Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Monitoring sítě, implementace bezpečnostních systému ve firmě

Bc. Jan Resler

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jan Resler

Veřejná správa a regionální rozvoj – c.v. Hradec Králové

Název práce

Monitoring sítě, implementace bezpečnostních systémů ve firmě

Název anglicky

Network monitoring and implementation of security systems in company

---

Cíle práce

Cílem diplomové práce je zodpovězení otázky, zda existuje open source nástroj, prostřednictvím kterého lze efektivně chránit počítačovou síť vybrané firmy z pohledu kybernetické bezpečnosti. V teoretické části se budu zabývat kybernetickou bezpečností, aktuálními hrozbami a open source programy určenými k ochraně počítačové sítě. V praktické části budu realizovat průzkum u vybraných společností jehož cílem bude zjištění povědomí o kybernetické bezpečnosti a její pozice v rámci dotazovaných subjektů. Dále navrhnu konkrétní efektivní řešení ochrany počítačové sítě založené na open source programech.

Metodika

Teoretická část práce bude založena na studiu odborné literatury. V rámci praktické části budou použity následující metody

-dotazníkové šetření

-měření

-experiment

-komparace

Na základě zjištěných skutečností budou formulovány závěry diplomové práce.

Doporučený rozsah práce

60-80s.

Klíčová slova

počítačová síť, monitoring, firewall, kybernetická bezpečnost

---

Doporučené zdroje informací

KRETCHMAR, J M. – DOSTÁLEK, L Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. Brno: Computer Press, 2004. ISBN 80-251-0345-5.

KUROSE, J F. – ROSS, K W. Počítačové sítě. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

LUCAS, M W. Networking for Systems Administrators (It Mastery). Gross Pointe Woods: Tilted Windmill Press, 2015. ISBN 978-1642350340.

MAURO, D. – SCHMIDT, K. Essential SNMP, Second Edition. Beijing: O'Reilly Media, 2005. ISBN 05-960-0840-6.

VELTE, T J. – VELTE, A T. – KRÁSENSKÝ, D. Síťové technologie Cisco : velký průvodce. Brno: Computer Press, 2003. ISBN 80-7226-857-0.

Předběžný termín obhajoby

2022/23 ZS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 16. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 26. 03. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Monitoring sítě, implementace bezpečnostních systému ve firmě" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. března 2023 _____

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu práce Ing. Martinu Havránkovi, Ph.D. za jeho odbornou pomoc, cenné rady a trpělivost

Monitoring sítě, implementace bezpečnostních systému ve firmě

Abstrakt

Diplomová práce se soustředí na monitoring se zaměřením na kybernetickou bezpečnost v současném světě závislém na informačních a komunikačních technologiích. Práce zkoumá možnosti využití open source nástrojů, jako jsou Zabbix, Wazuh, Security Onion, OpenVAS a Nmap, pro ochranu a monitoring počítačových sítí a citlivých dat ve společnostech a institucích. Teoretická část se zabývá základními pojmy kybernetické bezpečnosti a analýzou aktuálních hrozeb, zatímco praktická část hodnotí úroveň povědomí o kybernetické bezpečnosti a její důležitost mezi vybranými subjekty. V praktické částí se dále analyzuje efektivní řešení založené na open source nástrojích pro ochranu počítačových sítí a jejich monitoringu. Výsledky by měly poskytnout užitečné informace pro společnosti a instituce hledající ekonomicky dostupná řešení pro zajištění kybernetické bezpečnosti svých informačních systémů a počítačových sítí a bude zodpovězena otázka, zda existuje komplexní open source systém pro monitoring sítí se zaměřením na kybernetickou bezpečnost.

Klíčová slova: počítačová síť, monitoring, firewall, kybernetická bezpečnost, open source nástroje

Network monitoring and implementation of security systems in company

Abstract

The thesis focuses on monitoring with a focus on cyber security in today's world dependent on information and communication technologies. The thesis explores the possibilities of using open source tools such as Zabbix, Wazuh, Security Onion, OpenVAS and Nmap to protect and monitor computer networks and sensitive data in companies and institutions. The theoretical part deals with basic cybersecurity concepts and analysis of current threats, while the practical part assesses the level of cybersecurity awareness and its importance among the selected subjects. The practical part further analyses effective solutions based on open source tools for computer network protection and monitoring. The results should provide useful information for companies and institutions looking for cost-effective solutions to ensure the cyber security of their information systems and computer networks, and the question of whether there is a comprehensive open source system for network monitoring with a focus on cyber security will be answered.

Keywords: computer network, monitoring, firewall, cyber security, open source software

Obsah

1 Úvod

Kybernetická bezpečnost se stala zásadním tématem v současném světě, který je stále více závislý na informačních a komunikačních technologiích. Společnosti a instituce všech velikostí a odvětví bez ohledu na to, zda jsou vlastněny soukromou osobou nebo se jedná o veřejnou správu se musí vyrovnat s různými hrozbami, které se v kyberprostoru vyskytují, a najít způsoby, jak chránit své počítačové sítě a citlivá data. Veřejná správa disponuje omezenými prostředky, které může vynaložit na monitoring sítí a zajištění kybernetické bezpečnosti.

Jednou z možností, jak zajistit bezpečnost informačních systémů, je implementace open source nástrojů pro monitoring sítě a ochranu před kybernetickými hrozbami. Open source nástroje disponují bohatou škálou funkcí a ve většině případů jsou zcela zdarma.

Teoretická část práce se bude zabývat základními pojmy a koncepty kybernetické bezpečnosti, aktuálními hrozbami a open source programy, které jsou určeny k monitorování a ochraně počítačových sítí, jako jsou Zabbix, Wazuh, Security Onion, OpenVAS a Nmap.

V praktické části práce bude proveden průzkum u vybraných subjektů s cílem zjistit úroveň povědomí o kybernetické bezpečnosti a její důležitost v rámci dotazovaných osob. Dále bude navrženo konkrétní efektivní řešení ochrany počítačové sítě založené na open source programech, které bude testováno a zhodnoceno a zodpovězena otázka existence vhodného komplexního nástroje pro monitoring sítě a implementaci bezpečnostních systémů.

Teoretická část poskytne pevný základ pro porozumění kybernetické bezpečnosti a její důležitosti pro ochranu počítačových sítí. Praktická část pak poskytne cenné informace o aktuálním stavu povědomí o kybernetické bezpečnosti v rámci vybraných společností a ukáže, jak mohou open source nástroje přispět k zajištění bezpečnosti a monitoringu počítačových sítí.

Při zpracování práce budou využity různé metodologické přístupy, jako je analýza odborné literatury, studium legislativy, dotazníkové šetření a implementace open source nástrojů v konkrétním prostředí. Tyto metody nám umožní zodpovědět výzkumnou otázku a dosáhnout stanovených cílů práce.

Výsledky diplomové práce by měly přinést užitečné informace o možnostech využití open source nástrojů pro ochranu počítačových sítí ve firmách a institucích, a to nejen z

pohledu technického, ale také z pohledu ekonomického. Práce také nabídne doporučení pro společnosti a instituce, které hledají efektivní a ekonomicky dostupné řešení pro zajištění kybernetické bezpečnosti svých informačních systémů a počítačových sítí, když zodpoví otázku, zda existuje open source nástroj, který bude komplexně pokrývat problematiku monitoringu a bezpečnosti počítačových sítí.

Očekává se, že zjištění z průzkumu povědomí o kybernetické bezpečnosti u vybraných společností a institucí poskytnou cenné informace o tom, jak se firmy a instituce vypořádávají s riziky spojenými s kybernetickou bezpečností a jaké priority kladou na ochranu svých počítačových sítí. Tato zjištění umožní lépe porozumět potřebám a očekáváním firem a institucí v oblasti kybernetické bezpečnosti a umožní navrhnout adekvátní řešení založené na open source nástrojích.

V průběhu implementace open source nástrojů do vybraného prostředí se bude ověřovat jejich funkčnost a efektivita v praxi. Tento proces poskytne důležitý vhled do možností a omezení jednotlivých nástrojů a umožní vyhodnotit jejich vhodnost pro zabezpečení počítačových sítí ve firmách a institucích.

Zhodnocení výsledků průzkumu a implementace open source nástrojů umožní identifikovat nejlepší kombinace a konfigurace nástrojů pro zajištění kybernetické bezpečnosti. Na základě těchto závěrů bude možnost poskytnout doporučení pro firmy a instituce, které hledají efektivní a ekonomicky dostupné řešení pro ochranu a monitoring svých počítačových sítí.

V závěru diplomové práce budou shrnuty hlavní závěry a doporučení, které chtějí využít open source nástroje pro zajištění kybernetické bezpečnosti svých počítačových sítí. Práce tak poskytne ucelený pohled na problematiku kybernetické bezpečnosti ve firmách a představí efektivní a dostupné řešení založené na open source nástrojích.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této diplomové práce je provést analýzu a hodnocení vybraných open source nástrojů pro zajištění kybernetické bezpečnosti a ochrany počítačových sítí vybrané společnosti či instituce a zodpovězení otázky, zda existuje vhodný open source nástroj, prostřednictvím kterého lze efektivně chránit počítačovou síť vybrané firmy nebo instituce z pohledu kybernetické bezpečnosti.

Práce se zaměří na identifikaci vhodných nástrojů, které lze efektivně využít pro prevenci, detekci a reakci na kybernetické hrozby a útoky.

V rámci této práce bude nejprve provedena rešerše současných open source řešení pro kybernetickou bezpečnost a monitoring a jejich klíčových vlastností a funkcí. Následně budou tyto nástroje porovnány z hlediska efektivity, uživatelské přívětivosti, škálovatelnosti a integrace s existujícími technologiemi a procesy.

Dále bude provedeno podrobné hodnocení vybraných nástrojů na základě kritérií, která zohledňují specifické požadavky a potřeby dané společnosti či instituce. Toto hodnocení bude zahrnovat laboratorní testování, simulaci útoků a analýzu schopnosti těchto nástrojů detekovat a reagovat na různé typy kybernetických hrozeb.

Výsledkem práce bude doporučení optimálního open source nástroje pro zajištění kybernetické bezpečnosti a monitoringu v konkrétním prostředí společnosti či instituce. Toto doporučení bude zahrnovat návrh implementace, konfigurace a správy vybraného nástroje, aby bylo dosaženo maximální efektivity a kompatibility s existujícími systémy a procesy.

2.2 Metodika

V první části diplomové práce se provede literární rešerše z dostupných zdrojů s cílem nalézt různé perspektivy na kybernetická bezpečnost, legislativu České republiky a kybernetické hrozby. Provede se analýza různých přístupů ke kybernetickým útokům z pohledu EU a GDPR a bude zjištěn původ, rozdělení a motivace kybernetických incidentů.

Další část práce se zabývá moderními open source nástroji a popisujeme jejich klíčové vlastnosti a možnosti využití pro monitoring a zabezpečení počítačových sítí. Tyto nástroje zahrnují například softwarová řešení pro detekci hrozeb nebo síťové nástroje pro monitorování provozu.

V praktické části práce se provede konkrétní implementace navrženého řešení na počítačové síti organizace. V dalším kroku se tyto nástroje podrobí srovnání z hlediska účinnosti, uživatelské přívětivosti, škálovatelnosti a schopnosti integrovat se stávajícími technologiemi a procesy. Poté následuje podrobné hodnocení vybraných nástrojů na základě specifických požadavků a potřeb dané společnosti nebo instituce. Hodnocení zahrnuje laboratorní testování, simulaci útoků a analýzu schopnosti těchto nástrojů detekovat a reagovat na různé typy kybernetických hrozeb.

Výběr respondentů

Respondenti průzkumu byli vybráni tak, že 50 % respondentů bylo možné kontaktovat osobně a předat jim odkaz na elektronické vyplnění dotazníků a seznámit je s průzkumem. Ostatní respondenti byli osloveni náhodným výběrem a byli požádáni o laskavost vyplnit elektronický dotazník. Do průzkumu bylo zařazeno 12 subjektů a z nich 10 subjektů dotazník vyplnilo.

Vypracování otázek

Stěžejní částí celého provedeného průzkumu byl správný výběr otázek, které byly zařazeny do dotazníku. Tyto otázky by měly pomoci při vyhodnocení výsledků průzkumu, dále by měly objasnit připravenost dotazovaných subjektů v rámci kybernetické bezpečnosti a připravenost IT oddělení obecně. Otázky byly formulovány jasně a srozumitelně tak, aby každý správce sítě, který bude dotazník vyplňovat mohl rychle a správně odpovědět. Z problematiky monitoringu sítě a kybernetická bezpečnosti jsem vybral ty nejdůležitější oblasti, které by měly být pro průzkum zodpovězeny. V dotazníku se nevyskytují otevřené odpovědi a otázky jsou koncipovány na ano nebo ne kromě jedné otázky, kde je možnost vybrat více odpovědí.

Realizace průzkumu

Formuláře Google je webový nástroj pro průzkumy vyvinutý společností Google, který uživatelům umožňuje snadno vytvářet a sdílet vlastní online formuláře, průzkumy a kvízy. Pomocí formulářů Google je možné vytvářet formuláře, které obsahují různé typy otázek, například otázky s výběrem odpovědí, zaškrtávací políčka, krátké odpovědi a další. Formuláře Google nabízejí uživatelsky přívětivé rozhraní, které umožňuje přizpůsobit formuláře pomocí motivů a šablon. Do formuláře je možné také přidávat obrázky, videa a sekce, aby byl poutavější a interaktivnější. Jednou z nejlepších funkcí formulářů Google Forms je jejich integrace s tabulkami Google Sheets. Jakmile se vytvoří formulář a

shromáždí odpovědi, data se automaticky uloží do tabulky Google Sheets, což usnadňuje prohlížení, analýzu a sdílení výsledků s ostatními. Formuláře Google lze použít k různým účelům, například k provádění průzkumů, vytváření registračních formulářů, shromažďování zpětné vazby a organizování akcí. Je to výkonný nástroj pro firmy, pedagogy i jednotlivce, kteří potřebují shromažďovat informace a zpětnou vazbu od svého publika. Celkově jsou formuláře Google všestranným a snadno použitelným nástrojem pro průzkumy, který usnadňuje sběr a analýzu dat online.

Nástrojů pro vytváření dotazníku existuje celá řada. Mezi nejpoužívanější u nás patří zmíněné Google formuláře a dále to jsou Vyplňto, Survio nebo Click4survey.

3 Teoretická východiska

3.1 Kybernetická bezpečnost

Dnešní svět ve 21. století je čím dál více automatizován, technologie jsou na každém rohu, elektromobily jezdí bez nutnosti řízení řidičem a bez počítačové techniky se ve většině případů neobejdeme. Téměř každá domácnost má automobil, ve většině případů jich má i více, každý z rodiny má telefonní přístroj, tablet a také počítač nebo laptop. Každý, kdo nemá profil na sociální síti, je vyčleněn ze společnosti[1].

Ať chceme nebo ne dnešní svět hraje pravidly informačních a komunikačních technologií (dále jen „ICT“) a pokud si člověk nedá ve virtuálním světě pozor, přijde o data nadobro nebo bude muset zaplatit vysokou peněžní částku. S nárůstem techniky a objemu dat na jedné straně, se na druhé straně zvyšuje také riziko, že údaje či data budou odcizeny a už jen těžko se budou získávat zpět. Tento scénář je pro klasickou domácnost méně pravděpodobný, protože data nejsou tak lukrativní a cenná jako u firmy, společnosti, úřadu či vládní organizace. Každé etnikum, národ a společnost má svá pravidla a způsoby, podle kterých se na veřejnosti a v soukromí chová. Tyto pravidla se postupně vyvíjela až do dnešní podoby. Stejně jako kdekoliv, tak i v počítačovém světě existují pravidla chování, které by měl každý uživatel dodržovat. ICT se využívají každý den k interakci s blízkými, zákazníky nebo obchodními partnery, je nutností mít povědomí o kybernetické bezpečnosti. Nízké povědomí o rizicích či zanedbání pravidel totiž může snadno vést k prolomení bezpečnosti a odcizení či zašifrování dat. Útočníci na rozdíl od běžných uživatelů počítače se každý den věnují zdokonalování praktik prolomení do sítě, zkoumání zranitelností operačního systému (dále jen „OS“) nebo hledáním bezpečnostních děr v neaktuálních programech. Toto se nazývá kyberkriminalita, o které je zmíněno tak dále v práci.

Pro správné porozumění světu informačních technologií je potřeba znát určitou terminologii a pojmy, které jsou s ním spjaty. Tato kapitola má za cíl vymezit základní pojmy jako kybernetická bezpečnost, kyberprostor, kyberkriminalita a dále seznámit čtenáře s vládními nařízeními Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NUKIB“) a jeho postoji k bezpečnosti.

[1] Outsider je někdo, kdo stojí na kraji nebo mimo skupinu či společnost

3.1.1 Kyberprostor

Kyberprostor je to virtuální místo, kam se můžeme dostat jen za pomocí výpočetní techniky připojené k Internetu. Kyberprostor tvoří globální síť, která je základem pro online komunikaci. Stejně jako náš svět je tvořen jednotlivými zeměmi a kontinenty, tak i kyberprostor je tvořen menšími počítačovými sítěmi, které jsou rozprostřeny po celém světě a tvoří tak jednu enormní síť. V literatuře se ale můžeme setkat s různými definicemi tohoto pojmu. Příkladem může být definice podle G. Kostopoulose *„Kromě naší fyzické dimenze máme také dimenzi kybernetickou. Kromě toho, že jsme občany země X nebo Y, jsem také občany kyberprostoru. K cestování dovnitř, k pohybu v ní a ven není zapotřebí žádný fyzický pas. Ve skutečnosti tomu tak není a pas nahrazuje IP adresa, která je uložena všude, kde se v kyberprostoru pohybujeme.“* (Kostopoulos, 2017, s. 15, přeloženo autorem).

Vůbec první autor, který se zmínil o pojmu kyberprostor byl William Gibson. Ve svém románu Neuromancer definoval kyberprostor následovně: *„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Neodmyslitelná komplexnost. Linie světla seřazená v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, …“ (*Kolouch a kol. 2019, s 66). John Barlow, zakladatel Electronic Frontier Foundation, napsal deklaraci zvanou „A Declaration of the Independence of Cyberspace”, kde popisuje kyberprostor. Po vydání tohoto díla pojem přichází do obecného povědomí (Kolouch a kol. 2019).

Definicí, jak můžeme kyberprostor popsat je nespočetné množství a každý autor je definuje různě. Zároveň každý jedinec chápe kyberprostor odlišně. Jedna z nejlépe uchopitelných definicí je tato: *„V současné době se kyberprostor neskládá z jednoho homogenního prostoru. Je to nespočet rychle se rozšiřujících kyberprostorů, z nichž každý poskytuje jinou formu digitální interakce a sdělení. Obecně lze tyto prostory zařadit do těch, které existují v rámci technologie internetu, technologie virtuální reality a konvenční telekomunikace, jako je telefon a fax, přestože dochází k rychlé konvergenci technologií vznikají nové hybridní prostory.“* (Dodge, Kitchin 2003, s.1, přeloženo autorem). Z definice vyplývá, že kyberprostor je ovlivňován technologiemi, a to nejen počítačovými. Kyberprostor nemá vymezené hranice, přes které se nemůže dostat. Naopak se stále dynamicky a rapidně vyvíjí a propojuje jednotlivé infrastruktury napříč.

Podle Koloucha je kyberprostor složen z ICT technologií, které komunikují pomocí TCP/IP protokolu, a tím tvoří největší počítačovou síť a počítačové systémy, které jsou součástí této sítě. Uživatelé, kteří tuto síť spravují se nazývají administrátoři neboli správci sítě. Kyberprostor, nemající hranice by však nemohl existovat bez příslušného hardwaru, který se nachází v reálném světě. Je na něj bezpodmínečně vázaný. Kyberprostor lze definovat jako nehmotné médium a stroj nebo server, na kterém běží jako hmotné médium. Hmotným médiem mohou být jednotlivé prvky sítě či počítačové systémy. Tato virtuální realita má specifický charakter a předpokládat, že algoritmy, které používáme v našem světě, budou fungovat i zde je naprosto chybné. Kyberprostor je dnes nazýván jako takzvaná pátá doména a je mu v posledních letech věnována velká pozornost. Bezpochyby lze říct, že uživatelé jsou do značné míry ovlivněni kyberprostorem. Jejich chování v tomto prostředí může ovlivnit i to, co se děje mimo něj. Jeho základní znaky jsou otevřenost, globálnost a zdroj většiny informací (Kolouch a kol. 2019). Z tohoto tvrzení lze usoudit, že kyberprostor nemá konec ani začátek a kdokoliv se v něm může svobodně pohybovat, surfovat, kohokoliv dohledat a kontaktovat. V kyberprostoru je potřeba být obezřetný a racionální, neboť nikdy nevíme, kdo nás může najít a kontaktovat, co tento člověk chce, a zda opravdu existuje. Z toho plyne, že v kyberprostoru lze očekávat padouchy a zločince, kteří budou páchat zločin. V kybernetická bezpečnosti se tomu říká kyberkriminalita.

V posledních letech je kybernetické bezpečnosti věnovaná čím dál větší pozornost, protože dochází k neustálým kybernetickým útokům, a to nejen v zahraničí, ale také v České republice.. V nedávné době byly zaznamenány útoky na nemocnici Benešov, nemocnici svaté Anny v Brně nebo psychiatrické nemocnice v Kosmonosech. Pod nátlakem hackerů nejsou jenom nemocnice, ale také školy a další organizace soukromého a veřejného sektoru. Všechny tyto subjekty má na svědomí útok zvaný ransomware, kterým se budeme zabývat dále v této práci.

3.1.2 Kyberkriminalita

Jednou z hlavních bezpečnostních výzev kyberprostoru a ICT vůbec, je hrozba kyberkriminality. Prakticky každá oblast života dnes závisí na kybernetické infrastruktuře, která je zranitelná vůči útokům. Kybernetická kriminalita a využívání kyberprostoru zločinci je v dnešní době denní rutina, kterou lze v budoucnosti očekávat ve značně větším měřítku. Ještě v nedávné minulosti tomu tak však nebylo a na vnější útok firemní sítě nebyl brán velký důraz. K nárůstu kyberkriminality přispěl rozmach Internetu na konci 20. století,

zejména od 90. let. Od té doby počet uživatelů, kteří jsou připojení k Internetu dramaticky roste. ICT nemají jenom kladnou stranu jako je procházení Internetem, chatování s přáteli na sociálních sítích nebo stahování a nahrávání dat na úložiště. Má také stinné stránky, o kterých většina běžných, nezaškolených uživatelů neví. Díky bleskovému vývoji technologií, exponenciálnímu nárůstu uživatelů připojených do Internetu a nepřipravenosti správců sítě, je pro zločince kyberprostor dalším polem působnosti, kde mohou páchat kriminální delikty.

Podobný názor má i Kolouch, který spojuje rozvoj kyberkriminality s propojením čtyř univerzitních uzlů a vytvoření sítě určené ke sdílení dat. Druhým faktorem rozvoje bylo vytvoření prvního osobního počítače (dále jen „PC“) společností IBM.. Posledním důvodem bylo zpřístupnění Internetu široké veřejnosti. (Kolouch, 2016).

Ucelený pohled na problematiku kyberkriminality má švýcarský autor Kriangsak Kittichaisaree, který tvrdí že kybernetická kriminalita představuje každodenní hrozbu pro každého, kdo se zabývá kybernetickými aktivitami. Aktivity zahrnují: nezákonný přístup k počítačovému systému, nezákonný přístup k počítačovým datům, jejich zachycení nebo získání, výrobu, distribuci nebo držení nástrojů pro zneužití počítače a porušení ochrany soukromí nebo dat. Počítačové trestné činy zahrnují také jednání související s počítačem za účelem osobního nebo finančního prospěchu nebo škody, které spočívá v počítačovém podvodu nebo padělání. V počítačových trestných činech týkajících se identity, v počítačových trestných činech týkajících se autorských práv nebo ochranných známek, v rozesílání nebo kontrole rozesílání nevyžádané pošty, v počítačových trestných činech způsobujících osobní újmu, a ve výrobě, distribuci nebo držení dětské pornografie. (Kittichaisaree, 2017, přeloženo autorem).

Z výše uvedeného lze vyvodit, že ať už se jedná o domácí uživatele nebo firemní zaměstnance, kteří mají ze svého zařízení přístup k Internetu, jsou vystaveni vážnému riziku, že se stanou obětí kyberzločinu.

Podle Koloucha můžeme nejobecněji definovat kyberkriminalitu jako „*Jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu“* (Kolouch, 2016, s. 35). Kolouch dále doplňuje, že před definováním pojmu kyberkriminalita je zároveň nutné vymezit i pojem kriminalita a to jako „*Souhrn všech jednání, která lze podřadit pod některou skutkovou podstatu, upravenou trestním zákonem. Podle tohoto vymezení tedy nejsou kriminalitou*

taková jednání, která nenaplňují žádnou skutkovou podstatu trestného činu, tedy ani přestupku či jiného správního deliktu.“ (Kolouch, 2016 s. 36).

3.1.3 Legislativa

V České republice existuje mnoho právních předpisů, které se týkají kybernetické bezpečnosti a ochrany osobních údajů. Některé z těchto předpisů jsou součástí evropského práva, například Obecného nařízení o ochraně osobních údajů (GDPR), zatímco jiné jsou vnitrostátní právní předpisy, jako například zákon o kybernetické bezpečnosti nebo zákon o ochraně osobních údajů.

Zákon o kybernetické bezpečnosti byl přijat v roce 2018 a vstoupil v platnost v roce 2019. Tento zákon stanovuje základní požadavky na kybernetickou bezpečnost, včetně požadavků na ochranu kritické infrastruktury a na hlášení kybernetických incidentů. Zákon také ukládá povinnosti pro správce kritické infrastruktury a pro poskytovatele informačních služeb, aby zajistili bezpečnost svých systémů a služeb.

Zákon o ochraně osobních údajů byl přijat v roce 2018 a implementuje GDPR do vnitrostátního práva. Tento zákon stanovuje požadavky na ochranu osobních údajů, včetně požadavků na zpracování, uchování a ochranu osobních údajů. Zákon také ukládá povinnosti pro správce osobních údajů a pro subjekty, které zpracovávají osobní údaje jako subdodavatelé, aby zajistili bezpečnost osobních údajů a ochranu soukromí.

V roce 2020 byla přijata novela zákona o kybernetické bezpečnosti, která mimo jiné stanoví nové požadavky pro správce kritické infrastruktury a pro poskytovatele informačních služeb, a to včetně povinností týkajících se hodnocení rizik a implementace opatření na zajištění kybernetické bezpečnosti.

Celkově lze říci, že právní předpisy v oblasti kybernetická bezpečnosti v České republice se neustále vyvíjejí, aby se zlepšila ochrana osobních údajů a snížila se rizika kybernetických útoků. Je důležité, aby organizace a jednotlivci dodržovali tyto předpisy a zajistili tak bezpečnost svých informačních systémů a ochranu osobních údajů.

3.2 Kybernetické hrozby

Kybernetický útok je útok vedený kyberútočníky pomocí jednoho nebo více počítačů proti jednomu nebo více počítačům či sítím. Kybernetický útok může zákeřně vyřadit z provozu počítače, ukrást data nebo použít napadený počítač jako výchozí bod pro další útoky.

Kromě kybernetické kriminality mohou být kybernetické útoky spojeny také s kybernetickou válkou nebo kyberterorismem. Motivace mohou být různé, zejména existují tři hlavní kategorie: kriminální, politické a osobní.

Kriminálně motivovaní útočníci usilují o finanční zisk prostřednictvím krádeže peněz, odcizení dat nebo narušení chodu podniku. Stejně tak osobně motivovaní útočníci, jako jsou nespokojení současní nebo bývalí zaměstnanci, využijí peníze, data nebo pouhou příležitost narušit systém společnosti. Primárně však usilují o odplatu. Společensky a politicky motivovaní útočníci usilují o pozornost pro své cíle. V důsledku toho upozorňují na své útoky veřejnost. Mezi další motivace kybernetických útoků patří například špionáž.

