Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra Informačních Technologií

Bakalářská práce

Monitoring sítě, implementace bezpečnostních systémů ve firmě

Jan Soukup

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Soukup

Informatika

Název práce

Monitoring sítě, implementace bezpečnostních systémů ve firmě

Název anglicky

Network monitoring, implementation of security systems in firm

---

Cíle práce

Hlavním cílem je implementovat efektivní monitorovací systém pro detekci a prevenci potenciálních hrozeb.
Dílčí cíle práce jsou:
-Analýza – stanovení cílů, inventarizace aktiv, discovery proces a další.
-Vulnerability management.
-Implementace.
-Monitoring a vyhodnocování.

Metodika

1. Krokem práce bude zvolení a vytvoření (aktiva, velikost, síťové segmenty atd.) imaginární firmy pro kterou budu následně práci psát.

2. U vytvořené firmy se začne analýzou současného stavu zabezpečení informačních systémů ve firmě a identifikací potenciálních hrozeb a slabých míst v síti. Bude zkoumáno, jakým způsobem mohou útočníci proniknout do sítě a jaké důsledky by to mohlo mít pro firmu. Bude-li ve firmě už nějaký bezpečnostní systém existovat tak se rozhodnout, jestli na něj navázat, či začít nanovo. Celkově stanovit další cíle a směr.

3. Na základě analýzy rizik budou navržena vhodná bezpečnostní opatření a systémy, které pomohou chránit informační systémy před možnými hrozbami. To může zahrnovat implementaci firewallu, antivirového softwaru, přístupových kontrol, šifrování dat a dalších bezpečnostních opatření. (Volba vhodných opatření záleží na zvolené velikosti firmy, rozpočtu a dalších faktorech).

4. Práce bude také zahrnovat návrh a implementaci monitorovacího systému, který bude sledovat provoz v síti a identifikovat podezřelé aktivity nebo anomálie. Tento systém bude schopen detekovat a reagovat na pokusy o neoprávněný přístup, útoky založené na síťových hrozbách nebo neobvyklé chování uživatelů. Testování může probíhat pouze na zvoleném segmentu před plnou implementací do celé sítě firmy.

5. Implementované bezpečnostní systémy a monitorovací mechanismy budou testovány a jejich účinnost bude vyhodnocena. Práce se zaměří na hodnocení detekce a reakčních schopností systému a na zhodnocení přesnosti a spolehlivosti monitorovacího procesu. Vyskytne-li se nějaký nedostatek, chyba či hrozba, návrat k bodu 3 se snahou zachovat co nejvíce, již funkčních a bezproblémových systémů.

Doporučený rozsah práce

35-45s.

Klíčová slova

SIEM, DLP, segmentace, SOAR, EDR, IDS, Firewall, MITRE ATT&CK Framework, Flowmon, Tiering

---

Doporučené zdroje informací

Computer system and network security. WHITE, Gregory B.; FISCH, Eric A.; POOCH, Udo W.; CRC PRESS.

HERRMANN, Debra S. *Complete guide to security and privacy metrics : measuring regulatory compliance, operational resilience, and ROI.* Boca Raton (Florida): Auerbach Publications, 2007. ISBN 0-8493-5402-1.

Honeypot Frameworks and Their Applications. [elektronický zdroj] /. NG, Chee Keong.; PAN, Lei.; XIANG, Yang.

LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. *Teorie bezpečnosti počítačových sítí.* Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.

MARTELLINI, Maurizio. Cyber security: deterrence and IT protection for critical infrastructures. Cham: Springer, 2013. ISBN 3319022784;9783319022789

NORTHCUTT, Stephen. *Bezpečnost sítí : velká kniha.*.

Windows networking tools : the complete guide to management, troubleshooting, and security. HELD, Gilbert.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 9. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Monitoring sítě, implementace bezpečnostních systémů ve firmě" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské 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(ka) uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.03.2024 _____

Poděkování

Rád(a) bych touto cestou poděkoval(a) Ing. Martinu Havránekovi, Ph.D. za vedení této práce.

Monitoring sítě, implementace bezpečnostních systémů ve firmě

Abstrakt

Tato bakalářská práce se zaměřuje na problematiku implementace bezpečnostních systémů do firem s cílem zlepšit ochranu dat, systémů a dalších. V současném digitálním prostředí čelí firmy stále sofistikovanějším hrozbám, jako jsou kybernetické útoky, krádeže dat či fyzické napadení. Cílem této práce je analyzovat postupy a metody implementace bezpečnostních systémů do firem a navrhnout optimální strategie pro zajištění co nejefektivnější ochrany.

