4-5 Popis identifikovaných ekonomicky významných prvků	60
Tab. 5-1 Souhrn požadavků na návrh řešení.....	65
Tab. 5-2 Popis komponent monitorovacího systému Zabbix	68
Tab. 5-3 Souhrn metod instalace systému Zabbix	74

SEZNAM PŘÍLOH

Příloha P I: CD s elektronickou verzí diplomové práce a konfiguracemi

PŘÍLOHA P I: CD

Přiložené CD obsahuje:

- Diplomovou práci ve formátu .pdf: DP_JanKincl_2022.pdf
- Exportovanou konfiguraci instalovaných kontejnerů
- Exportovanou konfiguraci systému Zabbix a jeho prvků