3.2.1 Typy malware

Malware, zkratka pro „škodlivý software“, je obecný termín používaný k popisu všech typů softwarových programů, které mohou poškodit nebo ukrást data z cílového počítače. Většinu typů malware musí uživatel spustit, aby mohl spustit svůj škodlivý kód a rozšířit se do dalších počítačů a sítí. Malware lze šířit ručně (fyzicky) pomocí disket, CD/DVD a USB flash disků a dalších vyměnitelných médií a také prostřednictvím sítí (jako jsou přílohy e-mailů, pirátský software, bezplatné internetové programy a sociální sítě). Ovlivňují různé typy operačních systémů (Windows, Linux, Unix, Android, iOS a Mac). Existují různé kategorie malware, z nichž každá má mnoho podtypů. Níže je uveden přehled některých typů škodlivých programů.

Grubb definuje malware jako „*Poškození způsobené neoprávněnou akcí, která je považována za neobvyklou pro daný systém. Normální operace může například zahrnovat přihlášení uživatele do systému pomocí uživatelského jména a hesla nastaveného interním správcem. Pokud aplikace umožní černému klobouku přístup do systému bez použití uživatelského jména a hesla, provedla neautorizovanou akci*“ (Grubb, s. 56, 2021).

Ransomware

Ransomware je typ malware, který odepře přístup k souborům uživatele, někdy zašifruje celý pevný disk nebo dokonce všechny připojené externí pevné disky a sdílené síťové položky, a poté požaduje, aby uživatel zaplatil výkupné za znovu získání přístupu k systému a jeho datům. Analýza je primárně zaměřena na ransomware, ale v zásadě platí i pro většinu malware. Doporučené postupy jsou zejména obecné, neboť eliminují zranitelnosti sítě a koncových stanic (včetně mobilních telefonů), čímž zároveň snižují možnost šíření dalšího malware a hackerských útoků.

Jenkinson definuje ransomware jako typ malware z oblasti krypto virologie, který typicky hrozí zveřejněním dat oběti nebo zablokováním přístupu k nim, pokud nebude zaplaceno výkupné (Jenkinson, 2022, přeloženo autorem).

Phishing

Phishing je forma kybernetického útoku, při kterém se útočník snaží získat citlivé informace, jako jsou hesla, uživatelská jména, kreditní karty nebo bankovní údaje tím, že se vydává za důvěryhodnou osobu nebo organizaci. Typicky to probíhá tak, že útočník pošle oběti e-mail nebo zprávu s odkazem na falešnou webovou stránku, která vypadá jako legitimní, ale ve skutečnosti slouží k získání citlivých informací od oběti. Například falešná webová stránka může vyzývat uživatele k zadání svého uživatelského jména a hesla, což poté může útočník použít k získání přístupu k osobním účtům uživatele. Phishing je běžnou technikou používanou k podvodům a krádežím identity a je důležité být opatrný a obezřetný při otevírání e-mailů a klikání na odkazy od neznámých odesílatelů.

Grubb popisuje, že útočníci využívající phishing se snaží vystupovat jako legitimní osoby nebo organizace a nabízejí nějakou odměnu nebo prezentují krizi, kterou může vyřešit pouze osoba, kterou kontaktují. Mohou například předstírat, že jsou z banky a sdělit, že "se musí okamžitě reagovat a sdělit údaje o účtu, jinak bude účet zablokován". Přidáním naléhavosti a zastrašováním doufají, že vyděsí osobu, kterou kontaktují natolik, že udělá, co požadují, aniž by byla prohlédnuta jejich taktika. Při těchto pokusech obvykle hledají údaje, jako jsou osobní identifikační údaje, čísla kreditních karet nebo hesla k důležitým online účtům, jako jsou bankovní nebo e-mailové účty. Někdy tyto informace požadují přímo v e-mailu. Často žádají, aby oběť klikla na odkaz na webovou stránku, která napodobuje skutečnou webovou stránku, ale ve skutečnosti je to škodlivá stránka, která ukradne a zaznamená všechny informace, které se na ni zadají. (Grubb, 2021, přeloženo autorem).

Spyware

Spyware je druh škodlivého softwaru (malware), který se nainstaluje na počítač bez vědomí uživatele a sleduje jeho aktivity, aby získal citlivé informace, jako jsou hesla, bankovní údaje, historie prohlížení webových stránek a další. Tento druh škodlivého softwaru se často šíří prostřednictvím spárování se s legitimním softwarem, který uživatel stáhne a nainstaluje na svůj počítač. Spyware může také způsobit zpomalení počítače a jeho nestabilitu. Existuje mnoho různých typů spyware, včetně adware, keyloggerů, trackingu, hijackerů a dalších.

Kromě spárování s legitimním softwarem se spyware může šířit také prostřednictvím phishingových emailů, nelegálních webových stránek a neaktualizovaného softwaru. Je také důležité zmínit, že spyware se často vyskytuje spolu s dalšími druhy škodlivého softwaru, jako jsou viry, trojské koně a ransomware. Proto je důležité mít na svém počítači kvalitní antivirový software a pravidelně aktualizovat operační systém a další software. Pokud existuje podezření na infekci spywarem, je vhodné spustit antivirový sken a provést další kroky k odstranění škodlivého softwaru z počítače.

Distributed Denial-Of-Service

Útoky DDoS (Distributed Denial-of-Service) patří k nejčastějším a nejničivějším hrozbám, na které si obránci sítí musí dávat pozor. Při tomto útoku lidé se zlým úmyslem používají nástroje, které jsou často dostupné na síti, k narušení webových stránek, databází nebo podnikových sítí tím, že nejprve shromáždí informace o jejich slabinách a později je využijí. DDoS je koordinovaný útok, který je veden pomocí velkého počtu napadených hostitelů. Útok DDoS je považován za útok s vysokou rychlostí, pokud generuje velké množství paketů nebo extrémně velký objem provozu během velmi krátké doby a narušuje tak služby. Útok se referuje jako útok s nízkou rychlostí, pokud je veden v průběhu minut nebo hodin. Pro boj s útoky DDoS bylo vyvinuto několik významných obranných mechanismů. (Bhattacharyya, 2016, přeloženo autorem).

Na základě interních dat Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) byl v říjnu 2022 zaznamenán neobvykle vysoký počet DDoS útoků. Celkem 13 incidentů, což téměř dorovnává souhrnné hodnoty za prvních devět měsíců roku 2022. K části říjnových útoků se na svém telegramovém kanále přihlásila skupina Anonymous Russia. Je důležité podotknout, že zvýšený počet útoků byl pozorován již v dubnu roku 2022, kdy se české organizace staly obětí útoků ruskojazyčné skupiny Killnet.

Tyto údaje svědčí o nutnosti věnovat zvýšenou pozornost zabezpečení proti DDoS útokům a řešit tuto problematiku jako prioritní oblast v oblasti kybernetické bezpečnosti (NÚKIB, 2022).

Jedním z nejúčinnějších způsobů, jak se bránit proti útokům DDoS, je použití specializovaných nástrojů pro detekci a filtraci provozu. Tyto nástroje dokážou rozlišovat mezi legitimním provozem a provozem pocházejícím z botnetů nebo jiných zdrojů, které jsou součástí útoku DDoS. Další obrannou strategií je použití CDN (Content Delivery Network), které jsou navrženy tak, aby minimalizovaly dopad útoku na webové stránky a zákazníky. Tyto sítě fungují tak, že umožňují distribuovat obsah na mnoho serverů po celém světě, čímž minimalizují dopad útoku na jakýkoli jednotlivý server.

Kromě těchto technických opatření mohou organizace také provádět různá cvičení a tréninky, aby zlepšily schopnost svých týmů reagovat na útoky DDoS v reálném čase. Je důležité, aby všichni zúčastnění měli jasnou představu o tom, jak postupovat v případě útoku, a aby byli dostatečně obeznámeni s dostupnými nástroji a technologiemi.

Závěrem je třeba podotknout, že útoky DDoS se stávají stále sofistikovanějšími a útočníci používají stále nové a vylepšené techniky. Proto je důležité, aby organizace neustále aktualizovaly své obranné mechanismy a zůstávaly v obraze s nejnovějšími trendy a technologiemi.

3.2.2 Typy ransomware

Existují dva hlavní typy ransomware: šifrovací ransomware a zamykací ransomware. Ransomware však spadá do kategorie kybernetické kriminality digitálního vydírání, která zahrnuje i další typy kybernetické kriminality zaměřené na nelegální získání nebo odepření přístupu k datům výměnou za výkupné. V této části probereme typy ransomware a různé typy kybernetické kriminality, které spadají pod digitální vydírání.

Locker Ransomware (uzamykací)

Locker ransomware funguje tak, že brání obětem v přístupu k jejich osobním souborům tím, že jim odepře přístup k operačnímu systému (například uzamkne plochu nebo zabrání oběti v přihlášení) a poté požaduje výkupné, aby uživatel mohl znovu získat přístup. Ve srovnání s krypto vyděračskými válkami používá typický typ vyděračské války relativně jednoduché techniky k odepření přístupu k osobním souborům, které mohou zkušenější

uživatelé překonat. Výsledkem je, že skripty ransomware mohou být odstraněny z infikovaných systémů, aniž by to ovlivnilo základní operační systém a soubory.

Crypto ransomware

Ransomware zašifruje všechna data na cílovém počítači a drží uživatele jako rukojmí, dokud oběť nezaplatí výkupné a nezíská od útočníka dešifrovací klíč. Některé varianty krypto-ransomware postupně mažou soubory obětí nebo je zveřejňují, pokud oběti nezaplatí výkupné včas. Moderní rodiny ransomware jsou z velké části založeny na tomto typu. Bez záloh pro obnovu z útoků před ransomware to může mít zničující účinky, zejména pro podniky a vládní organizace. V tomto případě má oběť pouze jednu možnost, jak zašifrovaná data obnovit, a tou je zaplacení výkupného.

3.2.3 Rozdíly mezi ransomware a dalším malware

Jak již bylo zmíněno, ransomware je podtyp malware, ale existuje mnoho různých vlastností, které jej odlišují od jiných typů malware.

Některé typy malware jsou navrženy tak, aby ukradly důvěrné informace uživatelů (jako jsou uživatelská jména, hesla, stisknutí kláves a osobní soubory) nebo poskytovaly vzdálený přístup k zařízením obětí. Škodlivější typy malware způsobí poškození konfigurace (např. smazání souborů, změny systému) nebo přeformátování a poškození základního operačního systému a souborů operačního systému, čímž se stanou nefunkčními. Ransomware na druhou stranu zašifruje soubory oběti a oznámí jejich existenci tím, že požaduje výkupné. Konečným cílem ransomware je vydírat a platit od obětí, aniž by došlo k poškození operačního systému nebo uložených dat. Ransomware pro šifrování nevyžaduje administrátorská práva k počítači oběti. Na rozdíl od jiného malware, který k provádění škodlivých akcí obvykle vyžaduje přístup správce k cílovému počítači. Ransomware šifruje všechna dostupná data, včetně místního úložiště a síťového úložiště. V mnoha případech využívá neošetřené zranitelnosti a získává přístup k dalším souborům, ke kterým se uživatel nedostane, a zašifruje data. Šifrování ransomware má schopnost zašifrovat všechny typy souborů a některé typy ransomware mají schopnost zakódovat názvy souborů, takže oběti neznají skutečný počet nebo názvy zašifrovaných souborů.

3.2.4 Primární cíle útoků Ransomware

Před rokem 2015 byla většina obětí ransomware jednotlivci, ale v roce 2015 se operátoři ransomware zaměřili na podniky a akademické organizace, aby na svých útocích

vydělali více peněz. V těchto případech jsou primárními cíli soubory a databáze Microsoft Office. Firmy jsou velkým cílem ransomware.

Ransomware však napadá různé oběti, jako jsou celebrity, politici, jednotlivci, veřejné organizace, soukromé organizace, a dokonce i charitativní a neziskové organizace. Ransomwarové kampaně jsou realizovány v dávkách (například zasíláním nevyžádaných e-mailů s odkazy na stažení ransomware), aby infikovaly co nejvíce zařízení. Zdravotnictví bylo hlavním cílem ransomwarových útoků v roce 2016 z mnoha důvodů. Rychlé přijetí IT technologií nemocnicemi a zdravotnickými středisky nebylo doprovázeno nezbytným školením v oblasti bezpečnosti IT, které by se vypořádalo s potenciálními kybernetickými útoky.

Ransomware infikuje téměř všechny typy IT zařízení, včetně serverů, mobilních zařízení a mnoha typů zařízení IoT, s výjimkou úložných zařízení připojených k počítačům obětí, jako jsou USB flash disky, SD karty, digitální fotoaparáty a externí pevné disky.

Většina ransomwarových kampaní cílí na zařízení se systémem Windows a Android, protože tyto dva operační systémy dominují celosvětovému podílu operačních systémů podle nejnovějších statistik zveřejněných StatCounterem v roce 2019.

V poslední době jsou pozorovány změny v trendech v oblasti ransomware, zejména v jeho cílení. Historicky byli jednotliví soukromí uživatelé nebo náhodné společnosti hlavními oběťmi ransomware. Nicméně v posledních letech se tento trend změnil a ransomware cíleně útočí na konkrétní firmy, podniky a organizace.

Společnost ESET na svém webové portálu v příspěvku o ransomware napsala: „*V květnu 2017 zaútočil po celém světě WannaCryptor alias WannaCry, který se rapidně šířil kvůli uniklému exploit kitu EternalBlue z Národní bezpečnostní agentury v USA. Ten úspěšně využíval zranitelnost v nejpopulárnějších verzích operačního systému Windows, a to i navzdory faktu, že Microsoft vydal opravný balíček již několik měsíců před vypuknutím nákazy. Výsledkem bylo nakažení tisíců firem po celém světě a škody v řádech miliard dolarů.Hned měsíc poté vypukla další ransomware nákaza v podobě Diskcoder.C také známý jako (Not)Petya, která se zpočátku šířila pouze na Ukrajině, ale postupně se dostala do celého světa. Tentokráte byla zneužita chyba v populárním účetním programu. I když škodlivý kód (Not)Petya primárně cílil na ukrajinské organizace a firmy, došlo i na globální firmy jako je např. Maersk, Merck, Rosneft nebo FedEX. Škody se počítaly na milióny dolarů* “ (ESET, 2022). Příspěvek popisuje dva případy ransomware útoků, které se staly v roce

2017. První z nich, WannaCry, se rychle rozšířil po celém světě díky zranitelnosti operačního systému Windows, na kterou byl úspěšně využit exploit kit EternalBlue. Tento útok způsobil škody v řádech miliard dolarů. Druhý útok, (Not)Petya, se původně objevil na Ukrajině a využil zranitelnost v účetním programu, aby se šířil po celém světě. Tento útok způsobil škody za miliony dolarů a postihl nejen ukrajinské organizace, ale také globální firmy jako Maersk, Merck nebo FedEx. Tyto dva případy ilustrují rostoucí hrozbu, kterou ransomware představuje pro organizace a firmy po celém světě.

Existují dva hlavní důvody, proč jsou firmy, organizace a veřejné instituce stále častějšími cíli ransomware. Za prvé, tyto subjekty jsou často pod velkým tlakem svých zákazníků nebo veřejnosti, aby co nejdříve obnovily své služby. Pokud ransomware úspěšně zašifruje klíčová data potřebná k provozu obchodní společnosti, každý den, kdy není schopna plnit své zakázky přichází o zisk. V případě dopravní infrastruktury, jako jsou letiště, přístavy a vlaková nádraží, může napadení malware způsobit i poškození reputace. V případě státních a městských institucí může nedostupnost služeb způsobit negativní reakci veřejnosti, zatímco v případě zdravotnických zařízení může ohrozit zdraví pacientů nebo dokonce vést k smrti. Za druhé, tyto subjekty obvykle disponují většími finančními prostředky. V kombinaci s tlakem na obnovení služeb a udržení dobrého jména se oběti z řad firem a státních organizací často rozhodnou zaplatit požadovanou výkupné (NÚKIB, 2020).

3.2.5 Požadavky na oznámení útoků Ransomware

Jakýkoli typ kybernetického útoku může mít právní následky, zejména pokud zahrnuje ohrožení nebo narušení osobních údajů uživatelů. Prvním právním problémem, který je potřeba zvážit při útoku ransomware, jsou požadavky na oznámení. Požadavky na oznámení závisí na jurisdikci a typu odvětví. Například ve Spojených státech mají všechny státy zákony o deliktech. Podle těchto zákonů musí oběti (např. společnosti, charitativní organizace, vzdělávací instituce), instituce, poskytovatelé služeb, stránky sociálních sítí nebo jakýkoli subjekt a webová stránka, která uchovává osobní údaje o svých klientech, oznámit úřadům jakékoli porušení zabezpečení Zahrnuje přístup k osobním údajům uživatele.

V České republice a v rámci EU existuje několik právních předpisů. zvláště:

- Zákon č. 110/2019 Sb., o zpracování osobních údajů. Zákon zapracovává příslušné předpisy EU, přičemž se řídí přímo použitelnými předpisy EU, upravujícími práva

a povinnosti zpracovávat osobní údaje za účelem realizace práva každého na soukromí.

- Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o zrušení rámce Rady pro předcházení, vyšetřování, odhalování nebo stíhání trestných činů nebo o volném pohybu těchto údajů příslušnými orgány Rozhodnutí 2008/977/SVV ukládat trestní sankce.
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecná předpisy o ochraně údajů).
- Návrh zákona č. 181/2014 Sb., novely kybernetické bezpečnosti a souvisejících zákonů (návrh zákona o kybernetické bezpečnosti).

V Evropské unii Obecné nařízení o ochraně osobních údajů (25. května 2018), přijaté za účelem ochrany soukromí občanů EU, vyžaduje od společností, které zpracovávají osobní údaje občanů EU, aby do 72 hodin nahlásily jakékoli porušení zabezpečení údajů. Pokuta za porušení tohoto pravidla je vysoká (4 % celosvětového ročního rozpočtu nebo 20 milionů eur) (EUR-Lex.europa.eu, 2016, přeloženo autorem).

Vzhledem k tomu, že hrozba ransomware neustále roste a diverzifikuje se, společnosti, které shromažďují/zpracovávají osobní údaje uživatelů, si musí být vědomy zákonných požadavků na hlášení v případě narušení dat, aby se předešlo opožděnému oznámení a později zbytečně vysokým pokutám.

Ransomware se ukázal jako vysoce efektivní forma kybernetického útoku postihující podniky i jednotlivce. V této části se popisuje ransomware, jak funguje, jeho typy a jak se liší od ostatních typů malware.

3.2.6 Distribuční metody ransomware

Ransomwarové kampaně každým rokem eskalují a útoky po celém světě přibývají. Nikdo se nezdá být vůči těmto hrozbám imunní. Autoři malware neustále vyvíjejí nové a sofistikované varianty ransomware, které se mohou vyhnout detekci a používat nové techniky k infikování více systémů. Zejména z tohoto důvodu a rychle rostoucího průmyslu ransomware a ransomwarových infekcí je důležitá prevence a nasazení účinných nástrojů. Je zřejmé, že je nutné se věnovat různým typům útoků, které ransomware používá k

infikování počítačových systémů, pro získání přehledu o všech možných způsobech, jak je infekce ransomwarem zatím známa. Ostatní malware používá prakticky stejné techniky a přístupy k útoku. V budoucnu se očekává, že tyto cesty budou pokračovat, pouze se bude zlepšovat technologie a nově objevené zranitelnosti budou využívány ve všech možných zařízeních.

E-mail

E-mail je největší bránou, kterou kyberzločinci používají k šíření ransomware. Ransomware a další typy malware mohou využívat e-mailové služby k šíření tak, že se „maskují“ jako přílohy e-mailů. Když si nevědomý uživatel stáhne a otevře škodlivou přílohu, ransomware okamžitě infikuje systém. Další technikou distribuce ransomware prostřednictvím e-mailu je vložení odkazu (URL) do těla e-mailu na škodlivý web, který obsahuje ransomware. Když uživatelé kliknou na tyto odkazy, jsou přesměrováni na škodlivé webové stránky, které infikují jejich systémy.

Vzdálená plocha (RDP - Remote Desktop Connection)

S rychlým růstem globální internetové komunikace mnoho společností outsourcuje svou IT podporu. Tito dodavatelé mohou být ve stejné zemi nebo v zámoří. Aby jim systém Windows pomohl monitorovat a odstraňovat problémy se sítěmi Windows, poskytuje vestavěnou funkci nazvanou Protokol vzdálené plochy (RDP) (k dispozici také v jiných operačních systémech), která uživatelům umožňuje zrcadlit obrazovku, klávesnici a myš vzdáleného systému. na místním zařízení. RDP používá pro komunikaci port 3389.

Útočníci mohou k získání pověření RDP použít hrubou sílu (pomocí slabých hesel) a techniky sociálního inženýrství. Jakmile jsou tyto informace dostupné, otevře se cesta. Kromě infiltrace do cílených sítí mohou zločinci do počítačů obětí instalovat jakýkoli typ malware.

Zranitelnost Zero-Day

Zero-day zranitelnosti jsou chyby, které nebyly zjištěny dodavatelem nebo antivirovým softwarem. Jedná se o zranitelnosti objevené black hat hackery, které se obvykle nacházejí ve webových prohlížečích, zásuvných modulech prohlížečů nebo aplikacích. Někdy mohou existovat v samotném operačním systému. Zločinci zneužívají tyto zranitelnosti k provádění svých špatných úkolů (například infikování počítačů ransomwarem), aniž by se museli obávat maření útoků antivirů a dalších bezpečnostních řešení. I hodina stačí na to, aby škodlivý nástroj infikoval systém malwarem. Doporučujeme nasadit některé z těchto neobjevených nástrojů k předvídání pokusů o chování a doplnění cloudových služeb, které s ohledem na velký počet zapojených uživatelů dokážou během několika hodin odhalit některé nové zranitelnosti.

Antivirová společnost Kaspersky definuje zero-day jako široký pojem, který označuje nedávno objevené bezpečnostní chyby, které mohou hackeři využít k útoku na systémy. Termín "zero-day" odkazuje na skutečnost, že se dodavatel nebo vývojář o chybě teprve dozvěděl - což znamená, že má "nula dní" na její opravu. K útoku nultého dne dochází, když hackeři využijí chybu dříve, než ji vývojáři stihnou odstranit (Kaspersky, 2022, přeloženo autorem).

- Zranitelnost nultého dne je neznámá bezpečnostní zranitelnost nebo chyba softwaru, na kterou může útočník zacílit škodlivý kód.
- Zneužití Zero-Day Exploit je technika nebo taktika, kterou záškodník použije k využití zranitelnosti k útoku na systém.
- K útoku Zero-Day dochází, když hacker vydá škodlivý software, který zneužívá zranitelnost softwaru dříve, než vývojář softwaru chybu opraví.

(Crowdstrike, 2022, přeloženo autorem)

Nedostatek školení

Každý rok utrpí mnoho organizací porušení nebo ztrátu dat, což má za následek odhalení velkého množství soukromých údajů. Různé statistiky a studie ukázaly, že nedostatečné povědomí o bezpečnosti (a také nedostatek kvalifikovaných zaměstnanců) hraje klíčovou roli ve vystavování organizací různým kybernetickým hrozbám, zejména ransomware.

Povědomí zaměstnanců o bezpečnosti IT je považováno za první linii obrany při ochraně informačních systémů. Školení a povědomí o zabezpečení zajišťují, že zaměstnanci rozumí různým technikám útoků, které mohou kyberzločinci použít k infiltraci do systémů organizace, a vědí, jak zmírnit a hlásit incidenty příslušným lidem. Například bez ohledu na typ a počet bezpečnostních řešení (jako jsou firewally a IDS) implementovaných k ochraně sítě organizace, pokud nekvalifikovaný zaměstnanec klikne na škodlivý odkaz v phishingovém e-mailu, může být ohrožena celá síť, takže zabezpečení jakékoli organizace Ochranná opatření přijatá týmem jsou k ničemu! Kromě toho v této analýze se podrobně proberou různé perspektivy školení v oblasti kybernetické bezpečnosti, které musí znát každý uživatel počítače, aby se mohl bránit kybernetickým útokům.

Ransomware se může šířit různými metodami, zejména prostřednictvím e-mailových systémů nebo infikovaných webových stránek, které využívají nástroje. V této části se popisují tyto metody a uvádí se příklady každé z nich. Je potřeba mít na paměti, že mnoho variant ransomware a dalších typů malware se může šířit samo. Mohou tak identifikovat a infikovat všechny počítače připojené k síti oběti.

3.3 Monitoring počítačových sítí

Pojem monitoring počítačových sítí je v dnešním světe rozšířen v celém IT odvětví. V informačních technologiích je monitoring sítě kritický proces, při kterém jsou všechny síťové komponenty jako jsou routery, switche, počítače nebo servery monitorovány z hlediska poruch a výkonu. Cíle monitoringu je udržet a optimalizovat dostupnost těchto komponent. Jeden z hlavních aspektů monitoringu počítačové sítě je proaktivní sledování sítě. Proaktivní analýza problémů s výkonem sítě a slabých míst pomáhá objevit problémy v prvotních fázích. Díky proaktivnímu monitoringu můžeme předejít poruchám nebo výpadkům sítě.

Pomocí systémů monitorování sítě, ať už to jsou nástroje hardwarové či softwarové, můžeme sledovat různé aspekty sítě a jejího chodu. Sledují se aspekty jako je využití šířky pásma nebo doba provozu sítě.

Mezi hlavní výhody monitoringu sítě patří jasný přehled o síti, rostoucí složitost, lepší využití IT zdrojů, včasný náhled na budoucí potřeby infrastruktury a schopnost identifikovat bezpečnostní hrozby. Prostřednictvím monitorování sítě mohou správci získat jasný přehled o všech připojených zařízeních v síti. Zjistit, jak se mezi nimi pohybují data, a rychle identifikovat a odstranit problémy, které mohou ohrozit výkon a vést k výpadkům. Moderní podniky se spoléhají na řadu služeb závislých na internetu, které jsou pro ně kritické. Patří sem poskytovatelé cloudových služeb, ISP, CDN, ale i poskytovatelé SaaS, UCaaS. Každá služba funguje přes internet, takže je náchylná k výkyvům výkonu způsobeným výpadky internetu nebo problémy se směrováním. Viditelnost síťových komponent mimo vaši kontrolu vám umožní sledovat problémy, které by mohly mít dopad na zaměstnance nebo zákazníky. Hardwarové a softwarové nástroje v systémech monitorování sítě snižují množství manuální práce týmů IT. To znamená, že pracovníci IT mají více času věnovat se důležitým projektům organizace. Systémy pro monitorování sítě mohou poskytovat zprávy o tom, jak síťové komponenty fungovaly za definované období. Analýzou těchto zpráv mohou správci sítě předvídat, kdy bude organizace potřebovat zvážit modernizaci nebo implementaci nové IT infrastruktury. Monitorování sítě pomáhá organizacím pochopit, jak vypadá "normální" výkon jejich sítí. Když se tedy objeví neobvyklá aktivita, například nevysvětlitelný nárůst síťového provozu, je pro správce snazší problém rychle identifikovat a určit, zda může představovat bezpečnostní hrozbu (CISCO, 2021, přeloženo autorem).

Monitoring sítě není jen účinným nástrojem pro identifikaci technických problémů a bezpečnostních rizik, ale také může pomoci organizacím splnit požadavky na ochranu osobních údajů stanovené v GDPR. Provozování monitoringu sítě může být náročné v závislosti na velikosti a složitosti sítě a může vyžadovat speciální nástroje a technologie. Nicméně existuje řada nástrojů, které jsou k dispozici zdarma nebo za přijatelnou cenu a mohou poskytnout užitečné informace o stavu sítě. V případě porušení osobních údajů může monitoring sítě pomoci organizacím včas identifikovat takové incidenty a informovat dotčené osoby, jak je požadováno GDPR.

Při implementaci monitoringu sítě je kritické zajistit jeho správnou konfiguraci, aby nedocházelo k falešným poplachům, které by mohly být zavádějící a zbytečně zatěžovat tým IT. Kromě toho je nutné chránit data shromažďovaná během monitoringu sítě, aby nebyla zneužita. V dnešní době, kdy mnoho organizací spoléhá na své počítačové sítě, je monitoring sítě nezbytnou součástí úspěšného IT řízení a zajištění bezpečnosti sítě.