První část práce se věnuje teoretickému základu bezpečnostních systémů a představuje klíčové prvky, jako jsou požadavky na ochranu dat, identifikace rizik a implementace technických opatření. Druhá část je věnována posouzení efektivity současných bezpečnostních systémů. Na základě získaných dat jsou identifikovány klíčové výzvy a potřeby firem v oblasti bezpečnosti.

V další části jsou navrženy konkrétní strategie implementace bezpečnostních systémů, které zohledňují specifika jednotlivých firem a přinášejí komplexní přístup k ochraně. Tyto strategie zahrnují kombinaci technických opatření, vzdělávání zaměstnanců a implementaci bezpečnostních politik. V závěrečné části jsou prezentovány výsledky implementace navržených strategií a zhodnocení jejich účinnosti na základě sledovaných ukazatelů.

Výsledkem této práce je komplexní pohled na problematiku implementace bezpečnostních systémů do firem a návrhy konkrétních opatření pro zlepšení ochrany. Navrhované strategie mohou sloužit jako užitečný nástroj pro manažery firem při rozhodování o investicích do bezpečnosti a optimalizaci procesů ochrany před různými hrozbami.

Klíčová slova: SIEM, DLP, segmentace, SOAR, EDR, IDS, Firewall, MITRE ATT&CK Framework, Flowmon, Tiering

Network monitoring, implementation of security systems in firm

Abstract

This bachelor thesis focuses on the issue of implementing security systems in companies to improve the protection of data, systems and more. In today's digital environment, companies face increasingly sophisticated threats such as cyber-attacks, data theft and physical attacks. The aim of this paper is to analyze the practices and methods of implementing security systems in companies and to propose optimal strategies to provide the most effective protection.

The first part of the thesis deals with the theoretical background of security systems and presents key elements such as data protection requirements, risk identification and implementation of technical measures. The second part is devoted to an assessment of the effectiveness of current security systems. Based on the data collected, key challenges and needs of companies in the field of security are identified.

In the next part, specific strategies for the implementation of security systems are proposed, which take into account the specifics of individual companies and bring a comprehensive approach to protection. These strategies include a combination of technical measures, employee training and implementation of security policies. The final part presents the results of the implementation of the proposed strategies and an evaluation of their effectiveness based on the monitored indicators.

The result of this work is a comprehensive view of the issue of implementing security systems in companies and suggestions for specific measures to improve protection. The proposed strategies can serve as a useful tool for company managers when making decisions about security investments and optimizing processes to protect against various threats.

Translated with DeepL.com (free version)

Keywords: SIEM, DLP, segmentation, SOAR, EDR, IDS, Firewall, MITRE ATT&CK Framework, Flowmon, Tiering

Obsah

1 Úvod

V dnešní době je nezbytné mít pevně zajištěnou síť pro každou firmu. Digitalizace proniká do všech aspektů podnikání a bezpečnostní otázky jsou klíčové pro úspěch organizace. S nárůstem objemu dat a sofistikovanějšími hrozbami je nezbytné zajistit, aby byla firemní síť chráněna před neoprávněným přístupem, útoky zločinců a zachováním důvěrnosti citlivých informací.

Ochrana a dohled nad sítí ve firmě zahrnuje celou řadu opatření s cílem chránit informace, udržovat dostupnost služeb a bránit případným útokům. To zahrnuje technologie jako firewally, šifrování dat, antivirové programy, bezpečnostní protokoly a školení zaměstnanců. Bezpečná síť je klíčová pro bezproblémový chod podnikání, efektivní spolupráci, bezpečnou výměnu dat a ochranu důvěrných informací.

Monitorování sítě je klíčové v prevenci a odhalování hrozeb. Pravidelné sledování síťové aktivity umožňuje identifikovat neobvyklé vzory chování, které mohou naznačovat možné útoky a umožňuje rychlou reakci. Monitorování zahrnuje sledování síťového provozu, detekci neobvyklých aktivit, analýzu bezpečnostních událostí a reakci na incidenty.