3.4 Open Source nástroje

Software s otevřeným zdrojovým kódem anglicky Open Source Software (dále jen „OSS“) je software, který je šířen se svým zdrojovým kódem, takže je k dispozici pro použití, úpravy a šíření s původními právy. Zdrojový kód je část softwaru, kterou většina uživatelů nevidí. Je to kód, se kterým počítačoví programátoři manipulují, aby mohli řídit chování programu nebo aplikace. Ti, kteří mají přístup ke zdrojovému kód, mohou program měnit tak, že do něj přidají nové části, mění ho nebo opravují části, které nefungují správně. Součástí OSS je obvykle licence, která programátorům umožňuje upravovat software tak, aby co nejlépe vyhovoval jejich potřebám.

Způsob open source je forma myšlení a spolupráce v rámci komunity open source. Tato filozofie je založena na intelektuální svobodě a základních principech: transparentnosti, spolupráci, poskytování, začlenění a komunitě. Výměna myšlenek a softwaru vyvíjeného komunitami je hnací silou tvůrčího, vědeckého a technologického pokroku v takových odvětvích, jako jsou: vzdělávání, státní správa, právo, zdravotnictví a výroba. Toto hnutí vytvořilo způsob, jak může globální komunita spolupracovat, sdílet a napomáhat individuálním i skupinovým cílům prostřednictvím zdrojového kódu (IBM, 2021, přeloženo autorem).

Software s otevřeným zdrojovým kódem je založen na spolupráci, spoléhá se na komunitní produkci a vzájemném hodnocení při používání, změnách a vzájemném sdílení zdrojového kódu. Vývojáři sdílejí poznatky, nápady a kódy, aby společně i jednotlivě vytvářeli inovativnější softwarová řešení. Tento škálovatelný a flexibilní software zajišťuje, že každý, kdo má k dispozici zdrojový kód, jej může upravovat, vylepšovat a dále šířit pro lepší opakované použití a dostupnost. Software s otevřeným zdrojovým kódem funguje na základních principech vzájemné tvorby a masové spolupráce, což vytváří udržitelnější vývoj softwaru pro koncové uživatele (IBM, 2021, přeloženo autorem).

Definici OSS podle Štědroňě *„Za open source software se pokládají takové aplikace, které jsou šířeny se zachováním určitých práv a svobod pro jejich koncového uživatele. Jde o práva spouštět program za jakýmkoliv účelem, studovat, jak program pracuje a přizpůsobit ho svým potřebám, redistribuovat kopie dle svobodné vůle, vylepšovat program a zveřejňovat tato zlepšení“* (Štedroň, 2009, s.17).

3.4.1 Zabbix

Zabbix je nástroj pro monitorování výkonu a dostupnosti zařízení, jako jsou CPU, paměť, diskové zdroje, teplota a další hardwarové parametry. Kromě toho sleduje dostupnost, odezvu a provoz na síťových zařízeních, jako jsou switche, routery a firewally. Tento nástroj také monitoruje výkon a dostupnost webových serverů, databázových serverů, e-mailových serverů a dalších aplikací a služeb. Je navržen pro sledování virtuálních strojů a prostředků v cloudových prostředích, jako jsou Amazon Web Services (AWS), Microsoft Azure a Google Cloud Platform. Tento nástroj shromažďuje a analyzuje systémové aplikace logy pro identifikaci problémů a varování. Navíc, Zabbix monitoruje vyvážení zátěže mezi servery a infrastruktury, zabezpečení a detekuje podezřelé aktivity, jako jsou pokusy o neoprávněný přístup nebo útoky.

Zabbix je vysoce integrované řešení pro monitorování sítě, které nabízí řadu funkcí v jediném balíčku. Balíček obsahuje shromažďování dat, který podporuje SNMP, IPMI, JMX a také VMware monitoring. Flexibilní definice prahů. Lze definovat velmi flexibilní prahové hodnoty problémů, tzv. triggery, odkazující na hodnoty z backendové databáze. Vysoce konfigurovatelné upozorňování, kde zasílání oznámení lze přizpůsobit pro plán eskalace, příjemce a typu média. Grafické zpracování v reálném čase, kde grafy ukazují sledované položky pomocí vestavěné funkce pro tvorbu grafů. (ZABBIX, 2021, přeloženo autorem).

Díky své flexibilitě a rozšiřitelnosti může být nástroj pro monitorování velkých a složitých IT prostředí s tisíci zařízeními přizpůsoben potřebám organizací různých velikostí. Jeho široká funkcionalita pro sledování a správu infrastruktury umožňuje snadnou integraci do firemního prostředí. Kromě toho lze s nástrojem pro monitorování propojit různé aplikace a služby třetích stran, například systémy pro řízení incidentů, notifikační platformy, automatizační nástroje a další. Tento přístup umožňuje rozšířit monitorovací schopnosti a zabezpečit, aby byli správci IT systémů včas upozorněni na případné problémy. Existuje podpora šablon, které zjednodušují a urychlují nastavení monitorování pro obvyklé typy zařízení, aplikací a služeb. Tyto šablony umožňují uživatelům vytvořit konfigurace, které lze snadno aplikovat na různá zařízení a prostředí, čímž se zvyšuje efektivita a snižují nároky na správu.

Zabbix nabízí mnoho způsobů monitorování různých aspektů IT infrastruktury a vlastně téměř všeho, co k ní je možno připojit. Lze jej charakterizovat jako částečně distribuovaný monitorovací systém s centralizovanou správou. Ačkoli mnoho instalací má jeden centrální systém, je možné použít distribuované monitorování pomocí proxy serverů (Olups, 2017, přeloženo autorem).

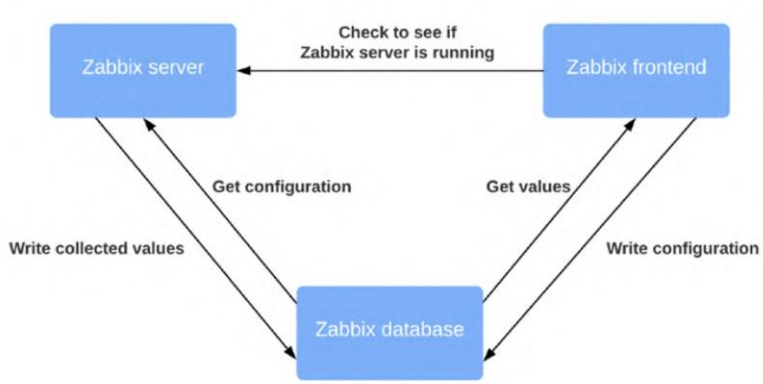
Zabbix server je centrální komponenta celého Zabbix monitorovacího systému. Jedná se o software, který zpracovává data z různých zdrojů, vyhodnocuje je a generuje upozornění a zprávy na základě nastavených pravidel a triggerů. Zabbix server komunikuje se Zabbix agenty, které jsou nainstalovány na monitorovaných zařízeních, a shromažďuje od nich různé statistiky a informace. Liefting popisuje Zabbix server jako hlavní proces nastavení Zabbix, který je zodpovědný za monitorování, upozorňování na problémy a mnoho dalších úloh. Kompletní Zabbix „stack“ se skládá minimálně z následujících částí:

- databáze (MySQL, PostgreSQL nebo Oracle).
- Server Zabbix
- Apache nebo NGINX, na kterém běží frontend Zabbix s PHP 7.2+, ale PHP 8 není v současné době podporováno.

(Liefting, 2022, přeloženo a upraveno autorem)

Obrázek 1 popisuje komunikační diagram mezi jednotlivými prvky Zabbix server, Zabbix database a Zabbix frontend.

Obrázek 1 - Diagram komunikace jednotlivých prvků



Zdroj: Liefting, s.6, Zabbix 6 IT Infrastructure Monitoring Cookbook

Mobilní aplikace pro operační systémy Android a iOS jsou nedílnou součástí Zabbixu, což umožňuje uživatelům sledovat stav monitorovaných prvků a přijímat upozornění na svých mobilních zařízeních. Uživatelé mohou jednoduše přistupovat k důležitým informacím o síťových zařízeních, jako jsou informace o využití šířky pásma, dostupnosti serverů a dalších prvcích, a zobrazit přehlednou statistiku o provozu sítě. Díky mobilnímu přístupu k monitorovaným datům mohou správci sítě reagovat na problémy v reálném čase a přijmout potřebná opatření. Provozování Zabbixu na mobilních zařízeních je snadné a intuitivní. Uživatelé si pouze stáhnou aplikaci pro svůj operační systém, přihlásí se k účtu Zabbix a mohou monitorovat svou síť kdykoli a kdekoli. Zabbix tak nabízí spolehlivé řešení pro monitorování sítě a umožňuje správcům sítě reagovat na problémy v reálném čase, aby zajistili neustálou dostupnost sítě.

3.4.2 Wazuh

Wazuh je bezplatná bezpečnostní platforma s otevřeným zdrojovým kódem, která sjednocuje funkce XDR a SIEM. Chrání pracovní zátěže v lokálních, virtualizovaných, kontejnerových a cloudových prostředích. Pomáhá organizacím i jednotlivcům chránit jejich datová aktiva před bezpečnostními hrozbami. Široce ji využívají tisíce organizací po celém světě, od malých firem až po velké podniky (Wazuh, 2023, přeloženo autorem).

Wazuh poskytuje řadu funkcí pro ochranu proti hrozbám, jako je například detekce a analýza síťového provozu, monitorování systémových a aplikačních logů, detekce zranitelností a hledání škodlivého kódu. Tyto funkce umožňují rychlé zjištění a odpověď na hrozby a zabezpečení systémů proti útokům.

Wazuh poskytuje také nástroje pro správu bezpečnosti, jako je například sledování souladu s bezpečnostními předpisy, správa incidentů a správa bezpečnostních politik. Tyto nástroje pomáhají organizacím zabezpečit své systémy v souladu s předpisy a standardy. Wazuh může být nasazen jako samostatný nástroj nebo může být integrován s dalšími bezpečnostními nástroji a technologiemi, jako jsou například firewall, antiviry nebo IPS. Wazuh je k dispozici jako open source projekt a lze ho používat zdarma.

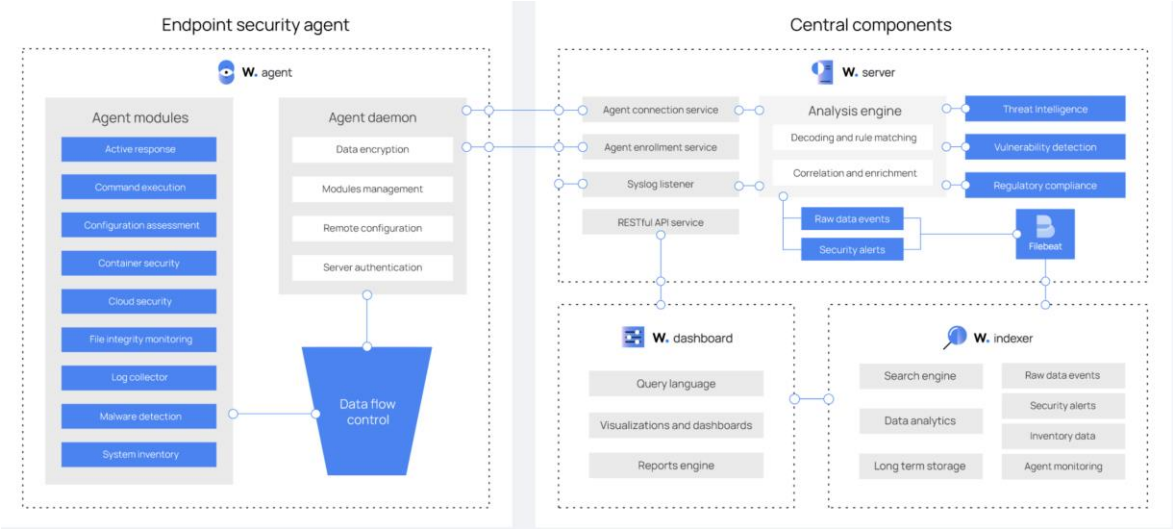
Systém Wazuh je závislý na použití speciálního agenta, který je nainstalován na sledovaných koncových zařízeních. Dále se skládá ze tří centrálních komponent: Wazuh serveru, Wazuh indexeru a Wazuh ovládacího panelu.

- Indexer Wazuh je vysoce škálovatelný fulltextový vyhledávač a analytický stroj. Tato centrální komponenta indexuje a ukládá výstrahy generované serverem Wazuh.
- Server Wazuh analyzuje data přijatá od agentů. Zpracovává je prostřednictvím dekodérů a pravidel a pomocí informací o hrozbách vyhledává známé indikátory kompromitace (IOC). Jeden server může analyzovat data od stovek nebo tisíců agentů a při nastavení jako cluster se může horizontálně škálovat. Tato centrální komponenta slouží také ke správě agentů a v případě potřeby je vzdáleně konfiguruje a aktualizuje.
- Přístrojový panel Wazuh je webové uživatelské rozhraní pro vizualizaci a analýzu dat. Obsahuje hotové ovládací panely pro události zabezpečení, dodržování předpisů, zjištěné zranitelné aplikace, údaje o monitorování integrity souborů, výsledky hodnocení konfigurace, události monitorování cloudové infrastruktury a další. Slouží také ke správě konfigurace systému Wazuh a ke sledování jeho stavu.

(Wazuh, 2023, přeloženo autorem)

Kromě monitorování na bázi agentů je platforma Wazuh schopná monitorovat i zařízení bez použití agentů, jako jsou například firewally, přepínače, směrovače nebo síťové IDS. Pro shromažďování log dat z takovýchto zařízení se může využít protokol Syslog, přičemž jejich konfigurace může být monitorována pomocí pravidelného sondování dat prostřednictvím SSH nebo rozhraní API (Wazuh, 2023, přeloženo autorem). Obrázek 2 znázorňuje, jak mezi sebou komunikují agenti a centrální komponenty.

Obrázek 2 - Komunikace agentů a centrálních komponent



Zdroj: Wazuh, 2023

3.4.3 SecurityOnion

Security Onion je bezplatná a otevřená platforma pro vyhledávání hrozeb, monitorování podnikového zabezpečení a správu protokolů. Zahrnuje vlastní nástroje pro výstrahy, ovládací panely ve webovém rozhraní a další. Security Onion vznikl v roce 2008 a původně byl založen na linuxové distribuci Ubuntu. V průběhu let verze Security Onion sledovala verzi Ubuntu, na které byla založena. Security Onion je nyní založen na kontejnerech, a proto již není omezen pouze na Ubuntu. Na znamení této změny má nyní Security Onion své vlastní schéma verzování a tato nová platforma se jmenuje Security Onion 2 (SecurityOnionSolutions, 2023, přeloženo autorem).

Umožňuje zachytávat síťový provoz a tím detekovat a monitorovat síťové útoky. Kromě toho obsahuje řadu nástrojů pro detekci neoprávněných přístupů a síťových útoků, včetně snifferu a IDS/IPS technologií, jako jsou Suricata a Snort. Dále je Security Onion propojen s řadou open source bezpečnostních informačních zdrojů pro rychlejší detekci a odstranění hrozeb. Security Onion umožňuje shromažďovat a spravovat logovací záznamy z různých zařízení a aplikací v síti, poskytuje nástroje pro analýzu malware a skenování sítě a detekci zranitelností. Security Onion také poskytuje nástroje pro rychlou reakci na bezpečnostní incidenty a možnosti pro automatizaci a usnadnění této činnosti.

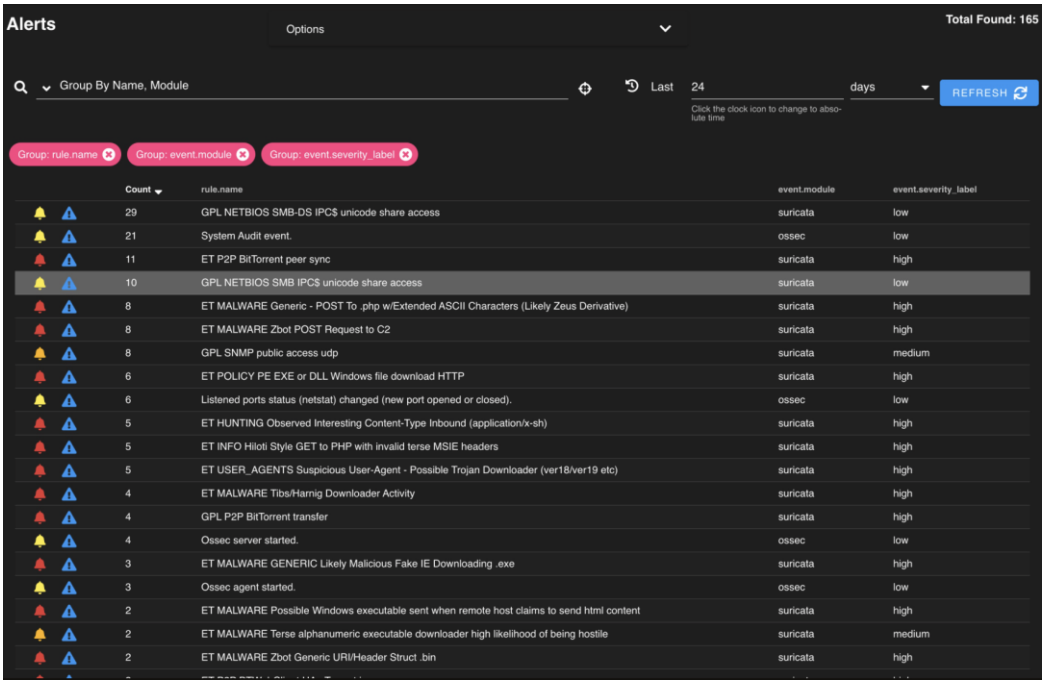
Mezi další funkce, které SecurityOnion umí ovládat jsou:

- Správa majetku - Security Onion umožňuje správu a sledování zařízení v síti, včetně softwarových a hardwarových konfigurací, aby bylo možné lépe chránit a spravovat tyto prvky.
- Monitoring síťového provozu- Security Onion poskytuje škálovatelnou a přizpůsobitelnou platformu pro monitorování síťového provozu, což umožňuje snadnější detekci a reakci na útoky.
- Threat Hunting - Security Onion umožňuje manuální vyhledávání a analýzu údajů o síťovém provozu a logování, aby bylo možné identifikovat skryté hrozby nebo nestandardní chování.

(SecurityOnionSolutions, 2023, přeloženo autorem)

Obrázek 3 ukazuje jeden z možných přehledů SecurityOnion, a to konkrétně rozhraní výsrah pro kontrolu a správu výstrah.

Obrázek 3 - Rozhraní výstrah pro kontrolu a správu výstrah



Zdroj:Wazuh, software, 2023

3.4.4 Greenbone OpenVAS

Greenbone OpenVAS je plnohodnotný skener zranitelností. Jeho možnosti zahrnují neautentizované a autentizované testování, různé vysokoúrovňové a nízkoúrovňové

internetové a průmyslové protokoly, ladění výkonu pro rozsáhlé skenování a výkonný interní programovací jazyk pro implementaci jakéhokoli typu testu zranitelnosti. Testy pro odhalování zranitelností skener získává z kanálu, který má dlouhou historii a denně se aktualizuje. OpenVAS vyvíjí a posouvá vpřed společnost Greenbone od roku 2006. Jako součást komerční rodiny produktů pro správu zranitelností Greenbone Enterprise Appliance tvoří skener spolu s dalšími moduly s otevřeným zdrojovým kódem Greenbone Community Edition (Greenbone OpenVAS, 2023, přeloženo autorem, přeloženo autorem).

Automatické skenování sítě a detekce potenciálních bezpečnostních slabostí je jednou z funkcí Greenbone OpenVAS. Jeho databáze zranitelností umožňuje identifikaci bezpečnostních nedostatků v různých aplikacích, službách a systémech. Greenbone OpenVAS dodržuje mnoho standardů, včetně CVE, CPE a CVSS. Výsledky skenování jsou zpracovány do podrobných zpráv, které poskytují přehled o identifikovaných zranitelnostech a nabízejí doporučení pro jejich opravu. Umožňuje integraci s dalšími bezpečnostními nástroji, jako jsou SIEM systémy a IDS/IPS systémy. Greenbone OpenVAS je navržen tak, aby umožňoval snadnou rozšiřitelnost a konfigurovatelnost dle potřeb uživatele.

Uživatelům Greenbone OpenVAS jsou k dispozici detailní a srozumitelné zprávy o identifikovaných zranitelnostech, které obsahují informace o závažnosti, dopadu na systém a možných důsledcích. Tyto zprávy jsou prezentovány v přehledné a srozumitelné formě, aby uživatelé mohli rychle rozpoznat nejvážnější zranitelnosti a začít je řešit. V rámci zpráv jsou také poskytována doporučení pro opravu zranitelností, aby uživatelé mohli účinněji řešit bezpečnostní problémy a minimalizovat riziko útoků. Celkově lze říci, že reportování v Greenbone OpenVAS je klíčovou funkcí, která pomáhá uživatelům identifikovat a řešit zranitelnosti v jejich systémech a sítích.

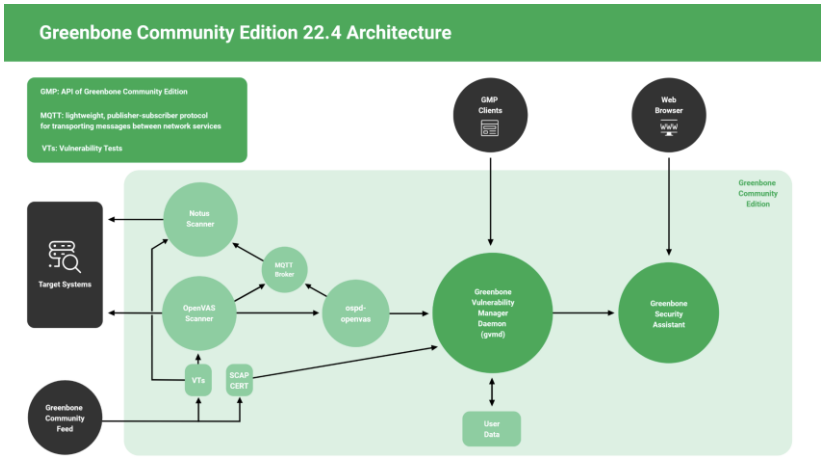
Architektura Greenbone Community Edition je rozdělena do tří hlavních částí:

- Spustitelné aplikace skeneru, které spouštějí testy zranitelností (VT) proti cílovým systémům.
- Greenbone Vulnerability Manager Daemon (gvmd).
- Greenbone Security Assistant (GSA) s démonem Greenbone Security Assistant (gsad).

(Greenbone OpenVAS, 2023, přeloženo autorem)

Obrázek 4 popisuje jakou architekturu používá Greenbone OpenVAS.

Obrázek 4 - Architektura Greenbone OpenVAS komunitní verze 22.4



Zdroj: OpenVAS github, architektura, 2023

3.4.5 Nmap

Nmap (Network Mapper) je bezplatný nástroj s otevřeným zdrojovým kódem pro zajišťování chodu sítě a bezpečnostní audit. Mnoho správců systémů a sítí jej také považuje za užitečný pro úlohy, jako je inventarizace sítě, správa plánů aktualizace služeb a sledování provozuschopnosti hostitelů nebo služeb. Nmap využívá surové pakety IP ke zjištění, jací hostitelé jsou v síti k dispozici, jaké služby tito hostitelé nabízejí, jaké operační systémy na nich běží, jaký typ paketových filtrů/firewallů je používán a desítky dalších charakteristik. Byl navržen pro rychlé skenování velkých sítí, ale funguje dobře i proti jednotlivým hostitelům. Nmap běží na všech hlavních počítačových operačních systémech a oficiální binární balíčky jsou k dispozici pro Linux, Windows a Mac OS X. Kromě klasického spustitelného programu Nmap pro příkazový řádek obsahuje sada Nmap pokročilé grafické rozhraní a prohlížeč výsledků (Zenmap), flexibilní nástroj pro přenos dat, přesměrování a ladění (Ncat), nástroj pro porovnávání výsledků skenování (Ndiff) a nástroj pro generování paketů a analýzu odezvy (Nping) (NMAP, 2021, přeloženo autorem)

Ačkoli skenování portů samo o sobě není nelegální, funkce Nmapu jsou užitečné pro záškodníky, kteří hledají zranitelnosti, které by mohli zneužít. Některá použití softwaru, zejména bez povolení, vás mohou stát pracovní místo nebo váš mohou dostat do právních problémů, i když skenujete zranitelnosti pro neškodné účely. I když jsou některá skenování Nmap poměrně nenáročná a nemusí vyvolat výstrahy, je vždy lepší nechat si skenování schválit příslušnými osobami v organizaci. Skenování portu je však užitečné zejména pro

správce sítě, kteří řeší nějaký problém v síti nebo etické hackery, kteří řeší zabezpečení sítě před opravdovým útočníkem.

Teoretická část diplomové práce se zaměřila na problematiku kybernetická bezpečnosti a open source nástroje v oblasti zabezpečení informačních technologií. Je potřeba mít na paměti, jak velký význam kybernetická bezpečnost má, jelikož digitální technologie pronikají do všech sfér našeho života a zároveň jsou stále více vystaveny kybernetickým hrozbám, jak v osobním životě tak i v profesionálním.

V průběhu teoretické části bylo uvedeno několik klíčových nástrojů open source: Zabbix, Wazuh, PfSense, OpenVAS a SecurityOnion. Každý z těchto nástrojů má své unikátní funkce a přednosti. Zabbix je vysoce konfigurovatelný monitorovací systém, který umožňuje široké škály zařízení a služeb. Wazuh se zaměřuje na sledování zabezpečení, řízení hrozeb a správu incidentů. PfSense je robustní firewall a router, který poskytuje komplexní síťovou ochranu. OpenVAS je nástroj pro skenování zranitelností, který pomáhá identifikovat a řešit potenciální slabiny v síti a aplikacích. SecurityOnion je komplexní platforma pro detekci a prevenci průniků, analýzu síťového provozu a správu incidentů.

Přestože se teoretická část zabývá zmíněnými nástroji, praktické část se bude týkat především Zabbixu. Praktická část bude obsahovat konkrétní implementace Zabbix a využití v reálném prostředí, aby bylo možné prozkoumat, jak tento nástroj přispívá k posílení kybernetická bezpečnosti a jak může být efektivně využit ve prospěch organizací. Na základě praktických zkušeností bude možné zhodnotit, jak je Zabbix účinný ve srovnání nebo za využití kombinace ostatních open source nástrojů, které se diskutovali v teoretické části. Takto získané poznatky mohou posloužit jako základ pro další výzkum a inovace v oblasti kybernetická bezpečnosti a open source technologií.

V průběhu teoretické části byl také zdůrazněn význam integrace a spolupráce mezi různými open source nástroji pro zajištění efektivní a komplexní ochrany kybernetického prostoru. Spolupráce mezi těmito nástroji a jejich správná konfigurace mohou vytvořit silný a komplexní systém pro monitorování a správu bezpečnosti. To nám umožní získat širší a hlubší přehled o hrozbách a rizicích, kterým jsou naše sítě a infrastruktury vystaveny, a zároveň nám poskytne nástroje pro rychlou a účinnou reakci na bezpečnostní incidenty.

V další část diplomové práce se zaměří na zkoumání, jak mohou být tyto open source nástroje integrovány a navzájem propojeny, aby bylo dosaženo maximální účinnosti a zajištění komplexního přístupu k zabezpečení. Toto úsilí nám umožní identifikovat možnosti

pro zlepšení stávajících nástrojů a procesů, a zároveň nám poskytne podklady pro navrhování nových řešení a inovací v oblasti kybernetická bezpečnosti.