Je klíčové mít integrovaný přístup k zabezpečení a monitorování sítě, který je přizpůsoben konkrétním potřebám a povaze podnikání. Efektivní zabezpečení a monitorování sítě nejsou pouze investicí do technologií, ale i do ochrany pověsti firmy, důvěry zákazníků a celkového úspěchu podnikání.

V této práci budeme zkoumat různé aspekty zabezpečení a monitorování sítě ve firmě, včetně nejnovějších technologií, strategií a osvědčených postupů, které pomáhají organizacím chránit své síťové prostředí a zajistit bezpečnost citlivých informací. Dále se zaměříme na výzvy, kterým firmy čelí v souvislosti se zabezpečením a monitorováním sítě, a nabídneme doporučení, jak tyto výzvy překonat a vytvořit bezpečné a spolehlivé síťové prostředí ve firmě.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je úspěšná implementace efektivního monitorovacího systému, který bude v síti vybrané (vytvořené) firmy detekovat a provádět preventivní opatření vůči hrozbám v ní se vyskytujících.

2.2 Metodika

V první řadě bude vytvořena příkladová firma, na které budeme následně monitorovací a zabezpečovací systém nasazovat. Aby bylo možné v analýze získat veškerá potřebná data bude firma vytvářena se stoprocentní transparentností. Klíčovými daty tak budou například i dostupný kapitál, a to jak investiční, tak zaměstnanecký.

U vytvořené firmy bude následně provedena analýza stávajícího stavu. Zkoumána tak bude velkost firmy, jak co se týče počtu zaměstnanců (dost často totiž platí, že co zaměstnanec, to pracovní stanice), tak i velikost sítě, což jsou již zmíněné stanice, virtuální stroje, data servery, firewally, směrovače, doménové servery a případně i další. Tímto krokem, který se jmenuje Discovery proces bude také zjištěno, jak je síť firmy segmentována. Díky předchozímu kroku budou identifikovány potencionální hrozby a slabá místa v síti, a bude-li firma mít i bezpečnostní systém tak i chyby v něm, která by útočníkům umožnila do firmy proniknout. Celkovou analýzou tak bude stanoven další směr a cíle práce.

V návaznosti na analýzu rizik budou navrženy bezpečnostní opatření a systémy, které pomohou zjištěné hrozby potlačit a monitorovat. Zástupci této kategorie jsou například: firewall, antivirový software, šifrování dat, ale třeba i fyzická kontrola přístupu do budovy firmy, formát a velikost hesel pro různé účty atd.

Dalším krokem bude implementace navrhnutých opatření a primárně systémů, které budou síť firmy monitorovat a v případě jakéhokoliv útoku, hrozby či chyby je detekovat a vyvolat na ně odpovídající reakci. V rámci nasazování systémů bude kladen důraz na dodržování zajetých postupů z reálného prostředí jako je třeba nasazení systémů do testovacího prostředí před plným uvolněním do celé sítě firmy.

Po implementaci opatření a systémů bude provedeno testování a vyhodnocení nasazených mechanismů, které se pak obzvlášť zaměří na schopnost detekce a reakčních schopností zvolených systémů.

3 Teoretická východiska

3.1 Zhodnocení hrozeb a bezpečnostních rizik

3.1.1 Identifikace hrozeb a rizik

Má-li být jakákoliv firma zabezpečena proti kybernetickým hrozbám a rizikům, musí předně vědět o jakým hrozbám a rizikům může vůbec čelit a přesně o tomto pojednává tato podkapitola.

3.1.1.1 Kybernetické hrozby

Slovním spojením kybernetické hrozby bývá primárně myšleno, jakým typům kybernetických útoků může firma čelit. V rámci analýzy této otázky bylo zjištěno, že existuje několik základních typů těchto útoků:

3.1.1.1.1 Malware

Malware neboli škodlivý software, se maskuje jako důvěryhodná e-mailová příloha nebo program (tj. šifrovaný dokument nebo složka souborů), aby mohl využít viry a umožnil hackerům proniknout do počítačové sítě. Tento typ kybernetických útoků často naruší celou IT síť. Mezi příklady malwaru patří trojské koně, spyware, červi, viry a adware.

3.1.1.1.2 Distribuovaný útok s cílem odepření služeb (DDoS)

Útok DDoS spočívá v tom, že se několik napadených počítačových systémů zaměří na určitý web nebo síť a znemožní uživatelům tento web nebo síť používat. Například stovky automaticky otevíraných oken, reklam, a dokonce i chybově ukončované weby můžou přispět k útoku DDoS na napadeném serveru.

3.1.1.1.3 Útoky phishing

Phishing je zasílání podvodných e-mailů jménem renomovaných společností. Hackeři používají útoky phishing k získání přístupu k datům v osobních nebo firemních sítích.

3.1.1.1.4 Útoky prostřednictvím injektáže SQL

Útok prostřednictvím injektáže SQL spočívá v tom, že kyberzločinec zneužije software tak, že využije aplikace (například LinkedIn, Target) ke krádeži nebo odstranění dat nebo k získání kontroly nad těmito daty.

3.1.1.1.5 Skriptování mezi weby (XSS)

Skriptování mezi weby (XSS) je situace, kdy kyberzločinec odešle do vaší doručené pošty odkaz na web vložený pomocí skriptu nebo spamu a při jeho otevření se tento kyberzločinec dostane k osobním údajům.

3.1.1.1.6 Botnety

Botnety jsou případy, kdy je více počítačů, obvykle v privátní síti, infikováno viry a jinými formami škodlivého softwaru, například automaticky otevíranými zprávami nebo spamem.

3.1.1.1.7 Ransomware

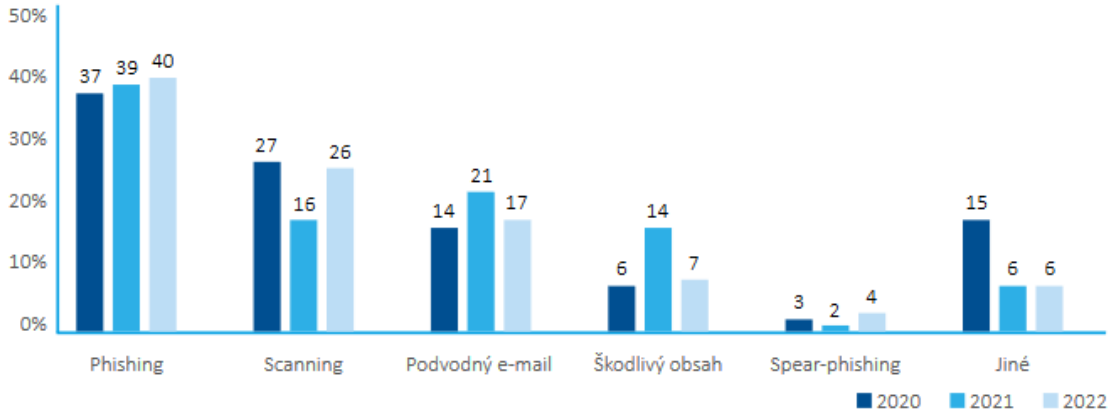
Ransomware je typ škodlivého softwaru neboli malwaru, který vyhrožuje obětem tím, že pokud nezaplatí výkupné, jejich klíčová data nebo systémy budou zničeny nebo přístup k nim bude zablokován. (Microsoft)

K těmto útokům je nutné podotknout, že byť se jedná o nejčastější typy útoků existuje nesčetně variant, jak je podniknou. Tyto základní typy je dobré držet v povědomí, avšak aby bylo zaručeno, co možná nejbezpečnější prostředí je nutné sledovat vývoj v tomto směru. Tomu je věnována následující kapitola.

Co se týče zdroje, lze Microsoft považovat za odborníka v oblasti kybernetiky, řadu let provozuje například ve svém operačním systému Windows antivirus, který je znám třeba i svou velmi rychlou aktualizací definic pro rozpoznávání hrozeb.

3.1.1.1.8 Statistiky hrozeb

Obrázek číslo 1 od Národního úřadu pro kybernetickou bezpečnost ukazuje, s jakými typy útoků se v roce 2022 setkávaly dotazované organizace nejčastěji a k těmto datům jsou přidány i statistiky z 2 předchozích let.