V konečném důsledku tato práce přispěje k lepšímu pochopení potenciálu open source nástrojů v kybernetická bezpečnosti a k rozšíření znalostí o jejich uplatnění v praxi. To může vést k posílení kybernetická bezpečnosti organizací, zvýšení povědomí o důležitosti ochrany digitálních prostředků a podpoření dalšího výzkumu a inovací v oblasti kybernetická bezpečnosti

4 Vlastní práce

4.1 Dotazníkový průzkum

Průzkum dotazníkovým šetřením byl vybrán z toho důvodu, aby praktická část efektivněji zohledňovala potřeby adresátů, měla vypovídající charakter a byla podložena reálnými poznatky. Část respondentů byla vybrána na základě pracovních i osobních kontaktů a druhá část byla vybrána náhodně hledáním na internetu. Respondenti z důvodu citlivosti sbíraných informací nesouhlasili s uvedením jejich identity, proto byla jejich identita anonymizována. Průzkum byl omezen na 12 respondentů. Dotazníkový průzkum byl vytvořen za pomoci online nástroje Google forms.

4.1.1 Cíl průzkumu

Cílem průzkumu je objasnit, jak velké úsilí jednotlivé dotazované subjekty vynakládají do bezpečnosti a monitoringu počítačové sítě, kolik finančních prostředku investují do IT infrastruktury a zda jsou implementovány bezpečnostní politiky v síti a mezi zaměstnanci. Průzkum vychází z předpokladu, že převážná většina dotazovaných subjektů věnuje této problematice pozornost a jejich počítačový síť je dobře zabezpečena.

Průzkum, který je zaměřen na bezpečnost a monitoring počítačových sítí, je velmi důležitý, protože každý subjekt, který používá počítačovou síť, by měl být obeznámen s riziky, která s jejím provozem souvisejí. Zabezpečení počítačových sítí by mělo být prioritou pro každou firmu, organizaci či jednotlivce, kteří používají internetové připojení. Průzkum může ukázat, jak často jsou IT systémy aktualizovány, jak jsou chráněny a zda jsou implementovány bezpečnostní politiky pro zaměstnance.

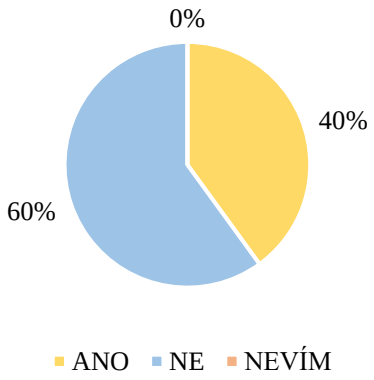
Je důležité zdůraznit, že každá firma by měla investovat do zabezpečení své IT infrastruktury a bezpečnostní politiky pro své zaměstnance. Tento investiční náklad může být na první pohled vysoký, ale je to nízká cena za ochranu důležitých informací, které by mohly být napadeny a ukradeny. Kromě toho, investice do bezpečnosti může být úspěšným krokem, který vyvolá vyšší důvěru u zákazníků a ostatních osob.

Po vyhodnocení výsledků průzkumu je nutné navrhnout konkrétní řešení a doporučení, která povedou ke zlepšení bezpečnosti počítačové sítě. Tyto návrhy by měly být srozumitelné a názorné, aby je bylo snadné implementovat. Doporučení by měla být zaměřena na nejvíce rizikové oblasti, které byly identifikovány v průzkumu.

4.1.2 Shrnutí průzkumu

Graf 1 ukazuje, že významná část respondentů odpověděla na otázku o implementaci kybernetické bezpečnosti záporně. Celkem 60 % respondentů odpovědělo "ne" a pouze 40 % odpovědělo "ano".

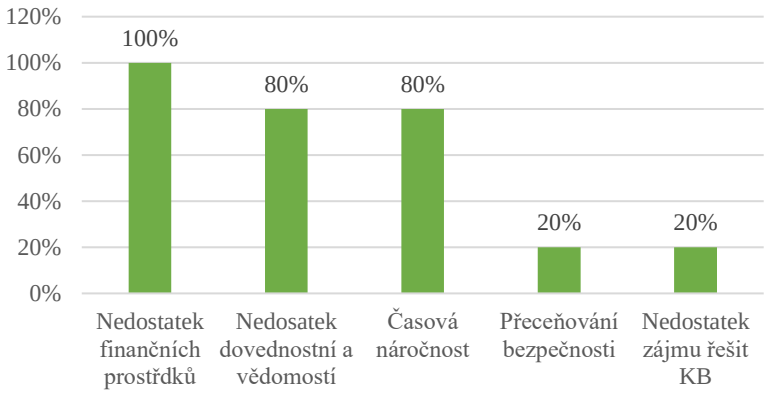
Graf 1 - Má vaše firma implementovanou politiku kybernetické bezpečnosti?



Zdroj: Vlastní zpracování

Výsledky získané z otázky na grafu číslo 2 ukazují, že všichni z respondentů (100 %) odpověděli, že nemají finanční prostředky na řešení kybernetická bezpečnosti. Dále, 80 % respondentů uvádí nedostatek znalostí o kybernetická bezpečnosti a stejný podíl respondentů (80 %) se kvůli časovým omezením nevěnuje kybernetická bezpečnosti s dostatečnou pozorností. Zároveň 20 % respondentů přeceňuje zavedení bezpečnostních prvků a dalších 20 % nemá zájem řešit kybernetická bezpečnost.

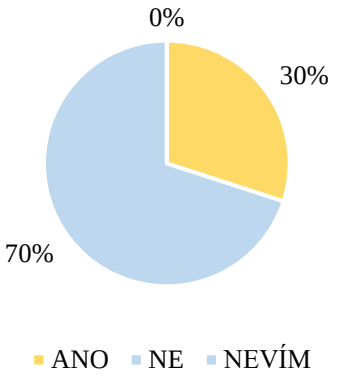
Graf 2 – Proč firmy kybernetická bezpečnost neřeší?



Zdroj: Vlastní zpracování

Graf 3 ukazuje, že většina respondentů (70 %) odpověděla záporně na otázku, zda provádějí pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti. Pouze 30 % respondentů odpovědělo kladně na tuto otázku.

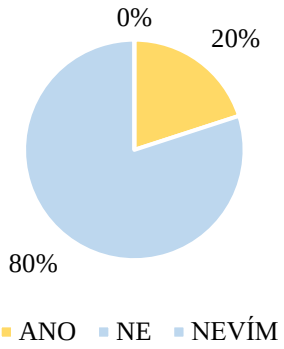
Graf 3 - Provádíte pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti?



Zdroj: Vlastní zpracování

Podle grafu číslo 4 většina respondentů (80 %) odpověděla záporně na otázku, zda mají zavedený incident response plán pro řešení bezpečnostních incidentů. Naopak pouze 20 % respondentů odpovědělo kladně na tuto otázku.

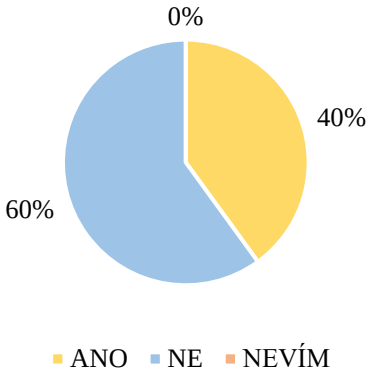
Graf 4 - Máte zavedený incident response plán pro řešení bezpečnostních incidentů?



Zdroj: Vlastní zpracování

Graf 5 ukazuje, že většina respondentů (60 %) odpověděla záporně na otázku, zda existuje u nich pravidelný audit bezpečnostních opatření a postupů. Pouze 40 % respondentů odpovědělo kladně na tuto otázku.

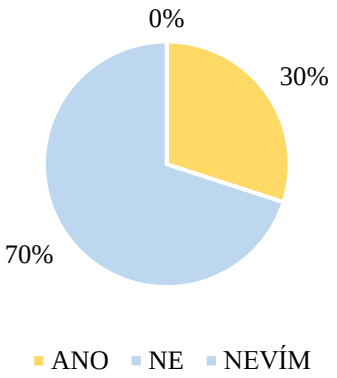
Graf 5 - Existuje u vás pravidelný audit bezpečnostních opatření a postupů?



Zdroj: Vlastní zpracování

Většina respondentů (70 %) podle grafu číslo 6 odpověděla záporně na otázku, zda používají pokročilé systémy detekce hrozeb a průniků do sítě. Naopak pouze 30 % respondentů odpovědělo kladně na tuto otázku.

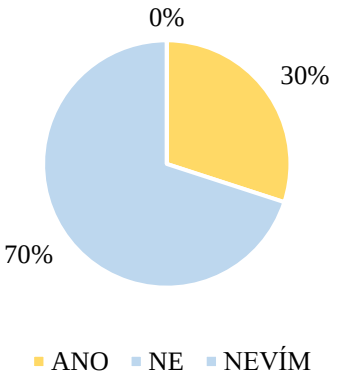
Graf 6 - Používáte pokročilé systémy detekce hrozeb a průniků do sítě?



Zdroj: Vlastní zpracování

Graf 7 ukazuje, že většina respondentů (70 %) odpověděla záporně na otázku, zda mají vnitřní nebo externí tým pro řešení kybernetických bezpečnostních hrozeb. Pouze 30 % respondentů odpovědělo kladně na tuto otázku.

Graf 7 – Máte vnitřní nebo externí tým pro řešení kybernetických bezpečnostních hrozeb?



Zdroj: Vlastní zpracování

Během průzkumu bylo získáno mnoho zajímavých poznatků a informací. Bylo zjištěno, že téměř všechny oslovené subjekty pravidelně zálohují svá důležitá data a systémy a udržují svá zařízení a systémy záplatované a aktualizované. Byly také zjištěny horší výsledky, neboť více než polovina respondentů nemá implementovanou politiku kybernetické bezpečnosti. Zaměstnanci nepodstupují školení o kybernetická bezpečnosti, zaměstnavatel neinformuje zaměstnance o aktuálních hrozbách a útocích, nevykonávají se testování zranitelností IT infrastruktury nebo nemají systém pro sledování a omezení nežádoucího síťového provozu. Z odpovědí získaných v průběhu dotazníkového průzkumu lze vyvodit, že 30 % respondentů věnuje kybernetická bezpečnosti značnou pozornost, 30 %

respondentů se této problematice okrajově věnuje a 40 % respondentů téměř nevěnuje kybernetická bezpečnosti a monitoringu žádnou nebo jen zanedbatelnou pozornost.

Výsledky průzkumu ukazují, že i když si mnoho organizací a firem uvědomuje význam kybernetická bezpečnosti a provádí některé preventivní kroky, jako jsou zálohování a aktualizace, stále existuje značné množství nedostatků v oblasti bezpečnosti. Některé organizace se dokonce ani nezabývají implementací politiky kybernetické bezpečnosti, což může být velkým rizikem.

Je také alarmující, že většina organizací nedostatečně informuje své zaměstnance o aktuálních hrozbách a útocích a nezabezpečuje své sítě proti nežádoucímu síťovému provozu. Tyto nedostatky mohou způsobit značné škody, jako například únik citlivých dat nebo přerušení provozu sítě.

V průzkumu se také ukázalo, že přibližně třetina respondentů věnuje kybernetická bezpečnosti značnou pozornost, což je velmi pozitivní signál. Další třetina respondentů již kybernetická bezpečností okrajově zainteresována, zatímco zbytek respondentů nevěnuje kybernetická bezpečnosti a monitoringu téměř žádnou nebo zanedbatelnou pozornost. Tato situace vyžaduje okamžitou pozornost a zlepšení v oblasti kybernetická bezpečnosti, aby organizace mohly efektivně chránit své sítě a data proti kybernetickým hrozbám.

4.2 Implementace open source nástrojů

Bezpečnost informačních systémů a správa IT infrastruktury jsou klíčovými faktory pro úspěch jakékoli organizace. V praktická část práce se bude soustředit na implementaci, instalaci a konfiguraci komplexního řešení pro monitorování a zabezpečení, které budou využívat open source nástroje k přehlednému zobrazování dat z různých zdrojů.

Pro integraci a zobrazování dat bude využíván především Zabbix. Univerzální open source nástroj pro monitorování IT infrastruktury, který poskytuje sledování různých aspektů systému, jako jsou výkon, dostupnost a bezpečnost. K posílení bezpečnosti se do Zabbixu integrují další open source nástroje, a to konkrétně Wazuh, OpenVAS a Security Onion.

Cíle této praktické části diplomové práce jsou následující:

- Instalace a konfigurace Zabbixu jako centrálního monitorovacího a bezpečnostního řešení.

- Integrace Wazuh, OpenVAS a Security Onion do Zabbixu, aby byla data z těchto nástrojů zobrazována v jednotné formě.
- Nastavení automatizovaných upozornění a reportů pro různé úrovně závažnosti bezpečnostních událostí.
- Optimalizace a úprava konfigurace jednotlivých nástrojů tak, aby bylo dosaženo co nejlepšího možného výkonu a efektivity při minimalizaci falešných poplachů.
- Testování celého systému za účelem ověření správného fungování a detekce potenciálních zlepšení.

V rámci této části práce se bude postupovat krok za krokem při implementaci, instalaci a konfiguraci jednotlivých nástrojů a jejich integrace do Zabbixu. V závěru se provede zhodnocení dosažených výsledků a jejich přínosu pro zajištění bezpečnosti IT infrastruktury.

Cílem je vytvořit ucelený a přehledný systém pro monitorování a zajištění bezpečnosti informačních systémů, který bude jednoduše škálovatelný a přizpůsobitelný dle potřeb organizace. Toto je potřeba zejména z toho důvodu, aby administrátor nebo správce sítě nemusel mít otevřené další systémy nebo okna v prohlížeči. Tím bude mít všechno přehledně v jednom systému. Výsledkem bude komplexní řešení, které umožní rychlou identifikaci, reakci a řešení bezpečnostních hrozeb, což povede ke zvýšení úrovně zabezpečení IT infrastruktury a informačních systémů.

4.2.1 Představení zkoumaného prostředí

Firma XYZ je středně velká společnost zaměřená na provoz a poskytování služeb civilního letiště. Firma byla založena v roce 2007 a od té doby si vybudovala silnou reputaci díky svému odbornému týmu a inovativním řešením. Společnost se zaměřuje na kvalitu, spolehlivost a bezpečnost svých služeb, což je důvod, proč si udržuje dlouhodobé vztahy se svými zákazníky a uživateli letiště.

IT infrastruktura společnosti Firma XYZ se skládá ze 100 počítačů, jež zaměstnanci využívají pro řízení letištních operací, administrativní práce a dalších úkolů. Firma provozuje 10 serverů, které nabízejí nezbytné služby, jako jsou databázové servery, aplikační servery, e-mailové servery a systémy pro zálohování dat.

Společnost pro správu a přenos dat mezi jednotlivými síťovými zařízeními využívá 4 switche, které zajišťují efektivní a spolehlivé spojení mezi počítači, servery a ostatními

síťovými komponenty. K naplnění potřeb tisku a kopírování zaměstnanců firma rovněž provozuje 5 síťových tiskáren.

Firma XYZ se rozhodla investovat do vývoje a nasazení komplexního monitorovacího a bezpečnostního řešení s cílem zlepšit zabezpečení IT infrastruktury a chránit citlivé informace a data klientů. Účelem tohoto řešení je zajistit, že všechny systémy a aplikace budou provozovány s co nejvyšším výkonem a dostupností. Diplomová práce se soustředí na návrh a nasazení tohoto řešení do IT infrastruktury firmy XYZ, aby se dosáhlo zvýšení bezpečnosti a efektivity IT prostředí firmy.

4.2.2 Implementace Zabbix

Příprava prostředí pro implementaci

Pro správnou implementaci a provoz Zabbixu je důležité splnit několik požadavků na hardware a software, které jsou uvedeny v tabulce 1. Tyto požadavky zahrnují:

Tabulka 1 - Požadavky na HW a SW

Server	Pro Zabbix server výrobce doporučuje alespoň 4 GB RAM, 2 CPU jádra a 20 GB volného místa na disku. Tyto parametry se mohou lišit podle velikosti a komplexnosti monitorovaného prostředí.
Databáze	Zabbix vyžaduje databázový systém, jako je MySQL, PostgreSQL, Oracle nebo SQLite.
Webový server	Zabbix potřebuje webový server, jako je Apache, Nginx nebo IIS.
PHP	Zabbix vyžaduje PHP verze 7.2 nebo novější s některými povinnými rozšířeními. Operační systém: Zabbix podporuje různé platformy, jako jsou Linux, Windows, macOS, FreeBSD a další.

Zdroj: Vlastní zpracování

Jedním z klíčových požadavků pro instalaci Zabbix je výběr platformy. Ne všechny platformy podporuji instalaci Zabbix serveru. Obrázek 5 znázorňuje přehled jednotlivých platforem a zda je možno instalovat server nebo agenta. Pro účely praktické části bude použit operační systém Linux, konkrétně Ubuntu 22.04.

Obrázek 5 - Zabbixem podporované platformy

Platform	Server	Agent	Agent2
Linux	x	x	x
IBM AIX	x	x	-
FreeBSD	x	x	-
NetBSD	x	x	-
OpenBSD	x	x	-
HP-UX	x	x	-
Mac OS X	x	x	-
Solaris	x	x	-
Windows	-	x	x

Zdroj: ZABBIX documentation HW requirements, 2023

Instalace a konfigurace Zabbix serveru

Zabbix lze nainstalovat různými způsoby, zde bude instalováno přímo z konzole serveru Ubuntu 22.04

Na počátku instalace je potřeba udělat aktualizaci systému, která se provede pomoci příkazu:

- *sudo apt update*
- *sudo apt upgrade*

Zabbix pro správnou funkčnost vyžaduje webový server, databázi a PHP. V tomto případě bude instalován Apache a MariaDB pomocí následujícího příkazu:

- *sudo apt install apache2 mariadb-server php php-mysql php-mbstring php-gd php-xml php-bcmath php-ldap php-xmlrpc libapache2-mod-php*

Následující příkaz vytvoří databázi a uživatele pro Zabbix:

- *sudo mysql_secure_installation*
- *sudo mysql -u root -p*
- *CREATE DATABASE zabbix character set utf8 collate utf8_bin;*
- *GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost' IDENTIFIED BY 'your_password';*
- *FLUSH PRIVILEGES;*
- *EXIT;*

Nyní lze instalovat Zabbix server. V prvním kroku se přidá repozitář Zabbix:

- *wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu22.04_all.deb*
- *sudo dpkg -i zabbix-release_6.0-1+ubuntu22.04_all.deb*
- *sudo apt update*

V tomto kroku je možno nainstalovat Zabbix server, webové rozhraní a agenta:

- *sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent*

Další krok provede import databázových schémat do vytvořené databáze:

- *zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -u zabbix -p zabbix*

Před dalším pokračováním je potřeba upravit konfigurační soubor:

- *sudo nano /etc/zabbix/zabbix_server.conf*
- *DBHost=localhost*
- *DBName=zabbix*
- *DBUser=zabbix*
- *DBPassword=your_password*

Dále je potřeba konfigurovat soubor PHP:

- *sudo nano /etc/zabbix/apache.conf*

V konfiguračním souboru PHP je třeba vyhledat řádek *„php_value data.timezone“* a nastavit správnou časovou zónu. V tomu případě musí být hodnota nastavena následovně:

- *php_value date.timezone Europe/Prague*

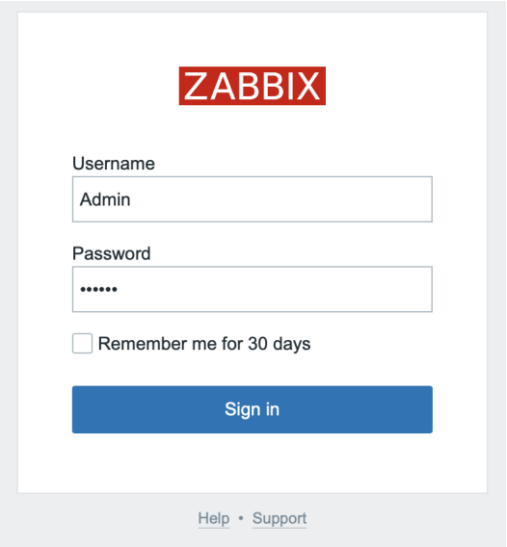
Tento krok vyžaduje restartování apache serveru, zabbix serveru a agenta. Systém dále vyžaduje nakonfigurovat následující služby tak, aby se spouštěly při startu systému:

- *sudo systemctl restart apache2*
- *sudo systemctl restart zabbix-server*
- *sudo systemctl restart zabbix-agent*
- *sudo systemctl enable apache2*
- *sudo systemctl enable zabbix-server*
- *sudo systemctl enable zabbix-agent*

Část instalace v konzoli je dokončená a nyní lze přejít do webového rozhraní Zabbix serveru.

Vyplněním zadané adresy do URL řádku v prohlížeči se otevře rozhraní zabbix, kde se musí nejdříve vyplnit uživatelské jméno a heslo, které se vytvořilo v průběhu instalace. Obrázek 6 ukazuje přihlašovací okno do Zabbix. Po zadání uživatelských přístupů se odemkne účet di nástěnky Zabbix.

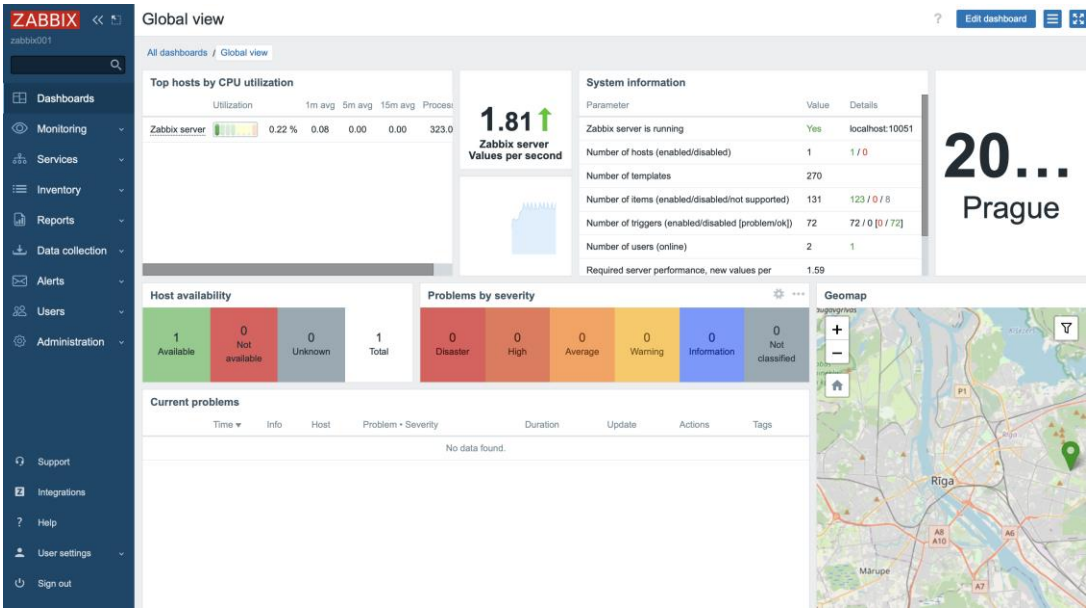
Obrázek 6 - Zabbix - přihlašovací okno do webového rozhraní



Zdroj: Vlastní zpracování

Na obrázku 7 je vidět nástěnka, která se zobrazí po vyplnění přihlašovacích údajů do Zabbix webového rozhraní.

Obrázek 7 - Zabbix - nástěnka ve webové rozhraní



Zdroj: Vlastní zpracování

Sledování zařízení a služeb pomocí Zabbix

Zabbix je vysoce flexibilní a konfigurovatelný nástroj pro monitorování IT infrastruktury, který umožňuje sledovat širokou škálu zařízení, služeb a metrik. Zde jsou vybrány některé z nich (ZABBIX, Zabbix documentation, 2023).

Sledování hardware:

- Využití CPU a zatížení.
- Využití paměti RAM
- Využití disku a volného místa na disku
- Teplota a chlazení hardwarových komponent
- Sledování stavu baterie UPS

Sledování síťových zařízení a protokolů:

- Sledování dostupnosti zařízení pomocí protokolů ICMP, TCP a SNMP
- Síťový provoz a využití šířky pásma
- Chybové a ztracené pakety
- Latence a odezva sítě

Sledování operačních systémů:

- Stav operačního systému a dostupnost
- Procesy a služby běžící na serverech
- Sledování logů a událostí operačního systému

Sledování aplikací a služeb:

- Stav a dostupnost aplikací a služeb
- Výkon aplikací a čas odezvy
- Sledování chyb a výjimek aplikací

- Sledování logů a událostí aplikací

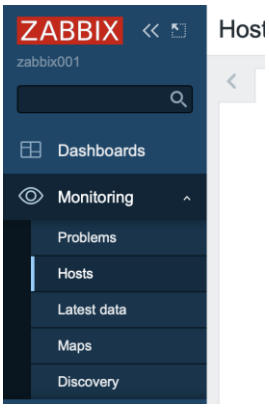
Sledování databázových systémů:

- Stav a výkon databázových systémů
- Počet připojení a transakcí
- Čas odezvy a latence databázových dotazů
- Sledování logů a událostí databázových systémů

Přidání a konfigurace zařízení

Pro přidání a konfiguraci zařízení je nutné se přihlásit do webového rozhraní Zabbix pomocí přihlašovacích údajů. Vlevo se nachází navigační menu rozhraní, které obsahuje jednotlivé položky. Přidání nového zařízení se provádí v „Monitoring“ a dále „Host“. U starších verzí Zabbix se nové zařízení přidává přes „Configuration“ a dále „Host“. Po otevření stránky se objeví seznam všech přidaných zařízení. Obrázek 8 ukazuje kde v navigačním menu lze přidat nového hosta.

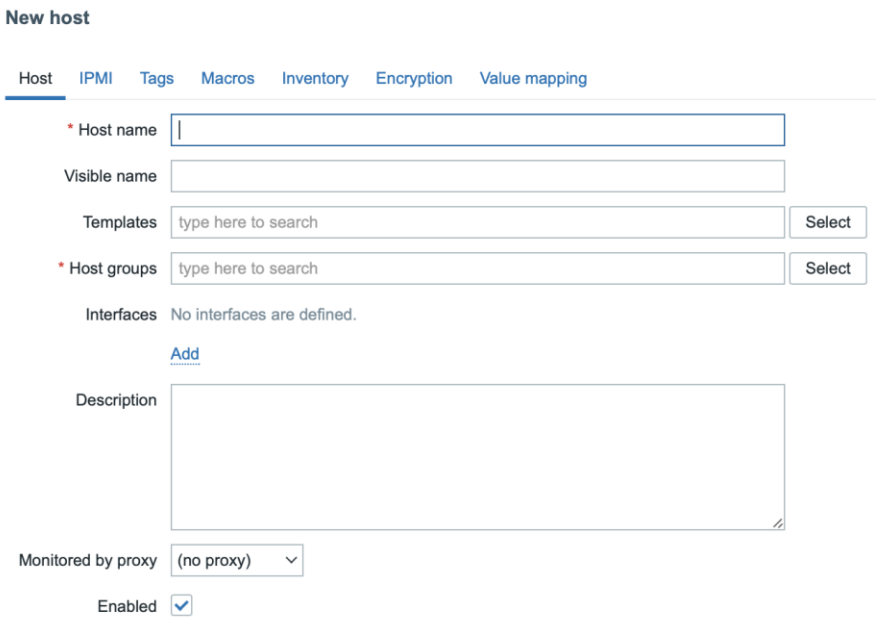
Obrázek 8 - Zabbix – přidání nového zařízení



Zdroj: Vlastní zpracování

Vlevo nahoře je tlačítko „Create host“, které slouží pro přidání nového zařízení. Po kliknutí na tlačítko se objeví formulář pro přidání nového zařízení. Parametry pro nového hosta lze vidět na obrázku 9.

Obrázek 9 - Zabbix – formulář pro přidání zařízení



Zdroj: Vlastní zpracování

Ve formuláři je třeba vyplnit několik položek, které jsou důležité pro sledování zařízení v rámci Zabbix serveru. Konkrétně se jedná o následující položky: Host name, Visible name, New group, Type, IP address, DNS name, Connect to a Port.