(N., 2022)Obrázek 1Typy kybernetických útoků

3.1.1.2 **Bezpečnostní rizika**

Bezpečnostní rizika představují hrozby pro organizaci, které mohou způsobit vážné problémy. Tato rizika mohou zahrnovat ztrátu důvěrných informací, finanční škody, přerušení provozu a porušení právních předpisů. Kybernetické podvody, útoky typu DDoS a ztráta služeb jsou jen několik příkladů, jak může organizaci hrozit. Takové incidenty mohou způsobit vážné ekonomické ztráty, poškodit pověst firmy a vést ke ztrátě důvěryhodnosti. Některá rizika jsou spojena i s interními faktory, jako jsou chyby zaměstnanců nebo neoprávněný přístup k citlivým informacím.

3.1.1.2.1 Ztráta Dat

Ztráta Citlivých Informací: K úniku citlivých dat může dojít v důsledku hackerských útoků nebo vnitřních hrozeb (např. zaměstnanci).

Porušení Soukromí: Neoprávněný přístup k osobním údajům klientů nebo zaměstnanců může způsobit porušení soukromí.

3.1.1.2.2 Finanční ztráty

Kybernetické Podvody: Podvodné aktivity jako phishing nebo podvržení identity mohou vést ke finančním ztrátám.

Vydírání: Útočníci mohou zašifrovat organizaci s cílem vydírat peníze za dešifrování dat.

3.1.1.2.3 Poškození pověsti firmy

Škody na Pověsti: Veřejný vnímání firmy může být poškozeno, pokud dojde k bezpečnostnímu incidentu, což může ovlivnit důvěru zákazníků a obchodní partnery.

Ztráta Důvěryhodnosti: Neschopnost chránit citlivé údaje může vést ke ztrátě důvěryhodnosti veřejnosti.

3.1.2 Proč vůbec Hackeři hackují?

Kybernetické útoky mohou probíhat z mnoha důvodů. Porozuměním těmto důvodům může organizacím přinést lepší ochranu proti potencionálním hrozbám. Zde je několik základních nejběžnějších motivů kybernetických útoků.

Finanční zisk: Je hlavní motiv pro mnoho kybernetických zločinců. Tyto útoky mohou používat různé metody k získání peněz, jako je krádež informací o platební kartě, držení dat jako rukojmí nebo prodej ukradených dat na černém trhu.

Uznání a úspěch: Někteří hackeři jsou motivováni pocitem úspěchu, který přináší prolomení velkého systému. Mohou pracovat ve skupinách nebo samostatně, ale chtějí být uznáni. To také souvisí s tím, že kybernetičtí zločinci jsou přirozeně soutěživí a milují výzvy, které jejich činy přinášejí.

Vnitřní hrozby: Osoby, které mají přístup k důležitým informacím nebo systémům, mohou snadno zneužít tento přístup na újmu své organizace. Tyto hrozby mohou pocházet od interních zaměstnanců, dodavatelů, subdodavatelů nebo partnerů a jsou považovány za jedny z největších kybernetických hrozeb pro organizace

Ideologie: Tato motivace může být trochu složitější. Tito jedinci cílí na společnosti kvůli rozdílu v hodnotách. Například politicky motivovaní útočníci jsou často spojováni s kybernetickou válkou, kyberterorismem nebo "hacktivismem". V kybernetické válce často státní aktéři cílí na vládní agentury nebo kritickou infrastrukturu svých nepřátel. Aktivistická hackeři, nazývaní "hacktivisté", nemusí svým cílům způsobovat rozsáhlé škody. Místo toho obvykle hledají pozornost pro své věci tím, že své útoky dávají veřejně známé.

Ego: Někteří kybernetičtí zločinci jsou motivováni touhou dokázat své schopnosti nebo získat notorietu. Mohou cílit na významné organizace nebo systémy, aby si udělali jméno.

Nenávist a pomsta: Kybernetické zločiny proti osobě, jako je kyberstalkování, kyberšikana, trolling, mstivá pornografie, jsou pravděpodobně motivovány nenávistí, touhou způsobit bolest a škodu známým nebo neznámým jednotlivcům, skupinám nebo komunitám.

Je důležité poznamenat, že motivace kybernetických zločinců jsou výrazně ovlivněny samotným zločinem a kvůli různorodosti různých online zločinů je obtížné zvažovat motivace pro kybernetickou kriminalitu na obecné úrovni.

3.1.3 **Analýza aktuálních kybernetických hrozeb**

Kybernetické hrozby jsou i nadále motivovány politickým a sociálním děním ve společnosti spolu s již zmíněnými dalšími důvody. V této části bude nahlédnuto na současné útoky, či útoky z blízké minulosti v době psaní této práce.

3.1.3.1 **Zprávy o Kybernetických Útocích**

I nadále se nacházejí na úvodních pozicích útoky typu DDoS a Ransomware.

Co se týče sociálního inženýrství stále v této kategorii vede phishing. Útoky tohoto typu jsou významnou částí kybernetických hrozeb.

Důležitým parametrem útoků je i sektor, na který míří. Společnost Trellix například ve svém reportu incidentů za první kvartál uvádí, že 8 % útoků cílilo na výrobu, 7 % na finanční sektor, 6 % na zdravotní sektor, 5 % na telekomunikace a 5 % na energetický sektor (Trellix, 2023). Oproti tomu data ze zprávy od Evropské agentury pro bezpečnost sítí a informací tvrdí, že na výrobu cílilo 4,12 %, na finanční sektor pak 5,49 %, na zdravotní sektor 3,3 % a 1,1 % bylo na energetický sektor (ENISA, 2022). A i když je rozdíl velikosti těchto vzorků veliký (1 kvartál od Trellixu oproti roku od ENISA), lze z nich vyvodit pár informací. Na první pohled se může zdát, že se v průběhu roku velmi mění trendy v kybernetických útocích a do určité míry je to i pravda, avšak spíše něž, že by se jednalo o tuto situaci, bude lepší hledat vysvětlení jinde. Trellix je poskytovatelem systémů na zabezpečení sítě a zařízení, a tak čerpá data přímo ze svých systémů. Oproti tomu ENISA jako vládní organizace čerpá data z daleko širších zdrojů.

3.1.3.2 **Trendy v Kybernetické Kriminalitě**

Tendence v oblasti kybernetické kriminality odhalují neustálý vývoj taktik a strategií kybernetických aktérů. Mezi klíčové směry patří stoupající výskyt ransomwarových útoků, soustředění na dodavatelské řetězce a podvody prostřednictvím firemních e-mailů. Zvýšená propojenost pomocí IoT zvyšuje riziko útoků na propojená zařízení. Šíření dezinformací a používání technologií pro hlubokou falšování jsou stále sofistikovanějšími prostředky manipulace s informacemi a obrazem. Využívání umělé inteligence a strojového učení posiluje jak útočníky při vytváření složitých útoků, tak obranné mechanismy při detekci. Zneužívání kryptoměn poskytuje kybernetickým zločincům anonymitu při výkupných útocích. Mezinárodní spolupráce se stává klíčovým faktorem v boji proti kybernetické

kriminalitě, kde sdílení informací a současná opatření jsou nezbytné pro účinnou ochranu před komplexními hrozbami. (The, 2023)

3.1.4 Faktory Zvyšující Bezpečnostní Rizika Bezpečnostních Slabostí

Faktory posilující bezpečnostní rizika v kyberbezpečnosti zahrnují širokou škálu potenciálních hrozeb a křehkých míst v digitálním prostoru. Nedostatek informovanosti mezi uživateli, zanedbávání aktualizací softwaru a systémů, lidské chyby, sociální podvody a šíření škodlivého kódu představují zásadní rizikové faktory. Bezpečnostní otázky spojené s nezabezpečeným přístupem, používání cloudových služeb a nedostatečným zálohováním dat také přispívají k narůstajícím bezpečnostním hrozbám. Kybernetické útoky se zaměřují na infrastrukturu pomocí DDoS útoků nebo cílených kybernetických operací. Obecně platí, že účinná kyberbezpečnostní strategie vyžaduje kombinaci technologických opatření, osvěty, a aktivní monitorování a reakci na aktuální bezpečnostní výzvy.

3.2 Analýza současných bezpečnostních systémů

V době, kdy je bezpečnost dat a informací důležitější než nikdy předtím a kdy informační systémy provozují i firmy, které neposkytují digitální služby, je existence zákona vymezujícím jasná pravidla o alespoň minimálních standardech nepřekvapující. V rámci zákona je vymezeno několik pojmů: Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. (§ 4 Zákon č. 181/2014 Sb.)– Tato definice v podstatě popisuje to, o čem tato práce pojednává.

3.2.1 Minimální bezpečnostní standard dle zákona 181/2014 Sb.

I k dosažení minimální bezpečnosti je nutno splňovat nějaké předpoklady. V úvodu této kapitoly jich bude několik jmenováno a zhodnoceno.