Položka Host name se týká jména zařízení, které je sledováno a mělo by být jedinečné v rámci Zabbix serveru. Položka Visible name zase určuje zobrazované jméno zařízení, které může být stejné jako Host name nebo může být odlišné, pokud je potřeba zařízení rozlišit jiným způsobem. Další důležitou položkou je New group, což je skupina, do které je možno zařízení zařadit. Skupiny slouží k organizaci zařízení podle různých kritérií, například podle umístění, typu zařízení nebo výrobce. Položka Type se týká typu komunikace mezi Zabbix serverem a sledovaným zařízením. Nejběžnější volbou je "Agent", ale lze zvolit i jiné typy, jako jsou SNMP, IPMI nebo JMX. Další položky jsou IP address, která určuje IP adresu zařízení, které Zabbix sleduje a DNS name, pokud je k dispozici. Zabbix může použít buď IP adresu nebo DNS jméno pro komunikaci se zařízením. Položka Connect umožňuje vybrat způsob, jakým se má připojit ke sledovanému zařízení, a to buď pomocí IP adresy nebo DNS

jména. Nakonec položka Port určuje, na kterém komunikuje Zabbix agent (nebo jiný protokol) na sledovaném zařízení. Výchozí port pro Zabbix agenta je 10050.

V záložce "Templates" lze přiřadit šablony, které definují metriky a pravidla pro sledování zařízení:

- Link new templates: Šablony, které je nutno přiřadit k zařízení. Můžu vybírat z předdefinovaných šablon nebo vytvořit vlastní.
- Linked templates: Zde vidím přiřazené šablony pro dané zařízení.

V záložce "Macros" je možnost nastavit uživatelské makro pro zařízení. Makra umožňují definovat proměnné hodnoty, které mohou být použity v rámci šablon a položek.

V záložce "Host inventory" lze zadat údaje o zařízení, jako jsou informace o hardwaru, softwaru, síťových rozhraních a další.

Kliknutím na tlačítko "Add" ve spodní části stránky je konfiguraci zařízení uložena. Zabbix nyní začne sledovat zařízení podle nastavených metrik a pravidel. Pokud byla zvolena komunikace typu "Agent", je třeba nainstalovat a nakonfigurovat Zabbix agenta na sledovaném zařízení.

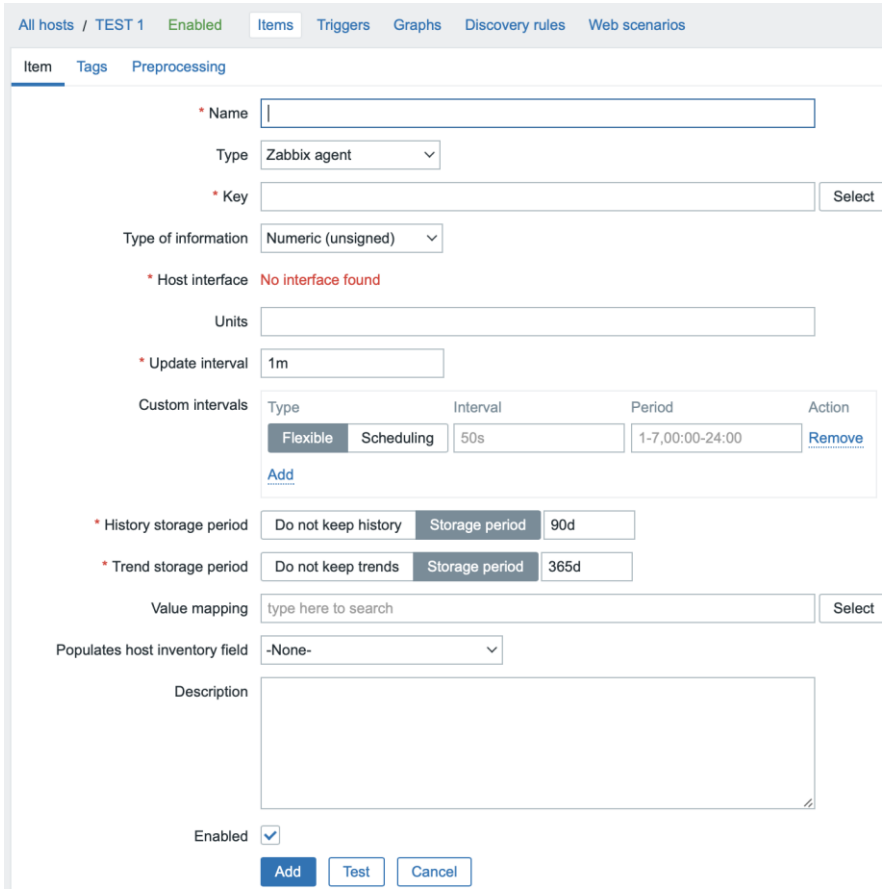
Definování metrik a pravidel pro sledování zařízení

Metriky a pravidla pro sledování jsou důležitou součástí monitorovacího systému, jelikož umožňují monitorovat výkon zařízení a provoz v síti. V aplikaci Zabbix se tyto metriky a pravidla definují pomocí položek, triggerů a šablon.

Položky jsou jednotlivé metriky, které Zabbix shromažďuje od sledovaných zařízení. Tyto metriky mohou zahrnovat informace o výkonu zařízení, jako je využití procesoru, paměti nebo disku, a informace o provozu v síti, jako je rychlost přenosu dat, zpoždění nebo počet aktivních spojení.

Novou položku lze nastavit pomocí navigačního menu vlevo. Nastavení položek se nachází v „Data collection“ a opět „Host“. Následně lze vybrat zařízení, které se přidalo v předchozím kroku a kliknu na položku „item“. Nyní lze vytvořit novou položku pomocí tlačítka „create item“. Jak vypadá přidání nové položky je znázorněno na obrázku 10.

Obrázek 10 - Zabbix – přidání nové položky



Zdroj: Vlastní zpracování

Při definování položky je třeba, aby uživatel nastavil několik klíčových parametrů. Prvním z nich je název, což je jednoznačný popisný identifikátor položky. Dále je třeba nastavit klíč, což je unikátní identifikátor, který se používá pro komunikaci se Zabbix agentem nebo jiným protokolem. Třetím důležitým parametrem je typ sběru dat, který může být Zabbix agent, SNMP, JMX, IPMI nebo externí skript. Další položkou, kterou je třeba nastavit, je typ informací, který položka shromažďuje. Typ dat může být například číslo, znak, text nebo log. Posledním klíčovým parametrem, který je třeba definovat, je interval aktualizace, což je frekvence, s jakou Zabbix shromažďuje data pro tuto položku.

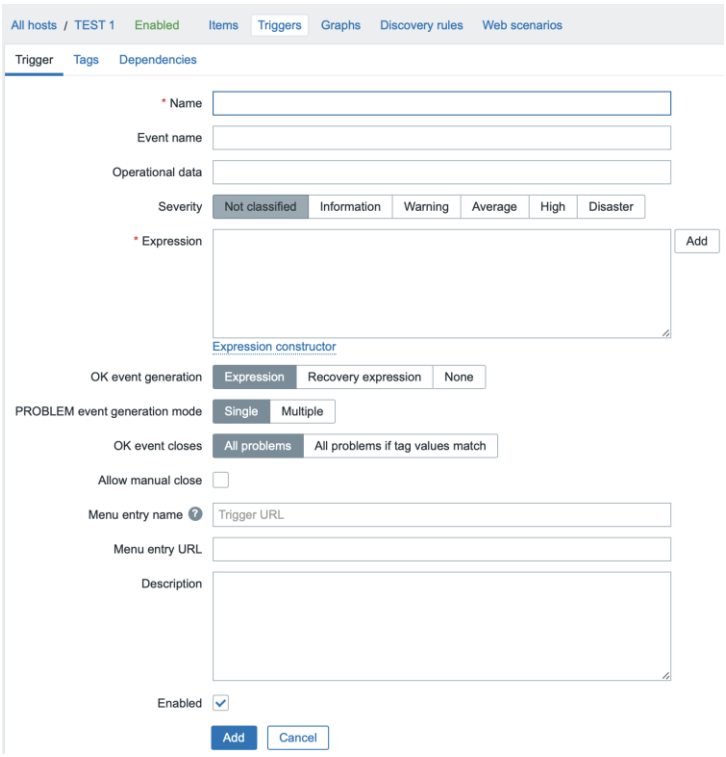
Triggery jsou pravidla, která definují, kdy je sledované zařízení nebo provoz v síti považován za problémový. Triggery vyhodnocují data shromažďovaná položkami a generují události, když jsou splněny určité podmínky.

Postup pro nastavení triggerů je podobný jako u položek. Triggery se nacházejí v „Data collection“ a „Hosts“. Zde stejným způsobem jako u položek vybrat požadované zařízení a dále vybrat „Triggers“.

Při definování triggeru v systému Zabbix je nutné specifikovat několik parametrů. Mezi tyto parametry patří název triggeru, který slouží k popisu triggeru a musí být jednoznačný. Dalším důležitým parametrem je výraz, což je logický výraz, který definuje podmínky pro vyhodnocení triggeru. Tento výraz může obsahovat reference na položky, operátory a funkce.

Jiným důležitým parametrem je závažnost, která určuje úroveň závažnosti problému, který trigger detekuje. V systému Zabbix je k dispozici několik úrovní závažnosti, včetně "Not classified", "Information", "Warning", "Average", "High" a "Disaster". Závažnost triggeru ovlivňuje kritičnost a způsob oznámení o problémech, které trigger detekuje. Konfigurace triggeru popisuje obrázek 11.

Obrázek 11 - Zabbix – konfigurace triggeru



Zdroj: Vlastní zpracování

Šablony jsou předdefinované sady položek a triggerů, které lze aplikovat na zařízení pro snadné sledování běžných metrik a pravidel. Zabbix obsahuje několik předdefinovaných

šablon pro běžné typy zařízení a služeb, jako jsou servery, síťové prvky, databáze a webové aplikace. Můžete také vytvářet vlastní šablony pro specifické potřeby vaší organizace.

Při práci se šablonami v Zabbixu je třeba vzít v úvahu několik aspektů. Zabbix umožňuje importovat a exportovat šablony ve formátu XML, což usnadňuje sdílení šablon mezi různými instalacemi Zabbix nebo s komunitou. Pro vytvoření vlastní šablony je třeba přidat relevantní položky a triggery, které chcete sledovat na zařízeních, na která bude šablona aplikována. Aby byla šablona aplikována na konkrétní zařízení, je třeba ji přidat do seznamu "Linked templates" v konfiguraci tohoto zařízení. Jakmile je šablona aplikována, všechny položky a triggery obsažené v šabloně budou automaticky sledovány na daném zařízení.

V některých případech může být nutné přizpůsobit metriky a pravidla pro sledování konkrétním potřebám organizace.

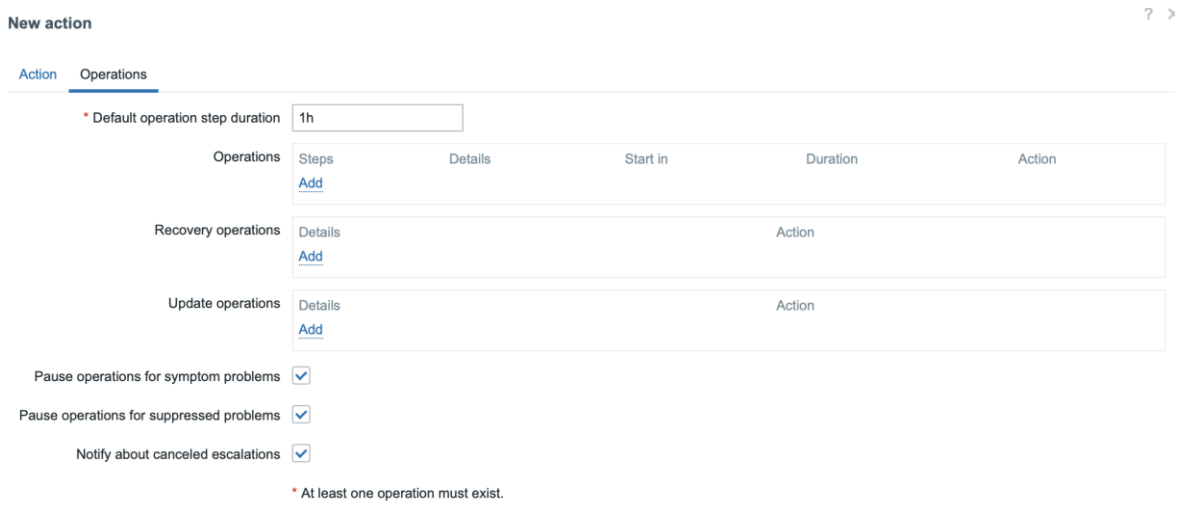
Nastavení upozornění a zasílání zpráv

V monitorovacím systému jsou upozornění a zasílání zpráv důležitými prvky, které informují správce a další zainteresované strany o problémech nebo událostech v monitorované infrastruktuře. Systém Zabbix poskytuje možnost flexibilní a konfigurovatelné konfigurace pro nastavení upozornění a zasílání zpráv.

V Zabbixu se akce provádějí jako procesy, které se spustí, když trigger detekuje problém nebo když jsou splněny určité podmínky. Tyto akce mohou zahrnovat zasílání upozornění, spuštění externích skriptů nebo změnu konfigurace sledovaných zařízení.

Aby bylo možné nastavit akci pro zasílání upozornění, je třeba provést následující kroky. V navigačním menu vlevo je položka „Alerts“ pod kterou je „Actions“. Kliknutím na actions se otevře nové okno, kde pomocí tlačíka „Creat action“ můžeme vytvořit akci. Na kartě "Conditions" mohu přidat podmínky, které musí být splněny, aby byla akce spuštěna. Podmínky mohou zahrnovat úroveň závažnosti, typ události nebo hodnoty získané z položek. Na kartě "Operations" lze nastavit typ operace, která má být provedena, když jsou splněny podmínky akce. Dále zde mohu nastavit, jakým způsobem chci být informován o aktivaci podmínky pro odeslání upozornění. Na obrázku 12 je možno vidět konfiguraci akce pro oznámení události.

Obrázek 12 - Zabbix – konfigurace akce pro oznámení události

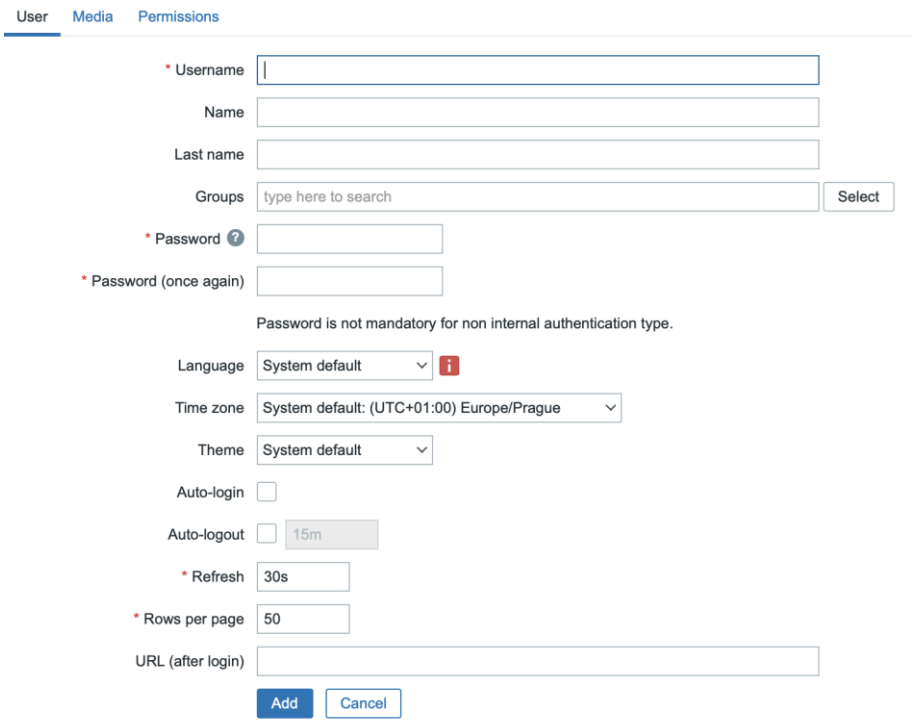


Zdroj: Vlastní zpracování

V aplikaci Zabbix se správa upozornění zakládá na uživatelských účtech a skupinách, které definují, kdo má přístup k informacím o událostech a kdo má dostávat upozornění.

V části "Administration" a poté na "Users" nebo "User groups" v navigačním menu se lze podívat na seznam uživatelů případně na uživateslské skupiny. Kliknutím na tlačítko "Create user" nebo "Create user group" se vytvoří nový uživatel. Vytvoření nového uživatele znázorňuje obrázek 13.

Obrázek 13 - Zabbix – vytvoření nového uživatele



Zdroj: Vlastní zpracování

V založení nového uživatele je nutné vyplnit požadované informace, jako jsou jméno, heslo, e-mailová adresa nebo telefonní číslo pro uživatele nebo jméno a členové pro uživatelskou skupinu. V záložce „Permissions“ lze uživateli nebo uživatelské skupině přiřadit přístupová práva k hostitelům, položkám a triggerům, které jsou vyžadovány sledovat.

Typy médií určují způsob, jakým jsou zprávy a upozornění posílány uživatelům a skupinám v aplikaci Zabbix. Zabbix nabízí podporu pro několik základních typů médií, jako jsou e-mail, SMS nebo Jabber, a je také možné přidat vlastní typy médií pomocí externích skriptů nebo API.

4.2.3 Propojení Zabbix a Wazuh

Instalace a konfigurace Wazuh serveru části

Wazuh server, jak již bylo zmíněno v teoretické části diplomové práce je bezpečnostní platforma s open source kódem, která je určena pro monitorování, detekci hrozeb a prevenci škod. Centrální komponentou Wazuh platformy je Wazuh server, který shromažďuje, analyzuje a spravuje bezpečnostní data z Wazuh agentů, nainstalovaných na různých zařízeních v síti.

Wazuh server může být nainstalován na 64bitovém operačním systému Linuxu. Wazuh platforma podporuje následující verze operačních systémů: Jaké operační systémy a jejich verze popisuje tabulka 2.

Tabulka 2 - Wazuh – operační systémy podporující Wazuh Server

Amazon Linux 2	CentOS 7,8
Red Hat Enterprise Linxu 7,8,9	Ubuntu 16.04, 18.04, 20.04, 22.04

Zdroj: Wazuh documentation, 2023

Minimální požadavky pro instalaci Wazuh serveru jsou 2 GB RAM a 2 jádra procesoru, doporučené jsou pak 4 GB RAM a 4 jádra. Celá instalace se skládá ze tří částí a to instalace Wazuh indexer, Wazuh server a Wazuh dashboard

Existují různé způsoby instalace Wazuh, které se liší v závislosti na preferencích a potřebách uživatele. Mezi základní způsoby instalace patří instalace pomocí balíčků, instalace pomocí obrazu disku a instalace pomocí kontejnerů.

Pro instalaci pomocí balíčků jsou k dispozici balíčky pro různé operační systémy, jako jsou Debian, Ubuntu, Red Hat, CentOS a SUSE. Tento způsob instalace je považován za poměrně snadný a umožňuje rychlé nasazení Wazuh serveru.

Další možností je instalace pomocí obrazu disku, který lze stáhnout a nainstalovat na vhodné hardwarové zařízení. Tento způsob instalace je vhodný pro uživatele, kteří chtějí instalovat Wazuh na fyzický stroj nebo virtuální stroj.

Alternativně lze Wazuh nainstalovat pomocí kontejnerů, což umožňuje snadnou a rychlou instalaci na různých platformách. Tento způsob instalace je vhodný pro uživatele, kteří používají technologie kontejnerizace, jako je například Docker.

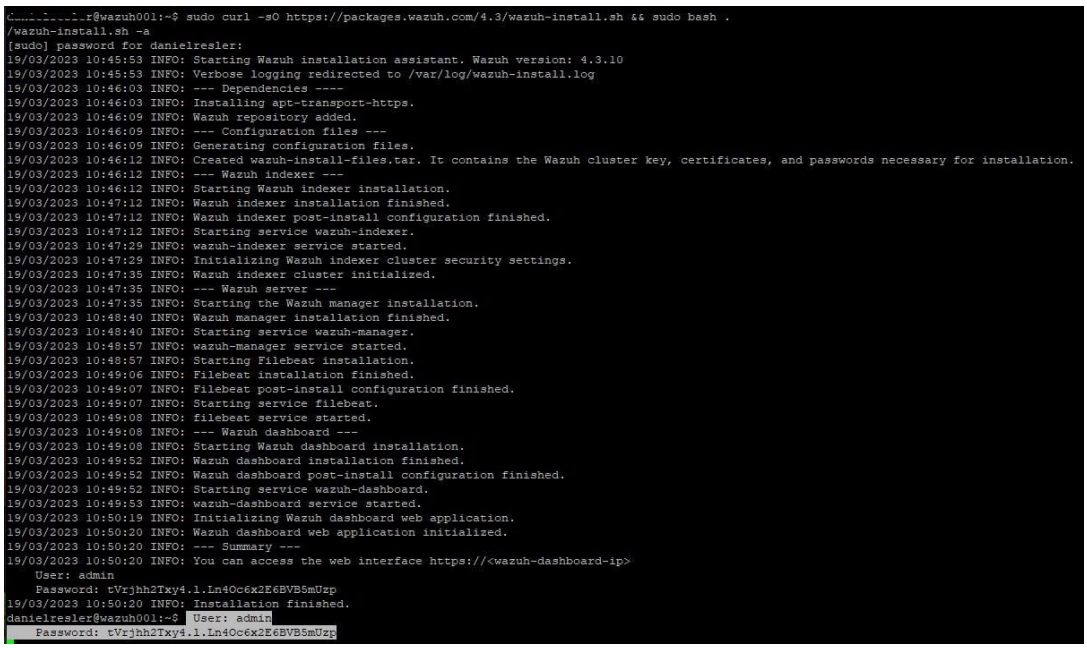
Při instalaci Wazuh je důležité dodržet dokumentaci a postup instalace, který je vhodný pro konkrétní operační systém nebo platformu. Pro účel praktické části diplomové práce bude serverová část nainstalována pomocí Wazuh instalačního asistenta, které značně urychlí proces instalace.

Stažení a instalace Wazuh instalačního asistenta je prvním krokem instalace, který se provede pomocí následujícího příkazu:

- *curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh && sudo bash ./wazuh-install.sh -a*

Jakmile asistent dokončí instalaci, na výstupu se zobrazí přístupové údaje a zpráva potvrzující, že je instalace úspěšně dokončená, to je možno vidět na obrázku 14.

Obrázek 14 - Wazuh – výsledek instalace



Zdroj: Vlastní zpracování

Při prvním přístupu do nástěnky Wazuh se v prohlížeči zobrazí varovná zpráva, že certifikát nebyl vydán důvěryhodnou autoritou. To je očekávané a uživatel má možnost přijmout certifikát jako výjimku, případně nakonfigurovat systém tak, aby používal certifikát od důvěryhodné autority (WAZUH, Wazuh documantation - quickstart, 2023). Obrázek 15 ukazuje přihlašovací okno do WAZUH rozhraní.

Obrázek 15 - Wazuh – přihlašovací obrazovka do rozhraní

Zdroj: Vlastní zpracování

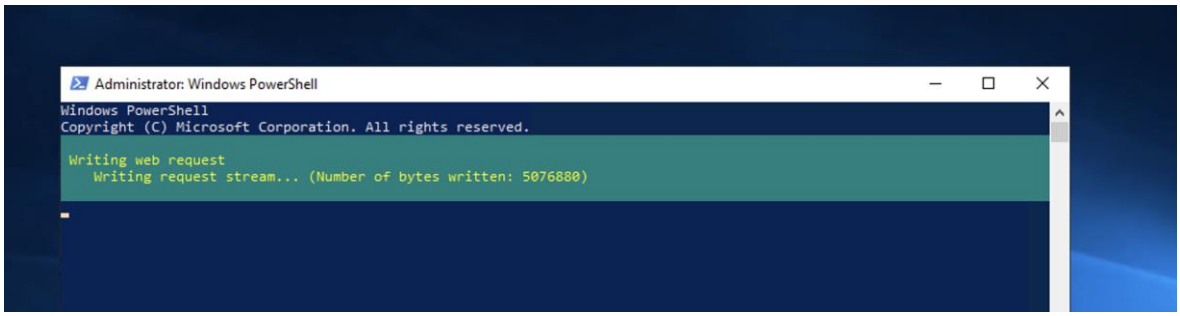
Instalace Wazuh agenta na klienta

Instalace Wazuh agenta je velice jednoduchá. Po přihlášení se do administrace Wazuh serveru nevidíme žádné agenty. Rozhraní zobrazuje „tlačítko“ přidat agenta, které přesměruje na další stránku s pokyny pro instalaci agenta. Na nově otevřené stránce je nutno vyplnit operační systém, na který je agent instalován, IP adresu Wazuh serveru a skupinu, která je v základu předdefinovaná jako default. Instalace se provádí pomocí powershell, který musí být spuštěný jako správce. To platí pro stanici i server. Vložením následujícího skriptu, který se automaticky vygeneruje po vyplnění zmíněných požadavků se začne agent instalovat:

- *Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.10-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.10.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.10.msi /q WAZUH_MANAGER='192.168.110.85' WAZUH_REGISTRATION_SERVER='192.168.110.85' WAZUH_AGENT_GROUP='default'*
- *NET START WazuhSvc*

Průběh instalace agenta ukazuje obrázek 16.

Obrázek 16 - Wazuh – průběh instalace agenta

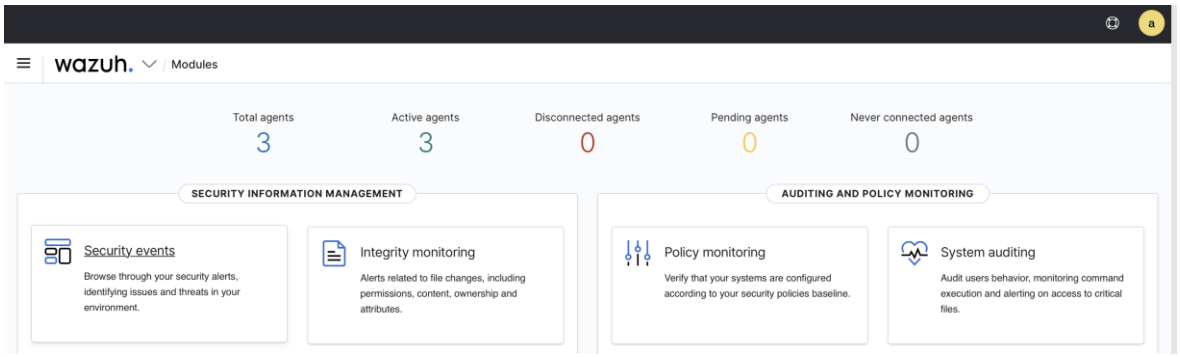


Zdroj: Vlastní zpracování

Po dokončení instalace se v nástěnce Wazuh serveru zobrazí celkový počet klientů a počet aktivních klientů. V případě, že je na nějaké stanici nebo serveru porucha a agent nekomunikuje, celkový počet agentů se nemění, ale aktivní se změní a to je dobrý indikátor chybového stavu. V aktivních agentech je možno zobrazit seznam všech připojených aktivních zařízení, u kterých vidíme informace jako název zařízení, IP adresu, verzi OS a tak dále.

Agenti nainstalovaní na stanici poskytují širokou škálu možností pro monitorování a detekci bezpečnostních incidentů. Systémové logy se sbírají a analyzují, aby se identifikovaly podezřelé aktivity a potenciální bezpečnostní hrozby. Detekce narušení umožňuje agentům monitorovat a detekovat pokusy o neoprávněný přístup k citlivým datům nebo neoprávněné změny konfigurace. Sledování souborové integrity a procesů a aplikací pomáhá identifikovat jakékoli neoprávněné změny nebo manipulace. Sběr metrik umožňuje agentům sbírat informace o výkonu a zdrojích hostitelů, což umožňuje sledovat, jak jsou využívány zdroje. Kromě toho mohou agenti kontrolovat zranitelnosti a konfiguraci, aby se zajistilo, že jsou systémy chráněny před potenciálními hrozbami. Celkově lze říci, že agenti nainstalovaní na stanici poskytují důležité nástroje pro detekci, analýzu a prevenci bezpečnostních incidentů. Náhled do nástěnky je možno vidět na obrázku 17.

Obrázek 17 - Wazuh – náhled do nástěnky



Zdroj: Vlastní zpracování

Integrace systému Wazuh se Zabbixem

Přímá integrace systému Wazuh a systému Zabbix není v dokumentaci obou systémů popsána. Propojení prostřednictvím již hotových modulů není v současné době dostupné, oba systémy lze propojit několika předpokládanými způsoby:

1. Zabbix Agent a Wazuh API:
   - Instalace Zabbix agenta na stejném serveru, kde běží Wazuh Manager.
   - Vytvořit uživatelský skript na Wazuh serveru, který získává data z Wazuh API a předávat je Zabbix agentovi.
   - Nakonfigurovat Zabbix agenta, aby spouštěl uživatelský skript pro získání dat z Wazuh API.
   - Vytvořit šablony a pravidla pro zpracování dat v Zabbix serveru.
2. Wazuh Modul pro Zabbix:
   - Vytvořit nebo najít Wazuh modul pro Zabbix, který zprostředkovává komunikaci mezi Wazuh a Zabbixem.
   - Nainstalovat a nakonfigurovat modul na Wazuh serveru.
   - Vytvořit šablony a pravidla v Zabbix serveru pro zpracování dat z Wazuh modulu.
3. Integrace pomocí scriptů a logů
   - Analyzovat logovací systém systému Wazuh.
   - Připravit script, který vyhodnotí požadované události v rámci logů systémů Wazuh.
   - Zamýšlené události odeslat ke zpracování do systému Zabbix.
   - Vytvořit šablony a pravidla v Zabbix serveru pro zpracování dat z logovacího systému Wazuh.

4. Přímá integrace pomocí Zabbix API:
    - Vytvořit skript nebo aplikaci, která získává data z Wazuh API a odesílá je do Zabbixu pomocí Zabbix API.
    - Spustit skript nebo aplikaci na Wazuh serveru nebo na jiném serveru s přístupem k oběma API.
    - Vytvořit šablony a pravidla v Zabbix serveru pro zpracování dat z Wazuh API.

Při propojování Wazuhu se Zabbixem je důležité zvážit bezpečnostní a výkonnostní aspekty, jako je šifrování komunikace a autentizace.

V rámci integrace obou systémů se také zvažuje náročnost a znalosti osoby, která implementaci provádí, tedy aby nebylo nutné příliš komplikované programování a testování. V integraci se zaměřuje na zprostředkování typických událostí, které v systému Wazuh vznikají a které obvykle administrátor v systému Wazuh manuálně vyhodnocuje a jsou klíčové pro okamžité řešení a okamžitý zásah a mohou vést k pokusu narušení systému nebo k jeho narušení. Propojení bude realizováno analýzou logů systému Wazuh a předání pozitivních nálezů systému Zabbix ke zpracování, vyhodnocení a zobrazení v dashboardu Zabbixu.

Logovací soubory a umístění událostí systému Wazuh

Logovací soubory alerts.log a alerts.json obsahují záznamy o detekovaných událostech a vytvořených varováních (alerts) v prostředí Wazuh. Tyto soubory jsou zásadní pro analýzu bezpečnostních incidentů a jejich řešení.

Typická umístění logovacích souborů ve Wazuhu jsou následující:

- alerts.log: /var/ossec/logs/alerts/alerts.log
- alerts.json: /var/ossec/logs/alerts/alerts.json

Obsah těchto souborů zahrnuje informace o detekovaných událostech, které splňují určitou úroveň závažnosti nebo pravidla, která jsou nastavena v konfiguraci Wazuh. Varování mohou být generována například při detekci neoprávněného přístupu, změně systémových souborů nebo podezřelé síťové aktivitě.

Alerts.log obsahuje záznamy ve formátu plain text, které jsou pro lidské čtení jednoduché a přehledné. Na druhou stranu, alerts.json obsahuje stejné informace, ale ve formátu JSON, což je vhodnější pro strojové zpracování a integraci s dalšími nástroji pro analýzu dat a vizualizaci.

Každé varování obsahuje následující informace:

- Datum a čas události
- ID pravidla, které spustilo varování
- Úroveň závažnosti
- Popis události
- Zdrojová a cílová adresa (pokud je relevantní)
- Detekční modul nebo integrace, který generoval varování (např. systémový audit, síťová detekce, File Integrity Monitoring apod.)
- Další podrobnosti relevantní pro konkrétní událost nebo pravidlo

Wazuh umožňuje správcům upravovat pravidla a úrovně závažnosti, aby byla varování relevantní pro jejich prostředí a potřeby.

Událost 4625

Událost 4625 v systému Windows označuje neúspěšný pokus o přihlášení. Tato událost se zaznamenává v logu systému Windows, pokud se někdo pokusí přihlásit k počítači nebo serveru s neplatnými přihlašovacími údaji nebo povoleními. Záznam obsahuje následující informace:

- Datum a čas události
- Zdrojový počítač a účet
- Cílový počítač a účet
- Typ přihlašovacího procesu (např. interaktivní, služba, síť)
- Přihlašovací ID
- Stav a podrobný kód stavu
- Důvod neúspěchu (špatné jméno, špatné heslo, omezený časový rozsah apod.)

Událost 4625 je důležitá z hlediska zabezpečení, protože může naznačovat pokus o neoprávněný přístup nebo útok na systém. Správci systému by měli být v případě opakovaných neúspěšných pokusů o přihlášení ostražití a zvážit další kroky k zabezpečení prostředí, jako jsou například zesílení pravidel hesel nebo omezení přístupu na základě IP adres a prověřit důvod vzniku události.

Instalace Zabbix_sender

Zabbix_sender je součástí balíčku zabbix-agent.

Zabbix_sender je nástroj pro odesílání hodnot sledovaných položek do Zabbix serveru. Tento nástroj umožňuje odesílat data z externích zdrojů, jako jsou skripty nebo aplikace, přímo do Zabbix serveru. Zabbix_sender využívá protokol zvaný "Zabbix trapper" a očekává, že na straně Zabbix serveru jsou nakonfigurovány příslušné trapper položky.

Příklad odeslání zprávy s textem "4625" na Zabbix server s IP 192.168.110.84:

zabbix_sender -z 192.168.110.84 -s wazuh001 -k udalost-60122 -o "4625"

Vyhodnocení událostí 4625

Událost 4625 je událostí, které by administrátor měl věnovat pozornost. Vhodným souborem k analýze je alerts.json. K analýze logu ve formátu JSON alerts.json bude vytvořen script v programovacích jazyce python, který zkontroluje ve stanoveném intervalu soubor alerts.json a všechny nové události 4625 a vypíše je na konzoli a prostřednictvím zabbix_senderu a odešle do systému zabbix. Pokud žádná nová událost nevznikne, tak script zobrazí informaci *Žádné nové informace.*

```
import json
import subprocess
from jq import jq
from datetime import datetime

last_processed_file = "last_processed_timestamp.txt"
alerts_file = "alerts.json"

if last_processed_file:
    with open(last_processed_file, "r") as f:
        last_processed_timestamp = f.read().strip()
else:
    last_processed_timestamp = "1970-01-01T00:00:00Z"

records = []
with open(alerts_file, "r") as f:
    for line in f:
        records.append(json.loads(line.strip()))
```

```
jq_query = f'.data.win.eventdata as $eventdata | .data.win.system as $system |
select($system.eventID == "4625") | select($system.systemTime >
"{last_processed_timestamp}") | {{agentIP: .agent.ip, agentName: .agent.name,
ipAddress: $eventdata.ipAddress, workstationName: $eventdata.workstationName,
targetUserName: $eventdata.targetUserName, eventID: $system.eventID, timestamp:
$system.systemTime}}'
new_records = []
for record in records:
    result = jq(jq_query).transform(record, multiple_output=True)
    if result:
        new_records.extend(result)
if new_records:
    print(json.dumps(new_records, indent=2))
    newest_timestamp = max([record["timestamp"] for record in new_records])
    with open(last_processed_file, "w") as f:
        f.write(newest_timestamp)
    # Send a message for each new record
    zabbix_server_ip = "192.168.110.84"
    zabbix_host_name = "wazuh001"
    zabbix_item_key = "udalost-4625"
    message_template = "Wazuh alert: "
    for record in new_records:
        message = f"{message_template}: {record}"
        subprocess.run(["zabbix_sender", "-z", zabbix_server_ip, "-s", zabbix_host_name, "-
k", zabbix_item_key, "-o", message])
else:
    print("Žádné nové informace.")
```

Skript provádí následující úkoly:

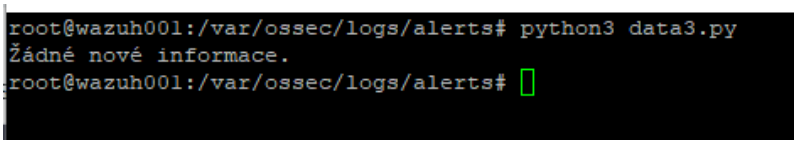
1. Importuje potřebné knihovny: json, subprocess, jq a datetime.
2. Nastavuje názvy souborů pro uložení posledního zpracovaného časového razítka a soubor s varováními ve formátu JSON.
3. Čte poslední zpracované časové razítko. Pokud neexistuje, nastaví ho na počáteční hodnotu "1970-01-01T00:00:00Z".

4. Načítá záznamy ze souboru alerts.json do seznamu records.
5. Definuje dotaz JQ, který filtruje záznamy s událostí ID 4625 a novějšími než poslední zpracované časové razítko. Výsledný objekt obsahuje informace o agentovi, IP adrese, názvu pracovní stanice, cílovém uživatelském jménu, ID události a časovém razítku.
6. Transformuje načtené záznamy pomocí dotazu JQ a ukládá nové záznamy do seznamu new_records.
7. Pokud existují nové záznamy:
8. Vytiskne nové záznamy ve formátu JSON s odsazením 2 mezer.
9. Aktualizuje soubor s posledním zpracovaným časovým razítkem.
10. Pro každý nový záznam:
11. Sestaví zprávu s textem "Wazuh alert: " a informacemi o záznamu.
12. Odešle zprávu pomocí nástroje zabbix_sender na zadaný Zabbix server, host a položku.
13. Pokud neexistují žádné nové záznamy, vytiskne "Žádné nové informace."

Tento skript je určen k analýze souboru alerts.json generovaného systémem Wazuh, extrakci událostí s ID 4625 novějších než poslední zpracované časové razítko a odeslání těchto událostí do Zabbixu pro sledování a upozornění. Obdobným způsobem lze analyzovat jakoukoli událost v systému Wazuh.

Po spuštění scriptu, pokud v logu nejsou žádné události typu 4625, se na konzolu vypíše následující událost, která je vidět na obrázku 18.

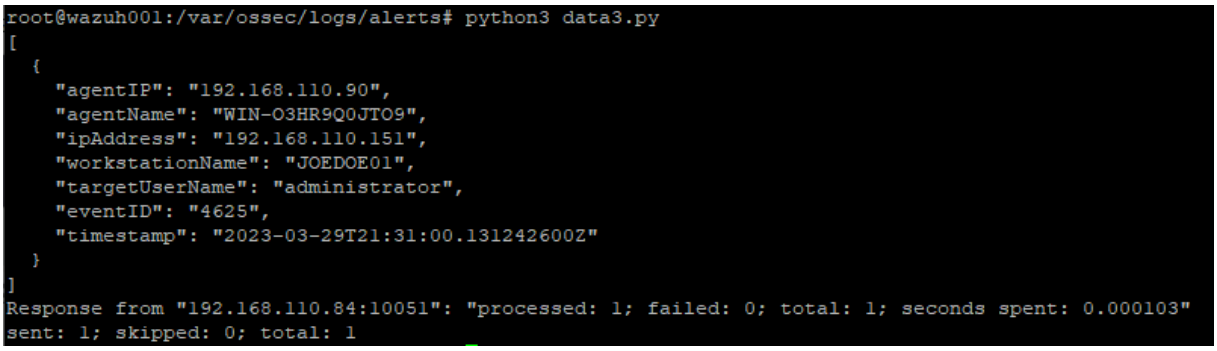
Obrázek 18 – Script bez události 4625



Zdroj: Vlastní zpracování

V případě, že došlo k události 4625, tak se na konzoli vypíše stručná informace o vzniklé události a tyto informace se odešlou přes zabbix_sender do systému Zabbix: To je možno vidět na obrázku 19.

Obrázek 19 - Script vypisující událost 4625



Zdroj: Vlastní zpracování

Konkrétně se vypíše IP adresa agenta, který detekuje událost 4625 agentIP: 192.168.110.90, dále agentName: WIN-O3HR9Q0JTO9 to je název počítače, který detekovat událost, dále ipAddress: 192.168.110.151 to je IP adresa potenciálního útočníka, workstationName: JOEDOE01 to je jméno počítače potenciálního útočníka, targetUserName: administrator to je uživatelské jméno, pod kterým vznikla událost 4625, eventID: 4625 to je typ události a jako poslední informace je timestamp: 2023-03-29T21:31:00.131242600Z to je datum vzniku události.

Nastavení systém Zabbix pro příjem událostí 4625

Pro příjem událostí systému Wazuh se vytvoří v systému Zabbix host, dále položka item a trigger, který zajistí zobrazení události na dashboardu a to ihned, jak takovou událost obdrží.

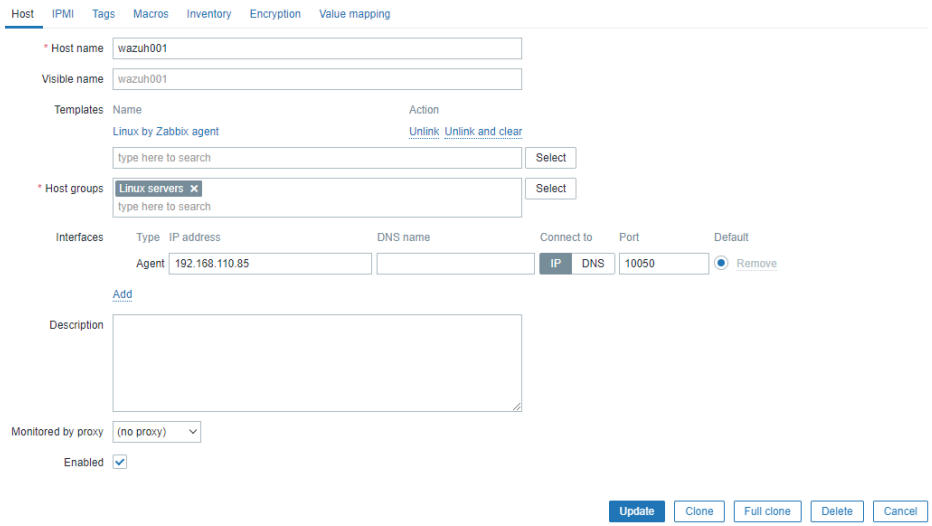
Pro nastavení Zabbix hosta s Zabbix trapperem a triggerem je postup následující:

1. Přihlášení do Zabbix UI:

   Otevřít webový prohlížeč a přihlásit se do Zabbix UI pomocí přihlašovacích údajů.
2. Přidání nového hosta
   - V levém vertikálním menu se klikne na Monitoring
   - V pravém horním rohu se klikne na Create host

Nastavení zabbix hosta pro účel diplomové práce je vidět na obrázku 20.

Obrázek 20 - Nastavení Zabbix hosta



Zdroj: Vlastní zpracování

3. Vyplní se informace o hostovi

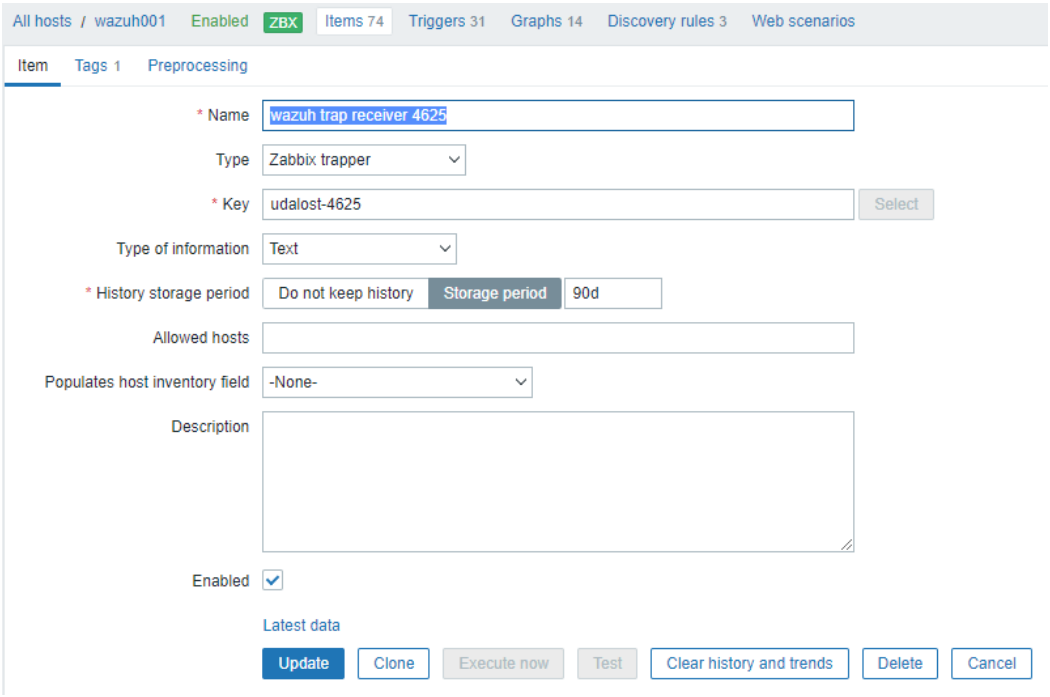
   - Host name: wazuh001
   - Visible name: wazuh001
   - Templates: Linux by Zabbix agent
   - Host Grou: Linux servers
   - Agent: 192.168.110.85

4. Nastavení Zabbix trapperu:

   - Klikne se na záložku "Items" a poté na tlačítko "Add".
   - Vyplní se následující informace:
     - Name: Zadá se název položky, např. " wazuh trap receiver 4625".
     - Type: Vybere se "Zabbix trapper" z rozbalovacího menu.
     - Key: Zadá se jedinečný klíč pro tuto položku, např. " udalost-4625".
     - Type of information: Vybere se typ informace, který bude odesílán, „Text“
     - History storage period: Vybere se Storage period 90d
   - Klikněte na "Add" pro uložení položky.

Nastavení Zabbix trapperu popisuje obrázek 21.

Obrázek 21 - Nastavení Zabbix trapperu

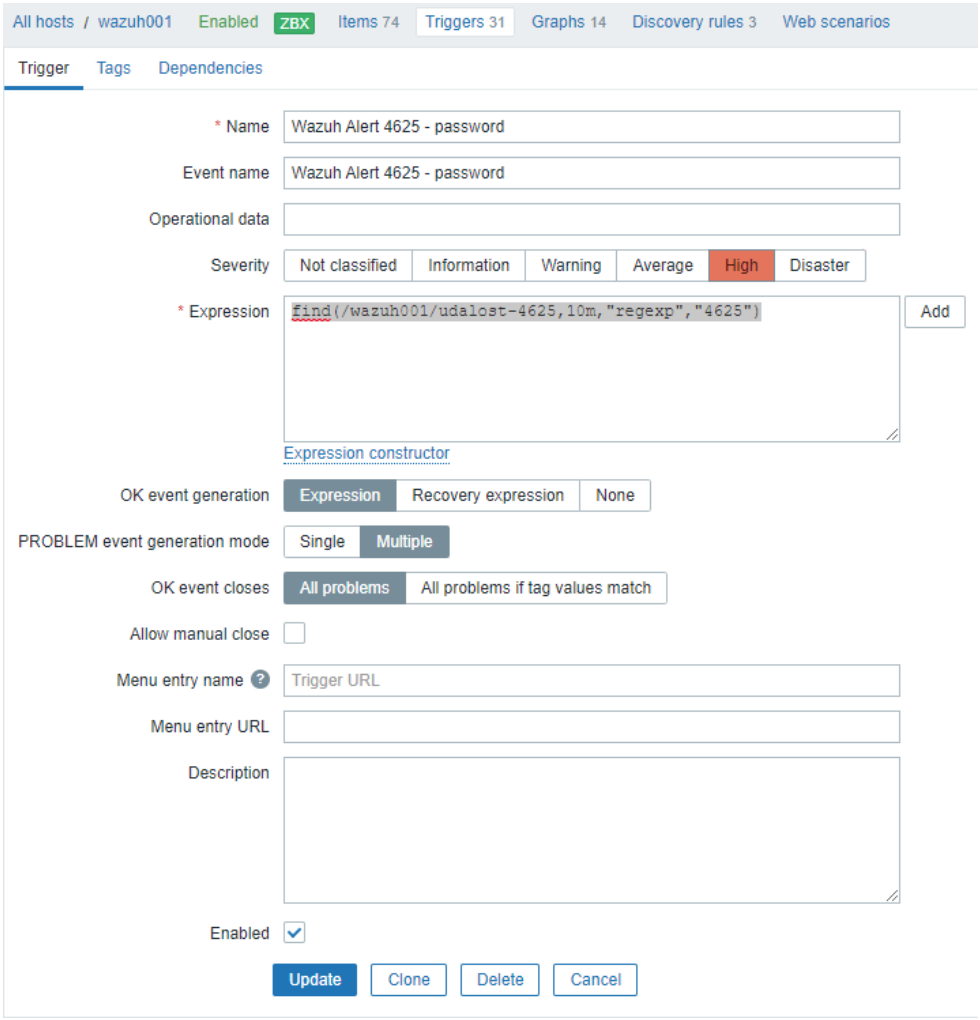


Zdroj: Vlastní zpracování

5. Nastavení triggeru:
    - Klikne se na záložku "Triggers" a poté na tlačítko "Add".
    - Vyplní se následující informace:
        - Name: Zadejte název spouštěče, např. " Wazuh Alert 4625 - password".
        - Severity: Vybere se úroveň závažnosti triggeru, např. "Warning", "Average", "High" nebo "Disaster".
        - Expression: Klikne se na tlačítko "Add" a vybere se položka, kterou jste vytvořili v kroku 4. Nastaví se podmínka spouštení triggeru, např. find(/wazuh001/udalost-4625,10m,"regexp","4625").
    - Povolí se trigger zaškrtnutím políčka "Enabled".
    - Klikne se na "Add" pro uložení triggeru.

Nastavení Zabbix triggeru je možno vidět na obrázku 22.

Obrázek 22 - Nastavení Zabbix triggeru

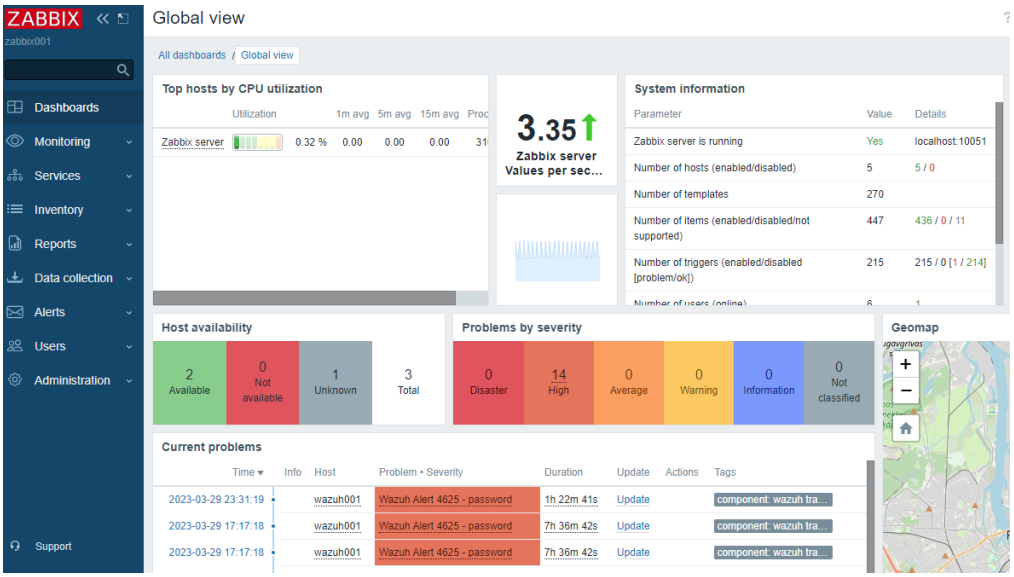


Zdroj: Vlastní zpracování

Vyhodnocení událostí v systému Zabbix

V případě, že nastala v systému Wazuh událost 4625 tak po jejím vyhodnocení scriptem, který bude zpravidla spouštěn v plánovači úloh, jako je např. cron v systému Wazuh, dojde k odeslání události do systému Zabbix a tato se objeví v dashboardu systému Zabbix. Vynesení události do nástěnky ukazuje obrázek 23.

Obrázek 23 - Vyhodnocení události v Zabbix nástěnce



Zdroj: Vlastní zpracování

V dashboardu lze identifikovat Hosta, ze kterého událost přichází a dále vážnost události. V items lze procházet zaznamenané události v položce lastest data a po vyhodnocení vážnosti situace přejít do systému Wazuh, kde lze najít kompletní informace o dané události ve formátu logu nebo json. Typický záznam v systému Zabbix popisuje obrázek 24.

Obrázek 24 - Záznam události v Items

Timestamp	Value
2023-03-29 23:31:19	Wazuh alert: : {'agentIP': '192.168.110.90', 'agentName': 'WIN-O3HR9Q0JTO9', 'ipAddress': '192.168.110.151', 'workstationName': 'JOEDOE01', 'targetUserName': 'administrator', 'eventID': '4625', 'timestamp': '2023-03-29T21:31:00.131242600Z'}
2023-03-29 17:17:18	Wazuh alert: : {'agentIP': '192.168.110.90', 'agentName': 'WIN-O3HR9Q0JTO9', 'ipAddress': '192.168.110.151', 'workstationName': 'JOEDOE01', 'targetUserName': 'administrator', 'eventID': '4625', 'timestamp': '2023-03-29T15:17:05.797596700Z'}

Zdroj: Vlastní zpracování

Závěrečná shrnutí k části propojení systému Wazuh a systému Zabbix

Oba systémy, Wazuh a Zabbix, mají nesmírný význam v oblasti sledování a monitorování. Avšak současné sledování několika systémů může být časově náročné, méně efektivní a náchylné k chybám. Správce obvykle ve Wazuh sleduje několik vybraných událostí s určitou mírou důležitosti. Tyto události lze předem určit a jejich výskyt přenášet ze systému Wazuh do systému Zabbix.

Zabbix se pak stává jediným monitorovacím systémem, který koncentruje nejen události, které může sledovat sám, ale také události přijaté ze systému Wazuh do jediného řídicího panelu neboli dashboardu. Toto propojení různých systémů se jeví jako velmi

efektivní a ekonomické řešení s možností okamžité reakce na vzniklé události, aniž by bylo nutné současně otevřít více různých systémů.

Výhody takového propojení mohou být ještě výraznější v situaci, kdy jeden subjekt sleduje systémy a události pro více různých společností. Tímto způsobem je možné zlepšit koordinaci a reakci na důležité události, zatímco se zároveň zvyšuje efektivita a snižuje náchylnost k chybám. Tato integrace nabízí významné výhody ve sledování a monitorování, což je klíčové pro úspěšné řízení infrastruktury a zajištění bezpečnosti.