Základním předpokladem systematického přístupu ke kybernetické bezpečnosti je podpora ze strany vrcholového vedení při jejím prosazování. Je potřeba vyčlenit potřebné zdroje, stanovit bezpečnostní role, vytvořit přiměřené bezpečnostní politiky a dokumentaci, včetně jejich schválení a následně kontrolovat jejich dodržování. Vrcholové vedení musí projevit dostatečnou podporu a přidělit přiměřené zdroje (finanční, lidské, technické) potřebné k zavedení a udržování principů vedoucích ke zvyšování kybernetické bezpečnosti a určit osobu odpovědnou za kybernetickou bezpečnost, včetně stanovení jejích povinností,

odpovědností a pravomocí. Tato role je odpovědná za řízení a rozvoj kybernetické bezpečnosti, průběžnou kontrolu stavu kybernetické bezpečnosti, dohlížení na naplňování plánu zavádění bezpečnostních opatření a komunikaci v oblasti kybernetické bezpečnosti s vrcholovým vedením. (N.Ú.K.I.B, 2023) – Jedním ze základních kroků k úspěchu je součinnost majitelů, garantů a obecně vrcholového vedení se správci informačních systémů. Ponechá-li management tento úkon pouze na správcích a nebude se o problém sám zajímat, tak i sebelepší správci s těmi nejlepšími úmysly budou s velkými obtížemi dodržovat, byť jen zákonem stanovené minimum.

Dále je potřeba vytvořit přiměřené bezpečnostní politiky a bezpečnostní dokumentaci. Tyto politiky a dokumenty musí být dostatečně návodné, aby bylo zajištěno, že výsledky budou reprodukovatelné - tzn., aby jiná osoba byla po jejich nastudování schopna postupovat shodným způsobem. Seznam oblastí, jež by měly bezpečnostní politiky a dokumentace zahrnovat, je uveden v příloze tohoto dokumentu. Při výběru vhodných politik a dokumentace je vždy nutné zohlednit jejich relevanci pro konkrétní prostřední organizace. Bezpečnostní politiky a dokumentace musí být schváleny na stejné úrovni jako jiné interní akty organizace (tedy nejčastěji vrcholovým vedením), a to mimo jiné i z toho důvodu, aby byla zajištěna jejich vymahatelnost. (N.Ú.K.I.B, 2023) – Obměna zaměstnanců je ve firemním prostředí standardní proces a díky vytvořeným politikám mohou noví zaměstnanci v již zavedeném systému fungovat. Pochopit však veškeré mechanismy a procesy pouze ze zdlouhavých manuálů a návodů nemusí být snadné ani rychlé, je tak stále doporučeno zaučení zaměstnance další osobou pracující na obdobné či stejné pozici.

Politiky a dokumentace by měly být v přiměřených intervalech aktualizovány tak, aby vždy reflektovaly aktuální stav. (N.Ú.K.I.B, 2023) – Zastaralá dokumentace a politiky může v určitých případech znamenat i vystavení se hrozbám, a to jak ze strany zákona, tak ze strany útočníků.

Jedním z dalších základních kroků by mělo být: stanovení hodnoty informací za účelem jejich adekvátní ochrany. Tím, že dochází k jejich třídění podle hodnoty a následné ochraně dle důležitosti, může docházet ke snižování nákladů, protože není nutné chránit všechny informace na stejné úrovni. (N.Ú.K.I.B, 2023) – Toto tvrzení je samozřejmě pravdivé, avšak nemusí být ke škodě toto hodnocení trochu nadhodnotit. Nemusí nám být totiž známo, jaké informace se v budoucnu ve firmě objeví. Obecně řečeno, je nad problematikou lepší přemýšlet s předstihem, nežli ve chvíli výskytu nějakého problému či

hrozby. Často může tento postup, byť zdánlivě v danou chvíli i nákladnější, ve výsledku vyjít levněji.