4.2.4 Propojení Zabbix a SecurityOnion

Instalace a konfigurace SecurityOnion

Distribuce Linuxu Security Onion byla navržena pro síťovou bezpečnost, monitoring a analýzu a je založená na Ubuntu. Obsahuje mnoho nástrojů pro detekci a analýzu síťových hrozeb. Stejně jako u předchozích nástrojů, lze SecurityOnion instalovat různými způsoby. Instalaci lze provést na fyzickém hardwaru, do virtuálního prostředí jako je VMware nebo Virtuál box, ale také lze instalovat do cloudového prostředí (SecurityOnionSolutions, SecurityOnion documentation, 2023, přeloženo a upraveno autorem)

Security Onion podporuje pouze architekturu x86-64 standardní 64bitové procesory Intel nebo AMD. Nepodporujeme ARM ani jiné procesory jiné než x86-64! SecurityOnion je o něco náročnější software na provoz, proto vyžaduje větší hardwarovou výbavu stroje, na kterém běží. Doporučuje se, aby SecurityOnion byl nainstalován na samostatném serveru. Doporučené sestava je 12GB operační paměti RAM, 4 jádra CPU a 200GB volného místa na disk.

I v případě SecurityOnion jej lze instalovat různými způsoby. Pro instalaci serveru bylo použito instalační médium ISO, které je volně stažitelné z dokumentace. Prvním krokem instalace je takzvané „nabootování“ ISO instalačního souboru. Tím započne instalace SecurityOnion, která je znázorněna v obrázku 25.

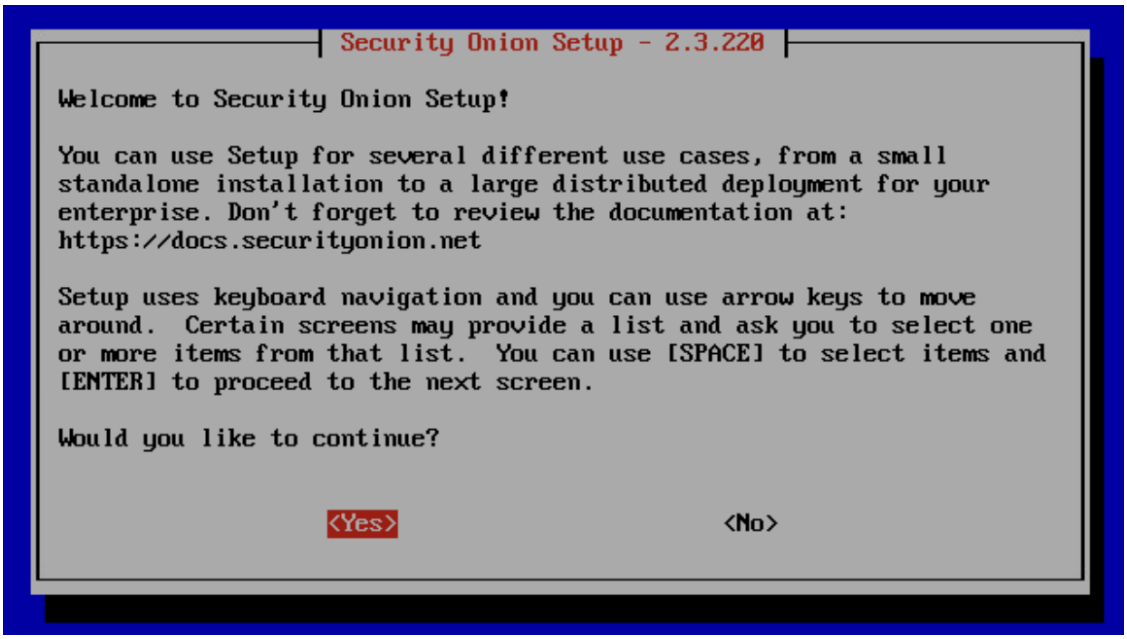
Obrázek 25 - SecurityOnion – počátek instalace

Zdroj: Vlastní zpracování

V druhém kroku je potřeba potvrdit instalaci napsáním slova „yes“ a potvrzením enterem, během okamžiku se musí vytvořit administrátorský uživatel. Jakmile je uživatel vytvořen. Začne prvotní instalace, která trvá zhruba 15 minut. Během tohoto procesu se již nic nemusí dělat a je třeba vyčkat na dokončení instalačního procesu. Po doběhnutí instalace se server začne restartovat a následuje vyplnění adiministrátorského přístupu, který byl vytvořen v prvotní instalaci.

Druhá část instalace zahrnuje vybrání verze SecurityOnion, která je požadována nainstalovat. V tomto případě verze standalone. Dále už jen IP adresu, adresu výchozí brány a DNS servery. SecurityOnion vyžaduje dvě síťová rozhraní, v této části instalace se vybírá, jaké síťové rozhraní slouží pro správu a jaké pro monitorování provozu. V průběhu instalace je potřeba vyplnit další náležitosti, nicméně pro účel práce nejsou podstatné. Druhá část instalace je zobrazena na obrázku 26.

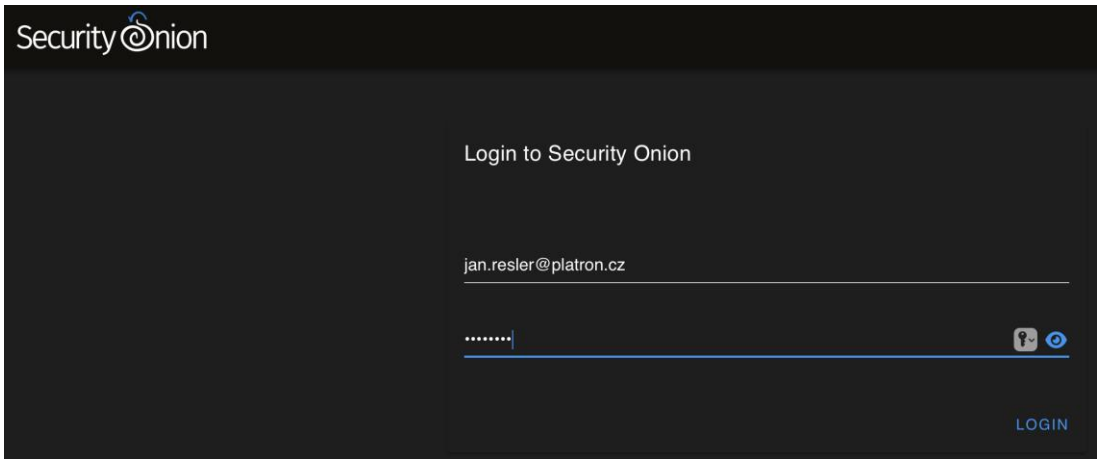
Obrázek 26 - SecurityOnion – druhá část instalace



Zdroj: Vlastní zpracování

Po úspěšném nainstalování SecurityOnion instalační průvodce oznámí, že je instalace dokončená a pod zvolenou IP adresou je přístupné webové rozhraní. V některých případech je stránka nedostupná. Před samotným spuštěním webové stránky je nutno se přihlásit přes konzoli k serveru a zadat příkaz „*sudo so-allow*“ a přidat některou z rolí pro adresu nebo celý rozsah. Přihlašovací okno do SecurityOnion je možno vidět na obrázku 27.

Obrázek 27 - SecurityOnion – přihlašovací obrazovka



Zdroj: Vlastní zpracování

Integrace systému Security Onion se systémem Zabbix

Security Onion jako bezpečnostní nástroj, který se zaměřuje na detekci a prevenci hrozeb lze propojit nebo umí předávat události a další informace následujícími metodami:

1. SNMP Traps:

SNMP Traps umožňují zařízením posílat asynchronní upozornění na události. Security Onion může být nastaven tak, aby odesílal SNMP Traps do Zabbixu. Pro toto propojení je třeba nakonfigurovat SNMP Trap přijímač v Zabbixu a nastavit Security Onion, aby odesílal Traps na správnou IP adresu a port.

2. Zabbix Agent:

Zabbix Agent je software, který je nainstalován na sledovaném zařízení a komunikuje se Zabbix serverem. Zabbix Agent se instaluje a konfiguruje tak, aby ze Security Onion odesílal data do Zabbixu. Poté se vytvoří uživatelské skripty nebo se použije předdefinované moduly pro sběr událostí a metrik ze Security Onion pro odesílání těchto dat do Zabbixu.

3. E-mailová integrace:

Security Onion může posílat e-mailová upozornění na základě detekovaných událostí. V Zabbixu je možné nakonfigurovat e-mailovou integraci tak, aby přijímal a zpracovával e-maily ze Security Onion. Tímto způsobem lze přenést informace o detekovaných událostech a upozorněních mezi oběma systémy.

4. API integrace:

Zabbix poskytuje API, které umožňuje přístup k funkcím monitorovacího software. Vytvoří se skript nebo aplikace, která bude používat Security Onion API pro získání informací o událostech a následně je odesílat do Zabbixu prostřednictvím Zabbix API. Tato metoda vyžaduje znalost programování a API obou systémů, ale umožňuje vytvořit velmi flexibilní a užitečnou integraci.

Z pohledu systému Zabbix a monitoringu je nejvhodnější použití zabbix agenta a dále zabbix_senderu, prostřednictvím kterého je možné odesílat jakékoli informace přes vytvořené scripty v programovacím jazyce python.

Logovací soubory a umístění událostí systému Security Onion

Security Onion ukládá logy v několika adresářích a souborech, které zaznamenávají různé aspekty svých komponent a detekčních nástrojů. Logy mohou být ve formátu plaintext nebo JSON. Následující jsou některé z hlavních adresářů a souborů, které obsahují logy v Security Onion:

1. /var/log:

Tento adresář obsahuje většinu systémových logů. Logy zde zaznamenávají různé události, chyby a stav komponent Security Onion. Například:

- /var/log/syslog: Obsahuje zprávy o systémových událostech a chybách.
- /var/log/auth.log: Zaznamenává události související s autentizací a autorizací.
- /var/log/suricata/: Tento adresář obsahuje logy od Suricata, což je síťový detekční nástroj IDS/IPS. Hlavní logy zahrnují:
    - suricata.log: Zaznamenává chyby a události týkající se Suricata.
    - eve.json: Ukládá detailní informace o detekovaných událostech ve formátu JSON.
- /var/log/zeek/: Tento adresář obsahuje logy od Zeek (dříve známý jako Bro), což je síťový detekční nástroj. Zeek logy jsou ve formátu TSV (tab-separated values) nebo JSON. Logy obsahují informace o síťových spojeních, DNS dotazech, HTTP požadavcích a dalších síťových událostech. Logy jsou rozděleny do různých souborů podle typu události, jako jsou conn.log, dns.log, http.log atd.

2. /opt/so/log/:

Adresář /opt/so/log/ obsahuje logy související s komponentami Security Onion. Zde se nacházejí logy pro různé služby, jako jsou:

- /opt/so/log/strelka/: Obsahuje logy od Strelka, což je nástroj pro analýzu souborů.
- /opt/so/log/elasticsearch/: Tento adresář obsahuje logy pro Elasticsearch, což je vyhledávací a analytický nástroj pro logy.
- /opt/so/log/kibana/: Zde se nachází logy pro Kibana, což je webový nástroj pro vizualizaci a analýzu dat uložených v Elasticsearch.

Tyto adresáře a soubory obsahují logy, které zaznamenávají činnost, chyby a detekované události v rámci Security Onion

Vybrané události, které je vhodné sledovat

Security Onion dokáže detekovat široké spektrum síťových a bezpečnostních událostí. Zde jsou tři nejdůležitější události, kterým by se měla věnovat pozornost:

1. Podezřelá síťová aktivita (vysoký počet připojení nebo přenos dat):

Tato situace může naznačovat, že dochází k útoku typu DDoS nebo pokusu o exfiltraci dat. Tuto událost lze identifikovat v logu Zeek conn.log, který je uložen v /var/log/zeek/. V tomto logu se hledají záznamy s vysokým počtem připojení nebo velkým objemem přenesených dat.

Identifikace: Zeek conn.log - vysoký počet připojení nebo přenos dat

2. Detekce malware:

Pokud Security Onion zaznamená podezřelý soubor, který může obsahovat malware, je důležité tuto událost okamžitě prověřit. Strelka je nástroj pro analýzu souborů integrovaný do Security Onion, který dokáže detekovat malware a další škodlivý obsah. Výsledky analýzy Strelky jsou uloženy v /opt/so/log/strelka/ ve formátu JSON.

Identifikace: Strelka JSON log - detekce malware nebo podezřelého souboru

3. Detekce podezřelé síťové komunikace:

Suricata je nástroj IDS/IPS, který dokáže detekovat podezřelou síťovou komunikaci, například pokusy o útok, škodlivé aktivity nebo komunikaci s C&C (Command and Control) servery. Suricata ukládá detailní informace o detekovaných událostech ve formátu JSON v

souboru eve.json, který se nachází v /var/log/suricata/. Události detekované Suricatou jsou identifikovány podle jejich SID (Signature ID).

Identifikace: Suricata eve.json - detekce podezřelé síťové komunikace (SID)

Důležité události zaznamenané Security Onion by měly být pravidelně kontrolovány a analyzovány, aby bylo možné rychle identifikovat a řešit bezpečnostní incidenty a hrozby.

Zabbix_sender

Instalace systému zabbix_sender je součástí zabbix_agenta a není nutné provádět samostatnou instalaci. Postup je stejný, jako v předcházejících integracích, a proto není nutné tento postup detailně uvádět.

Vyhodnocení důležitých událostí

Byly uvedeny tři vybrané události, které je vhodné sledovat formou zaslání vzniklé události do systému Zabbix. Pro vyhodnocení vzniklých událostí bude použit vlastní script python, který pro svůj běh potřebuje python 3.

- *import json*
- *import subprocess*
- *import os*
- *from datetime import datetime*

Cesta k souboru eve.json

- *eve_json_path = '/var/log/suricata/eve.json'*

zabbix_sender a konfigurační soubor Zabbix agenta

- *zabbix_sender = '/usr/bin/zabbix_sender'*
- *zabbix_agent_config = '/etc/zabbix/zabbix_agentd.conf'*

Klíčová slova pro detekci podezřelé síťové komunikace

suspicious_keywords = ['trojan', 'exploit', 'c&c']

def send_to_zabbix(item_key, value):

- *command = [zabbix_sender, '-c', zabbix_agent_config, '-k', item_key, '-o', value]*
- *subprocess.run(command, stdout=subprocess.DEVNULL)*

with open(eve_json_path, 'r') as file:

for line in file:

try:

- *event = json.loads(line)*
- *if event['event_type'] == 'alert':*
- *signature = event['alert']['signature'].lower()*

if any(keyword in signature for keyword in suspicious_keywords):

- *timestamp = datetime.fromtimestamp(event['timestamp']).strftime('%Y-%m-%d %H:%M:%S')*
- *sid = event['alert']['signature_id']*
- *src_ip = event['src_ip']*
- *dst_ip = event['dest_ip']*
- *message = f"Event: {signature}, SID: {sid}, Timestamp: {timestamp}, Source IP: {src_ip}, Destination IP: {dst_ip}"*
- *print(f"Sending suspicious event to Zabbix: {message}")*
- *send_to_zabbix('suspicious_event', message)*
- *except json.JSONDecodeError:*
- *print("Error decoding JSON line")*

Python skript slouží k monitorování a zasílání upozornění na podezřelou síťovou komunikaci prostřednictvím Zabbixu. Skript provádí následující akce:

1. Importuje potřebné knihovny.
2. Nastavuje cestu k souboru eve.json, který obsahuje záznamy o síťových událostech.
3. Nastavuje cestu k nástroji zabbix_sender a konfiguračnímu souboru Zabbix agenta.
4. Definuje klíčová slova pro detekci podezřelé síťové komunikace, jako jsou 'trojan', 'exploit' a 'c&c'.
5. Definuje funkci send_to_zabbix, která pomocí zabbix_sender zasílá data do Zabbixu.
6. Otevírá a čte soubor eve.json po řádcích.
7. Pro každý řádek souboru se pokouší načíst JSON objekt a zkontrolovat, zda se jedná o událost typu 'alert'.

8. Pokud je událost typu 'alert', zkontroluje, zda obsahuje některé z klíčových slov podezřelé síťové komunikace.
9. Pokud je událost podezřelá, načte informace o události, jako je časová značka, ID signatury, zdrojová a cílová IP adresa, a vytvoří zprávu o události.
10. Zobrazí zprávu o podezřelé události a pošle ji do Zabbixu pomocí funkce send_to_zabbix.

V případě chyby při dekódování JSON řádku skript vypíše chybovou zprávu "Error decoding JSON line".

Nastavení systému Zabbix pro příjem událostí ze systému Security Onion

Pro nastavení Zabbixu pro příjem událostí tohoto typu ze systému Security Onion je třeba provést několik kroků. Nejprve je potřeba nastavit Zabbix server a Zabbix agenta na Security Onion stroji. Následně je třeba vytvořit hosta, položku (item) a spouštěč (trigger) v Zabbixu. Část nastavení systému Zabbix pro příjem událostí byla detailně popsána dříve v této práci a liší se pouze v zobrazovaném oznámení na dashboardu Zabbixu.

Vyhodnocení událostí v systému Zabbix

Pokud v systému SecurityOnion dojde k události, která je analyzována scriptem, po jejím zpracování skriptem, který běžně spustí úlohu v plánovači, jako je například cron v systému Wazuh, bude tato událost odeslána do systému Zabbix. Poté se zobrazí na dashboardu systému Zabbix s vážností High, tedy, že je nutná tuto událost řešit bezodkladně. Kromě zobrazení na dashboardu lze pro různé události generovat různá oznámení, např. přes e-mail nebo aplikaci Telegram. Události je možné zobrazovat také v mobilním telefonu ve speciální aplikaci.

Obrázek 28 - Zabbix - vyhodnocení události Security Onion

Zdroj: Vlastní zpracování

Závěrečná shrnutí k části propojení systému SecuriyOnion a systému Zabbix

Integrace systému Security Onion se systémem Zabbix přináší řadu výhod, zejména možnost okamžité reakce na vzniklé důležité události bez nutnosti být přihlášený v systému Security Onion. Security Onion je bezpečnostní nástroj, který se zaměřuje na detekci a prevenci hrozeb a lze propojit se Zabbixem pomocí SNMP Trap, Zabbix Agent, e-mailové integrace nebo API integrace. Dále se v textu diskutuje o logovacích souborech a umístění událostí v systému Security Onion. Adresáře /var/log a /opt/so/log/ obsahují logy související s komponentami Security Onion. Dále se uvádí tři vybrané události, které by se měly sledovat, a to podezřelou síťovou aktivitu, detekci malware a podezřelou síťovou komunikaci.

Byl použit skript v Pythonu, který slouží k monitorování a zasílání upozornění na podezřelou síťovou komunikaci prostřednictvím Zabbixu. Skript provádí několik akcí, včetně definice klíčových slov pro detekci podezřelé síťové komunikace a zasílání dat do Zabbixu.

V závěru textu jsou uvedeny kroky, které je třeba provést pro nastavení systému Zabbix pro příjem událostí ze systému Security Onion. Krok za krokem jsou popsány úkony, které je nutné vykonat v rámci nastavení Zabbix serveru a Zabbix agenta na Security Onion stroji.

Vyhodnocení bezpečnostních hrozeb je kritické pro ochranu informačních systémů. Integrace Security Onion se Zabbixem umožňuje rychlou identifikaci a řešení bezpečnostních incidentů. Využitím skriptu v Pythonu lze monitorovat a zasílat upozornění na podezřelou síťovou komunikaci prostřednictvím Zabbixu. Použití logovacích souborů a vybraných událostí umožňuje rychlou identifikaci hrozeb a zlepšení bezpečnosti informačních systémů.

4.2.5 Propojení Zabbix a OpenVAS

V třetí kapitole bylo řečeno že komplexní nástroj pro skenování zranitelností OpenVAS (Open Vulnerability Assessment System) pomáhá identifikovat a řešit bezpečnostní slabiny v síti. V současnosti je OpenVAS přejmenován na Greenbone Vulnerability Management (GVM) a je k dispozici ve dvou verzích: komunitní edice (GVM-CE) a profesionální edice. Tento pro zkoumání problematiky praktické časti využijeme GVM-CE, která pro rozsah práce bude postačovat.

Instalace a konfigurace OpenVAS

Některé Linuxové distribuce, jako je Kali Linux, Debian nebo Ubuntu, poskytují OpenVAS/GVM ve svých softwarových repozitářích. Dále lze OpenVAS/GVM instalovat ze zdrojvého kódu nebo dockeru. Hardwarové požadavky závisí na velikosti prostředí, do kterého je OpenVAS/GVM nasazován. Pokud jde o střední až velké sítě, pokročilé skenování a produkční prostředí, doporučují se následující hardwarové požadavky, které je možno vyčíst z tabulky 3.

Tabulka 3 - OpenVAS – doporučené požadavky pro instalaci

CPU	4 nebo více jader
RAM	8GB nebo více
Uložiště	60GB nebo více

Zdroj: GREENBON, 2023

Instalace OpenVAS/GVM bude provedena na Ubuntu 22.04 stejně jako v předchozích instalacích nástrojů. Instalaci lze provést prostřednictvím příkazů, které postupně nainstalují finální produkt. Pro ušetření času vývojáři OpenVAS/GVM vytvořili script, který odvede veškerou práci:

- *curl -f -O https://greenbone.github.io/docs/latest/_static/setup-and-start-greenbone-community-edition.sh && chmod u+x setup-and-start-greenbone-community-edition.sh*

Pro spuštění skriptu je třeba spustit následující příkaz:

- *./setup-and-start-greenbone-community-edition.sh 22.4*

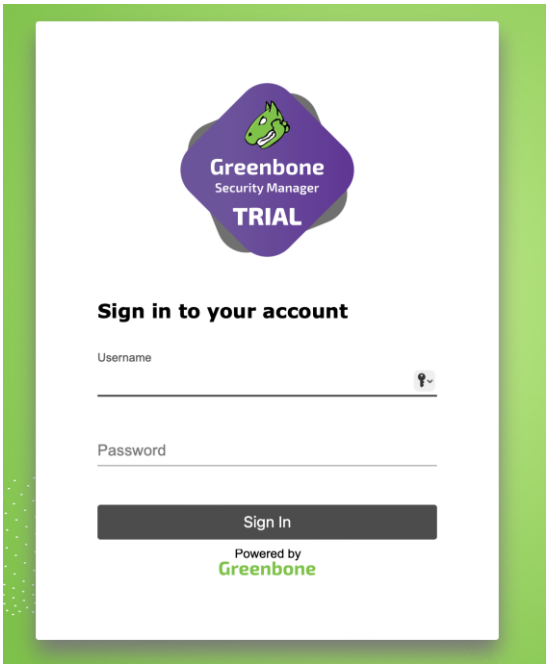
Nyní je instalace hotová a lze zpřístupnit OpenVAS/GVM přes webové rozhraní. Před prvním spuštěním lze změnit automaticky vygenerované heslo tímto příkazem:

- *docker-compose -f $DOWNLOAD_DIR/docker-compose.yml -p greenbone-community-edition \ exec -u gvmd gvmd gvmd --user=admin --new-password=<password>*

Po spuštění služeb a načtení všech vstupních dat lze v prohlížeči otevřít webové rozhraní Greenbone Security Assistant – GSA(Greenbone, Greenbone community documentation, 2023, upraveno a přeloženo autorem).

Přihlášení do webového rozhraní ukazuje obrázek 28.

Obrázek 29 - OpenVAS – přihlášení do webového rozhraní



Zdroj: Vlastní zpracování

Integrace systému OpenVAS se Zabbixem

Výrobce systému OpenVAS nenabízí přímou podporu spolupráce se systémem Zabbix. Pro zajištění bezpečnosti a hledání zranitelností v IT infrastruktuře je vhodné analyzovat logy systému OpenVAS, stanovit určitou úroveň zranitelnosti, která má být ihned řešena a tuto informace předat do systému Zabbix.

Pro předpokládané propojení systému OpenVAS, jako nástroje pro skenování zranitelností se systémem Zabbix jako nástroje pro sledování a správu infrastruktury existuje několik možných způsobů, jak zprávy zasílat:

1. Použití Zabbixových gRPC či REST API - Zabbix poskytuje API, které umožňuje jiným aplikacím zasílat data do Zabbixu. Pomocí tohoto API může OpenVAS zasílat zprávy o zranitelnostech do Zabbixu.
2. Použití externího skriptu - OpenVAS umožňuje vytvářet skripty, které se spouštějí při určitých událostech, jako například nalezení nové zranitelnosti. Pomocí externího skriptu může OpenVAS zasílat zprávy o zranitelnostech do Zabbixu.

   Použití Zabbixového skriptu - Zabbix má také skripty, které umožňují získávat data z jiných aplikací. Pomocí Zabbixového skriptu může OpenVAS zasílat zprávy o zranitelnostech do Zabbixu.

3. Použití Zabbixového agenta - Zabbixový agent je malý program, který běží na monitorovaných strojích a poskytuje Zabbixu informace o systému. OpenVAS může být nakonfigurován tak, aby zasílal zprávy o zranitelnostech přímo na monitorovaný stroj, kde je nainstalován Zabbixový agent. Poté může Zabbixový agent zaslat tyto zprávy do Zabbixu.

   S Ohledem na náročnost propojení obou systémů je vhodné se přiklonit k analýze logů systému OpenVAS, ze kterých se budou přenášet informace o zranitelnostech s CVSS vyšším než 8.

Záznamy o skenování a umístění událostí v systému OpenVAS

Výsledky skenování jsou obvykle uloženy ve formátu XML, který je strukturován do hierarchie značek a atributů. XML (Extensible Markup Language) je univerzální značkovací jazyk, který umožňuje definovat vlastní strukturu dat.

Umístění pro záznamy událostí o skenování je zvoleno:

- */opt/gvm/reporty*

Soubor obsahu detekované zranitelnosti ve formátu XML. Pro analýzu logu se vyhodnocují CVSS, které mají hodnotu rovnu 8. Takto lze vyhodnocovat události různé úrovni nebo také různého rozpětí, např. rovno nebo vyšší 8.

Instalace zabbix_sender

Zabbix sender není potřeba instalovat samostatně, protože je součástí balíčku zabbix_agnet. Popis instalace zabbix_agenta, který obsahuje zabbix_sender je již detailně popsán v jiné části této práce.

Vyhodnocení CVSS rovno 8

Pro vyhodnocování skenů byl vytvořen script v jazyce python, který bude analyzovat XML soubory s výsledky skenování OpenVAS. Script bude filtrovat výsledky podle zadaných kritérií, kdy bylo zvoleno CVSS skóre vyšší než 8. Pro každý nalezený výsledek by skript měl extrahovat informace o CVSS, PC a IP adrese.

- *import os*
- *import xml.etree.ElementTree as ET*
- *from subprocess import call*

- *OPENVAS_REPORTS_DIR = "/opet/gvm/reporty"*
- *ZABBIX_SENDER = "/usr/bin/zabbix_sender"*
- *ZABBIX_SERVER = "192.168.110.84"*
- *ZABBIX_HOST = "openVas_zabbix"*
- *CVSS_THRESHOLD = 8*
- *def parse_openvas_report(report_file):*
- *vulnerabilities = []*
- *tree = ET.parse(report_file)*
- *root = tree.getroot()*
- *for result in root.findall('.//result'):*
- *cvss = float(result.find('nvt/cvss_base').text)*
- *if cvss >= CVSS_THRESHOLD:*
- *ip_address = result.find('host').text*
- *port = result.find('port').text*
- *vulnerabilities.append((cvss, ip_address, port))*
- *return vulnerabilities*
- *def send_to_zabbix(vulnerabilities):*
- *for vulnerability in vulnerabilities:*
- *cvss, ip_address, port = vulnerability*
- *cmd = [*
- *ZABBIX_SENDER,*
- *"-z", ZABBIX_SERVER,*
- *"-s", ZABBIX_HOST,*
- *"-k", "openvas.cvss",*
- *"-o", str(cvss)*
- *]*
- *call(cmd)*
- *cmd = [*
- *ZABBIX_SENDER,*
- *"-z", ZABBIX_SERVER,*
- *"-s", ZABBIX_HOST,*
- *"-k", "openvas.ip",*

- *"-o", ip_address*
- *]*
- *call(cmd)*
- *cmd = [*
- *ZABBIX_SENDER,*
- *"-z", ZABBIX_SERVER,*
- *"-s", ZABBIX_HOST,*
- *"-k", "openvas.port",*
- *"-o", port*
- *]*
- *call(cmd)*
- *if __name__ == "__main__":*
- *for report_file in os.listdir(OPENVAS_REPORTS_DIR):*
- *if report_file.endswith(".xml"):*
- *report_path = os.path.join(OPENVAS_REPORTS_DIR, report_file)*
- *vulnerabilities = parse_openvas_report(report_path)*
- *send_to_zabbix(vulnerabilities)*

Skript slouží k automatickému odesílání zranitelností z reportů generovaných nástrojem OpenVAS do monitorovacího nástroje Zabbix. Skript předpokládá, že reporty jsou uloženy v adresáři OPENVAS_REPORTS_DIR a mají koncovku ".xml".

Funkce "parse_openvas_report" analyzuje každý report a prochází seznam zranitelností, které mají CVSS skóre vyšší nebo rovno hodnotě CVSS_THRESHOLD (v případě tohoto skriptu nastaveno na 8). Pro každou nalezenou zranitelnost jsou uloženy IP adresa a port, na kterém byla zranitelnost nalezena, spolu s hodnotou CVSS.

Funkce "send_to_zabbix" odesílá informace o nalezených zranitelnostech do Zabbixu pomocí nástroje zabbix_sender. Pro každou zranitelnost jsou vytvořeny tři zprávy. Jedna pro CVSS skóre, druhá pro IP adresu a třetí pro port. Tyto zprávy jsou odeslány na Zabbix server s parametry ZABBIX_SERVER a ZABBIX_HOST, které jsou definovány na začátku skriptu.

Hlavní funkce skriptu (na konci s podmínkou if name == "main") pak iteruje přes všechny XML soubory v adresáři s reporty, zavolá funkci "parse_openvas_report" pro každý

z nich a výsledky této funkce předá funkci "send_to_zabbix" pro odeslání informací do Zabbixu.

Nastavení systému Zabbix a vyhodnocení událostí

Postupy nastavení systému Zabbix jsou podobné, jako postupy, které byly použity v propojení systému Wazuh. Detailní popis nastavení systému Zabbix je již nadbytečný, protože v této části bude uveden stručný postup.

Vytvoření šablony v Zabbixu pro monitorování OpenVAS událostí:

Po přihlášení do webového rozhraní Zabbixu se vytvoří host pro OpenVAS. Přidá se položka (Items) do hosta, která budou monitorovat informace o CVSS, PC a IP adrese. Přidají se triggery pro upozornění na události s vyšším CVSS skóre než 8. Naplánování pravidelného spouštění skriptu pro zpracování logů prostřednictvím CRONu nebo jiném plánovači úloh na serveru OpenVAS, aby docházelo k pravidelnému spouštění skriptu pro zpracování logů.

Závěrečné shrnutí k části propojení systému OpenVAS a systému Zabbix

Propojení systému OpenVAS a Zabbixu je užitečným nástrojem pro sledování zranitelností IT infrastruktury a poskytuje důležité informace o potenciálních bezpečnostních hrozbách. Přestože výrobce OpenVAS nenabízí přímou podporu pro spolupráci se Zabbixem, existuje několik možností, jak propojit tyto dva nástroje.

První možností je použití Zabbixových gRPC nebo REST API. Druhou možností je použití externího skriptu, který se spouští při určitých událostech. Třetí možností je použití Zabbixového skriptu, který umožňuje získávat data z jiných aplikací. Čtvrtou a poslední možností je použití Zabbixového agenta. Propojení obou systémů může být náročné, a proto je vhodné se přiklonit k analýze logů systému OpenVAS, ze kterých se budou přenášet informace o zranitelnostech s CVSS vyšším než 8.

Pro vyhodnocení skenů byl vytvořen script v jazyce Python, který analyzuje XML soubory s výsledky skenování OpenVAS a filtrována zranitelnosti podle kritérií stanovených na základě CVSS skóre. Poté informace o zranitelnostech jsou odesílány do Zabbixu pomocí nástroje zabbix_sender. Je důležité určit umístění pro záznamy událostí o skenování, doporučeno je používat specifický adresář, například /opt/gvm/reporty.

V nastavení systému Zabbix je důležité vytvořit šablonu pro monitorování OpenVAS událostí. Poté jsou přidány triggery pro upozornění na události s vyšším CVSS skóre než 8. Naplánování pravidelného spouštění skriptu pro zpracování logů umožní pravidelné spouštění skriptu pro zpracování logů.

Celkově lze tedy konstatovat, že propojení systému OpenVAS se Zabbixem je velmi užitečné pro zajištění bezpečnosti a hledání zranitelností v IT infrastruktuře. Při propojování těchto systémů je nutné mít na paměti několik faktorů, jako je volba vhodného způsobu zasílání zpráv mezi systémy, správné nastavení systému Zabbix a vytvoření šablony pro monitorování OpenVAS událostí.

5 Zhodnocení výsledků

5.1 Zhodnocení dotazníkového průzkumu

Výsledek grafu 1 může naznačovat nedostatečnou informovanost nebo nedostatečné investice do kybernetické bezpečnosti v organizaci. Je důležité si uvědomit, že kybernetické hrozby jsou reálné a mohou mít vážné následky pro organizaci, včetně finančních ztrát, úniku důvěrných informací a poškození pověsti firmy. Z tohoto důvodu je důležité, aby firmy věnovaly pozornost a investice do kybernetické bezpečnosti a zajistily tak, že jsou chráněny před potenciálními hrozbami a zabezpečeny citlivé informace.

Výsledky získané z grafu 2 mohou naznačovat, že firmy si neuvědomují důležitost kybernetická bezpečnosti a nejsou ochotny investovat do ní dostatečné prostředky, ať už v podobě financí, času nebo odborných znalostí. Tento nedostatek investic a pozornosti ke kybernetická bezpečnosti může mít negativní dopad na bezpečnost a stabilitu organizace a může ji vystavit různým hrozbám, včetně úniku citlivých dat, vymáhání výkupného, poškození pověsti a dalších. Je důležité si uvědomit, že kybernetická bezpečnost by měla být prioritou pro každou firmu bez ohledu na její velikost a typ činnosti. Firmy by měly věnovat dostatečné zdroje a pozornost na zlepšení své kybernetická bezpečnosti a ochranu svých aktiv.

Na výsledcích grafu 3 si je důležité uvědomit, že zaměstnanci jsou často první linií obrany proti kybernetickým hrozbám a jejich neznalost nebo nedostatek pozornosti může znamenat vážné riziko pro organizaci. Pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti může pomoci zvýšit povědomí o rizicích a poskytnout zaměstnancům nezbytné znalosti a nástroje k ochraně organizace před kybernetickými hrozbami.

Firmy by měly věnovat dostatečné zdroje a pozornost na vzdělávání svých zaměstnanců v oblasti kybernetické bezpečnosti a zajistit tak, že jsou schopni identifikovat a reagovat na různé hrozby a chránit citlivé informace. To by mohlo vést ke zlepšení celkové bezpečnostní situaci a snížení rizika kybernetických útoků v organizaci.

Výsledek grafu 4 může naznačovat, že firmy si neuvědomují důležitost mít zavedený incident response plán, který by jim pomohl rychle a efektivně reagovat na bezpečnostní incidenty. Incident response plán by měl být součástí celkové strategie kybernetické bezpečnosti a měl by obsahovat postupy, které by měly být následovány v případě incidentů, jako jsou útoky, vymáhání výkupného, úniky dat atd. Zavedením incident response plánu by se firmy mohly lépe připravit na různé hrozby a minimalizovat dopad bezpečnostních incidentů na své obchodní činnosti.

Graf 5 může naznačovat nedostatečnou informovanost nebo nedostatečné investice do auditů bezpečnostních opatření a postupů. Je důležité si uvědomit, že pravidelné audity jsou důležitou součástí správy kybernetické bezpečnosti a pomáhají organizacím identifikovat slabá místa v jejich bezpečnostních opatřeních a postupech. Pravidelné audity mohou také pomoci organizacím zajistit, že jsou v souladu s relevantními předpisy a standardy, jako jsou například GDPR.

Výsledek grafu 6 může naznačovat nedostatečnou informovanost nebo nedostatečné investice do pokročilých systémů detekce hrozeb a průniků do sítě. Je důležité si uvědomit, že tradiční bezpečnostní opatření, jako jsou například antivirové programy, firewall a IDS/IPS, již nejsou dostačující k ochraně proti moderním a sofistikovaným hrozbám. Pokročilé systémy detekce hrozeb a průniků do sítě mohou pomoci organizacím identifikovat různé druhy hrozeb, jako jsou například malwarové útoky, phishing a útoky s využitím nulových dnů.

Graf 7 může vypovídat o nedostatečné informovanosti nebo nedostatečné investice do interního nebo externího týmu pro řešení kybernetických bezpečnostních hrozeb. Je důležité si uvědomit, že kybernetické hrozby se neustále vyvíjejí a organizace musí být schopny efektivně reagovat na tyto hrozby. Vnitřní nebo externí tým pro řešení kybernetických bezpečnostních hrozeb může pomoci organizacím identifikovat a reagovat na bezpečnostní incidenty, minimalizovat dopad těchto incidentů a chránit citlivé informace.

5.2 Zhodnocení Implementace open source nástrojů

V rámci práce bylo zjištěno, že neexistuje open source nástroj, který by plně pokrýval zkoumanou problematiku, tedy monitoring sítí se zaměřením na kybernetickou bezpečnost. Proto byly zkoumány další open source nástroje a možnosti jejich propojení. Samotné nástroje nabízejí více možností propojení a reportování mimo své vlastní prostředí. Důležitou vlastností jednoho ze zkoumaných systémů konkrétně systému Zabbix bylo, aby uměl koncentrovat všechny důležité nebo vybrané události do jednoho místa s jednou centrální konzolí tzv. dashboardem a s možností reportování dalšími způsoby např. na mobilní zařízení a dalšími cestami.

Jako centrální monitorovací software byl zvolen systém Zabbix, který nabízí velmi dobře propracované funkce monitorování prakticky jakéhokoliv zařízení. V Zabbixu je možné vytvořit hosty a do těchto hostů do položek s názvem item ukládat jakékoli informace, tyto informace hodnotit a provést s nimi nějakou akci, např. vybranou událost zobrazit v dashboardu tzv. centrální konzoli pro dohled.

Pro propojení s ostatními systémy, které byly vybrány a zjišťují takové funkce, které neposkytuje systém Zabbix byly vybrány systémy Wazuh, systém Security Onion a systém OpenVAS. Každý ze systémů provádí trochu jiné činnosti související s kybernetickou bezpečností. Každý systém byl analyzován a bylo vyhodnoceno, že je nutné naprogramovat scripty v programovacím jazyce python, které budou analyzovat logy a události v nich uložené a podle zadaných kritérií vytvoří a předají zprávu s informacemi do systému zabbix_agent, který požadované informace předá do systému Zabbix, který je zpracuje a případně zobrazí v centrální konzoli. Kladl se také důraz na jednotnost, tedy, aby pokud možnost každý systém používat podobné techniky analýzy a zasílání informací do Zabbixu.

Všechny výše uvedené záměry se podařilo realizovat a v laboratorním prostředí všechny činnosti, aktivity a vyhodnocení pracovaly bez problémů a plně splnily očekávání daná cílem práce i když nebyl nalezen jeden nástroj pro komplexní obsloužení monitoringu sítí se zaměřením na kybernetickou bezpečnost.

Bylo dosaženo výsledku, který přináší vyšší míru flexibility, než kdyby se použil pouze jeden produkt, protože bylo dosaženo propojení, které půjde realizovat i u dalších open source nástrojů za použití hlavního nástroje, kterým je systém Zabbix.

5.3 Doporučení

Lze navrhnout následující postup jako doporučení pro optimální open source nástroje pro zajištění kybernetické bezpečnosti a monitoringu v konkrétním prostředí společnosti či instituce:

1. Implementace a konfigurace Zabbixu jako centrálního systému pro monitorování a sběr událostí z ostatních bezpečnostních nástrojů.
2. Implementace a konfigurace Wazuhu pro prevenci, detekci a reakci na kybernetické hrozby a útoky, zejména v oblasti ochrany koncových bodů a analýzy bezpečnostních událostí. Propojení tohoto nástroje se systémem Zabbix.
3. Implementace a konfigurace Security Onion pro analýzu síťového provozu, detekci pokročilých hrozeb a zajištění proaktivní obrany proti kybernetickým útokům. Propojení tohoto nástroje se systémem Zabbix.
4. Implementace a konfigurace OpenVAS pro pravidelné skenování zranitelností v IT infrastruktuře a zajištění, že všechny systémy a zařízení jsou aktualizovány a zabezpečeny. Propojení tohoto nástroje se systémem Zabbix.

Tato kombinace open source nástrojů, které jsou prostřednictvím scriptů v programovacích jazyce pythonu propojeny se systémem Zabbix umožňuje efektivní ochranu počítačové sítě vybrané firmy nebo instituce z pohledu kybernetické bezpečnosti. Nicméně, je důležité zdůraznit, že úspěšná implementace a správa těchto nástrojů vyžaduje odborné znalosti a zkušenosti v oblasti kybernetické bezpečnosti. Kromě toho je nezbytné pravidelně aktualizovat a udržovat tyto nástroje, aby byly schopny efektivně čelit neustále se měnícím hrozbám a zranitelnostem.

6 Závěr

V diplomové práci byly analyzovány a hodnoceny vybrané open source nástroje pro zajištění kybernetické bezpečnosti a ochrany počítačových sítí vybrané společnosti či instituce. Na základě teoretické části práce, dotazníkového šetření a praktického zkoumání open source nástrojů bylo zjištěno, že existuje mnoho možností pro zlepšení kybernetické bezpečnosti. Nicméně, bylo také prokázáno, že žádný jednotlivý open source nástroj není komplexním řešením, které by plně pokrývalo všechny aspekty kybernetické bezpečnosti a monitoringu zároveň.

Přestože jednotlivé nástroje, jako jsou Zabbix, Wazuh, Security Onion, Greenbone OpenVAS a Nmap, jsou výkonné a užitečné ve svých oblastech, bylo nutné navrhnout propojení těchto nástrojů, aby bylo dosaženo maximální efektivity a kompatibility s existujícími systémy a procesy. Integrace těchto nástrojů do jednoho systému, který centralizuje události a zobrazuje je na jednom dashboardu, představuje nejlepší řešení pro kybernetickou bezpečnost a monitoring počítačových sítí zahrnující okamžitou reakci na vzniklé události podle jejich závažnosti.

Výsledkem práce je tedy doporučení optimálního řešení založeného na open source nástrojích pro zajištění kybernetické bezpečnosti a monitoringu v konkrétním prostředí společnosti či instituce. Toto doporučení zahrnuje návrh implementace, vytvoření scriptů v jazyce python, konfigurace a správy vybraných nástrojů, aby bylo dosaženo maximální efektivity a kompatibility s existujícími systémy a procesy.

Na základě výsledků dotazníkového šetření je zřejmé, že existuje mnoho oblastí, kde je třeba zlepšit kybernetickou bezpečnost a povědomí o kybernetických hrozbách. Je třeba důkladnější školení zaměstnanců, implementace bezpečnostních politik, pravidelné testování zranitelností IT infrastruktury a zavedení systémů pro sledování a omezení nežádoucího síťového provozu.

V budoucnu by bylo vhodné provést další průzkumy a analýzy v oblasti kybernetické bezpečnosti a monitoringu, aby bylo možné sledovat vývoj hrozeb a útoků a kontinuálně zlepšovat ochranu organizací s Zabbixem, Security Onion s Zabbixem a OpenVAS s Zabbixem.

V rámci testování byly simulovány různé kybernetické hrozby a útoky na zabezpečenou síť, která byla chráněna pomocí implementovaných open source nástrojů.

Výsledky testování ukázaly, že kombinace Zabbixu, Wazuhu, Security Onion a OpenVAS poskytuje efektivní ochranu před širokou škálou kybernetických hrozeb a umožňuje rychlou detekci a reakci na potenciálně škodlivé události v počítačové síti.

Na základě provedeného hodnocení a laboratorního testování lze konstatovat, že vhodné open source nástroje pro zajištění kybernetické bezpečnosti a ochrany počítačových sítí vybrané společnosti či instituce existují. Jedná se však o kombinaci Zabbixu, Wazuhu, Security Onion a OpenVAS, která nabízí komplexní řešení pro monitorování a zabezpečení počítačových sítí s vysokou úrovní efektivity, uživatelské přívětivosti, škálovatelnosti a integrace s existujícími technologiemi a procesy.

7 Seznam použitých zdrojů

[1] BHATTACHARYYA, Dhruba Kumar a Jugal Kumar KALITA. DDoS Attacks Evolution, Detection, Prevention, Reaction, and Tolerance. 1. 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742: CRC Press, 2016. ISBN 978-1-4987-2965-9.

[2] Bitlocker. *Microsoft* [online]. United States: © [cit. 2021-12-09]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

[3] ESET - Co je ransomware. *ESET - Essential Security against Evolving Threats* [online]. online: ©, 2022 [cit. 2023-01-30]. Dostupné z: https://www.eset.com/cz/ransomware/

[4] GREENBONE BACKGROUND ARCHITECTURE. *GREENBONE GITHUB DOCUMENTATION* [online]. online: ©, 2023 [cit. 2023-03-28]. Dostupné z: https://greenbone.github.io/docs/latest/background.html

[5] Greenbone. Greenbone [online]. online: ©, 2023 [cit. 2023-03-19]. Dostupné z: https://greenbone.github.io/docs/latest/22.4/container/index.html

[6] Group Policy Objects. *Microfosoft* [online]. United States: © Microsoft [cit. 2021-12-08]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects

[7] GRUBB, Sam. *HOW CYBERSECURITY REALLY WORKS*. 1. 245 8th Street, San Francisco, CA 94103: No Starch Press, 2021. ISBN 978-1-7185-0128-7.

[8] Hardware Requirements. *GREENBONE GITHUB DOCUMENTATION* [online]. online: ©, 2023 [cit. 2023-03-28]. Dostupné z: https://greenbone.github.io/docs/latest/22.4/source-build/hardware.html

[9] JENKINSON, Andrew. Ransomware and Cybercrime. 1. 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487–2742: CRC Press, 2022. ISBN 978-1-032-23549-3.

[10] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

[11] KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. *CYBERSECURITY*. Praha: CZ.NIC, z. s. p. o, 2019. ISBN 978-80-88168-34-8.

[12] KOLOUCH, Jan. *CYBERCRIME*. Praha: CZ.NIC, z. s. p. o, 2016. ISBN ISBN 978-80-88168-18-8.

[13] KOSTOPOULOS, George. *Cyberspace and Cybersecurity*. 2nd edition. Boca Raton, Florida: CRC press, 2017. ISBN 9781315116488.3

[14] LIEFTING, Nathan a Brian van BAEKEL. Zabbix 6 IT Infrastructure Monitoring Cookbook Second Edition. 2. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2022. ISBN 978-1-80324-691-8.

[15] *Mistrostvi - počítačové sítě*. Dotisk 1. vydání. Brno: Computer Press, a.s, 2011. ISBN 978-80-251-3363-7.

[16] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 [online]. online: ©, 2016 [cit. 2023-02-01]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[17] *Networking explaind*. 2nd edition. United States of America: Digital Press, 2002. ISBN 978-1-55558-252-4.

[18] NMAP - introduction. *NMAP - Network Mapper* [online]. California: © [cit. 2021-12-10]. Dostupné z: https://nmap.org/

[19] OLUPS, Rihards, Andrea Dalle VACCHE a Patrik UYTTERHOEVEN. Zabbix: Enterprise Networko Monitoring Made Easy [online]. 1. 35 Livery Street Birmingham B3 2PB, UK: PacktPub, 2017 [cit. 2023-03-24]. ISBN 9781787129047.

[20] OPEN Vulnerability Assessment Scenner. *OPEN Vulnerability Assessment Scenner* [online]. Greenbone Networks GmbH: © [cit. 2021-12-09]. Dostupné z: https://www.openvas.org/

[21] OpenVAS. *Greenbone OpenVAS* [online]. online: https://www.openvas.org, 2023 [cit. 2023-03-25]. Dostupné z: https://www.openvas.org

[22] *Počítačové sítě bez předchozích znalostí*. Brno: Vydavatelství a nakladatelství CP Books, 2005. ISBN 80-251-0538-5.

[23] Počítačové sítě pro začínající správce. 3. aktualizované vydání. Brno: Computer Press, a.s, 2006. ISBN 80-251-0892-9.

[24] SECURITY ONION SOLUTIONS - SOFTWARE. *SECURITY ONION SOLUTIONS* [online]. online: ©, 2023 [cit. 2023-03-28]. Dostupné z: https://securityonionsolutions.com/software

[25] SecurityOnion. *SecurityOnionSolutions* [online]. online: ©, 2023 [cit. 2023-03-19]. Dostupné z: https://docs.securityonion.net/en/2.3/hardware.html

[26] SecurityOnionSolutions. *SecurityOnionSolutions* [online]. online: ©, 2023 [cit. 2023-03-24]. Dostupné z: https://docs.securityonion.net/en/2.3/about.html

[27] SecurityOnionSolutions. *SecurityOnionSolutions* [online]. online: ©, 2023 [cit. 2023-03-24]. Dostupné z: https://securityonionsolutions.com/software

[28] Simple Network Management Protocol. *SAMURAJ* [online]. Česká Republika: © [cit. 2021-12-12]. Dostupné z: https://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/

[29] ŠTĚDROŇ, Bohumír. *Open Source software ve veřejné správě a soukromém sektoru*. Praha: Grada, 2009. Průvodce (Grada). ISBN 978-80-247-3047-9.

[30] Upozorňujeme na zvýšené riziko DDoS útoků. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. online: ©, 2023 [cit. 2023-02-25]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1901-upozornujeme-na-zvysene-riziko-ddos-utoku/

[31] WAZUH documentation - Wazuh server. *WAZUH* [online]. online: ©, 2023 [cit. 2023-03-28]. Dostupné z: https://documentation.wazuh.com/current/installation-guide/wazuh-server/index.html

[32] Wazuh documentation. *WAZUH* [online]. online: ©, 2023 [cit. 2023-03-24]. Dostupné z: https://documentation.wazuh.com/current/getting-started/index.html

[33] WAZUH. WAZUH [online]. ONLINE: ©, 2023 [cit. 2023-02-02]. Dostupné z: https://documentation.wazuh.com/current/quickstart.html

[34] What is Kali Linux?. *KALI* [online]. OffSec Services Limited: © [cit. 2021-12-10]. Dostupné z: https://www.kali.org/docs/introduction/what-is-kali-linux/

[35] What Is Network Monitoring? CISCO [online]. San Jose: ©, 2021 [cit. 2021-12-08]. Dostupné z: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

[36] What is the Internet Control Message Protocol (ICMP)?. *Cloudflare* [online]. United States: © [cit. 2021-12-15]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/

[37] What si zero-day attack?. *Kaspersky* [online]. online: ©, 2022 [cit. 2023-01-30]. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit

[38] Zabbix features. *ZABBIX* [online]. ©: ZABBIX [cit. 2021-12-09]. Dostupné z: https://www.zabbix.com/documentation/5.2/en/manual/introduction/features

[39] ZABBIX hardware requirments. *ZABBIX* [online]. online: ©, 2023 [cit. 2023-03-28]. Dostupné z: https://www.zabbix.com/documentation/6.2/en/manual/installation/requirements

[40] Zabbix. ZABBIX [online]. ONLINE: ©, 2023 [cit. 2023-01-02]. Dostupné z: https://www.zabbix.com

[41] Zero-day definition. *Crowdstrike* [online]. online: online, 2023 [cit. 2023-03-01]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/

8 Seznam tabulek, obrázků, grafů a použitých zkratek

8.1 Seznam použitých tabulek

8.2 Seznam použitých obrázků

8.3 Seznam použitých grafů

8.4 Seznam použitých zkratek

AMD	ADVANCED MICRO DEVICE
API	APPLICATION PROGRAMMING INTERFACE
AWS	AMAZON WEB SERVICE
CD	COMPACT DISC
CDN	CLOUD DELIVERY NETWORK
CPU	CENTRAL PROCESSING UNIT
CVE	COMMON VULNERABILITIES AND EXPOSURES
CPE	COMMON PLATFORM ENUMERATION
CVSS	COMMON VULNERABILITY SCORING SYSTEM
DDOS	DISTRIBUTED DENIAL OF SERVICE
DNS	DOMAIN NAME SERVER
DVD	DIGITAL VIDEO DISC
EU	EVROPSKÁ UNIE
GDPR	GENERAL DATA PROTECTION REGULATION
GSAD	GREENBONE SECURITY ASSISTENT DEAMON
GSA	GREENBONE SECURITY ASSISTENT
GVMD	GREENBONE VULNERABILITES MANAGER DEAMON
HW	HARDWARE
IAAS	INFRASTRUCTURE-AS-A-SERVICE
ICMP	INTERNET CONTROL MESSAGE PROTOCOL

IDS	INTRUSION DETECTION SYSTEM
IIS	INTERNET INFORMATION SERVICES,
IOT	INTERNET OF THINGS
IP	INTERNET PROTOCOL
IPMI	INTELLIGENT PLATFORM MANAGEMENT INTERFACE
IOC	INDICATOR OF COMPROMISE
ISO	SOUBOROVÝ FORMÁT, KTERÝ SE POUŽÍVÁ K DISTRIBUCI INSTALAČNÍCH SOUBORŮ OPERAČNÍHO SYSTÉMU
ISP	INTERNET SERVICE PROVIDER
IT	INFORMAČNÍ TECHNOLOGIE
JMX	AVA MANAGEMENT EXTENSIONS
NMAP	NETWORK MAPPER
NUKIB	NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORAMČNÍ BEZPEČNOST
OSS	OPEN SOURCE SOFTWARE
OS	OPERAČNÍ SYSTÉM
PAAS	PLATFORM AS A SERVICE
PC	PERSONAL COMPUTER
PHP	HYPERTEXT PREPROCESSOR
RDP	REMOTE DESKTOP PROTOCOL
RAM	RANDOM ACCESS MEMORY
RAAS	ANSOMWARE AS A SERVICE
SAAS	SOFTWARE AS A SERVICE
SD	SECURE DIGITAL
SIEM	SECURITY INFORMATION AND EVENT MANAGEMENT
SMS	SHORT MESSAGE SERVICE
SNMP	SIMPLE NETOWORK MESSAGE PROTOCOL
SQL	STRUCTURED QUERY LANGUAGE
SW	SOFTWARE
SYSLOG	STANDARD FOR MESSAGE LOGGING
TCP	TRANSMISSION CONTROL PROTOCOL
URL	UNIFORM RESOURCE LOCATORS
UCAAS	UNIFIED COMMUNICATIONS AS A SERVICE
USB	UNIVERSAL SERIÁL BUS
VT	VULNERABILITY TEST/TESTING

XDR	EXTENDED DETECTION AND RESPONSE
XML	EXTENSIBLE MARKUP LANGUAGE

9 Přílohy

Příloha A Dotazníkový průzkum

Dobrý den, jsem studentem Provozně-ekonomické fauklty České zemědělské univerzity v Praze a chtěl bych Vás požádat o vyplnění dotazníku. Dotazník se týka kyberbezpečnosti a její implementace v počítačové sitě. Je určený správce sítě. Odpovědi udou zpracovány anonymně a poslouží pro zpracování diplomové práce. Děkuji za vyplnění dotazníku a Váš čas.	
1) Má vaše firma implementovanou politiku kybernetické bezpečnosti?	
	ANO
	NE
	NEVÍM
2) Proč firmy kyberbezpečnost neřeší?	
	Nedostatek finančních prostředků
	Nedostatek vědomostí a znalostí
	Časová náročnost
	Přeceňování kyberbezpečosti
	Nedostatek zájmu řešit kyberbezpečenost
3) Provádíte pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti?	
	ANO
	NE
	NEVÍM
4) Máte zavedený incident response plán pro řešení bezpečnostních incidentů?	
	ANO
	NE
	NEVÍM
5) Existuje u vás pravidelný audit bezpečnostních opatření a postupů	
	ANO
	NE
	NEVÍM
6) Používáte pokročilé systémy detekce hrozeb a průniků do sítě?	
	ANO
	NE
	NEVÍM
	ANO
	NE
	NEVÍM

Zdroj: Vlastní zpracování