Velkou pozornost je zapotřebí věnovat také řízení lidských zdrojů. Je proto doporučeno: Poučit uživatele, administrátory a osoby zastávající bezpečnostní role o jejich povinnostech, teoreticky i prakticky je školit. (N.Ú.K.I.B, 2023) – Takto školení by měla být pravidelná, v rámci školení o kybernetické bezpečnosti by pak měli všichni zaměstnanci absolvovat školení minimálně 1 ročně. Zaměstnanci by měli být také proškoleni, jak se chovat v případě neobvyklého či podezřelého chování informačního nebo komunikačního systému, doručení nevyžádaného e-mailu, problémů s dostupností informací či služby nebo při jiné nestandardní situaci. Současně by měli být seznámeni se způsobem, jak tyto neobvyklé situace hlásit. (N.Ú.K.I.B, 2023) – Tomuto tvrzení nelze než dát za pravdu, je však nutné znovu podotknout, že nástroje a taktiky útočníků se neustále mění a přizpůsobují, a je tedy doporučeno tyto informace zaměstnancům předávat formou školení či informačních zpráv.

Každá firma se v průběhu své existence přeměňuje. Tyto změny mohou často probíhat i v informačních a komunikačních systémech. (N.Ú.K.I.B, 2023) - Tato problematika zahrnuje evidenci všech změn, systematické vyhodnocování, koordinování a implementaci schválených změn a konfigurací. V případě, že bude organizace provádět změnu, tak by měla zvážit možné dopady této změny. Změna, která by mohla mít nepříznivý dopad na informační nebo komunikační systém nebo bezpečnost informací, by měla být dokumentována. Změny v rámci informačního nebo komunikačního systému by měly být řízeny prostřednictvím změnových požadavků, které jsou schvalovány osobou odpovědnou za kybernetickou bezpečnost.

Dále je potřeba:

-přijmout opatření za účelem snížení všech nepříznivých dopadů spojených se změnami,
-aktualizovat relevantní bezpečnostní politiky a bezpečnostní dokumentaci,
-zajistit testování změn
-zajistit možnost navrácení do původního stavu.

V případě potřeby je vhodné provést penetrační testování.

Dostupnost aktuálních a použitelných plánů kontinuity (Business Continuity Plan - BCP), plánů obnovy (Disaster Recovery Plan - DRP) a havarijních plánů, aby v případě mimořádné situace (havárie, živelné pohromy nebo úspěšného kybernetického útoku) byla organizace schopna obnovit svoji funkčnost.

3.3 Posouzení efektivity současných systémů

Současné metody kyberbezpečnosti spočívají ve složitých soustavách technologií a postupů, které mají za úkol chránit informace, data, sítě a zařízení před různými formami kybernetických hrozeb. Tyto systémy se průběžně rozvíjejí a zdokonalují, aby odolaly novým, stále sofistikovanějším útokům. Zde je stručný popis několika klíčových prvků současných zabezpečovacích systémů v oblasti kyberbezpečnosti:

Programy na ochranu před škodlivým kódem (Antiviry): Tyto nástroje jsou základními součástmi kyberbezpečnosti. Identifikují, blokují a likvidují škodlivý software, jako jsou viry, trojské koně a spyware, které by mohly narušit integritu a bezpečnost dat.

Ochranné bariéry (Firewally): Firewally slouží k dohledu a regulaci síťového provozu na základě předem definovaných pravidel. Síťové bariéry operují na úrovni celé sítě, zatímco hostitelské bariéry se zaměřují na konkrétní zařízení, chráníce tak síťový provoz před neoprávněným vniknutím a útoky.

Systémy detekce a prevence neoprávněného vniknutí (IDS/IPS): Tyto systémy sledují síťový provoz a identifikují či brání v potenciálně nebezpečných aktivitách. Intruzivní útoky jsou rozpoznány a následně mohou být přijata patřičná opatření.

Šifrování dat: Tato metoda je klíčová pro ochranu citlivých informací před neoprávněným přístupem. Šifrování dat zabezpečuje, že i v případě získání přístupu k datům útočník nemá schopnost jejich čtení nebo interpretace.

Dvoufaktorová autentizace (2FA) a autentizace pomocí více faktorů (MFA): Tyto metody zvyšují úroveň autentizace vyžadováním více než jednoho způsobu ověření identity, což komplikuje neoprávněným osobám získání přístupu k systémům.

Behaviorální analýza: Monitorování normálního uživatelského a síťového chování umožňuje odhalení odchylek, které mohou signalizovat možné útoky nebo neoprávněný přístup.

Ochranné brány pro internetový provoz: Tyto brány sledují a filtrování provoz na internetu, chráníce uživatele před nebezpečnými webovými stránkami a hrozbami.

Ochrana koncových bodů (Endpoint Security): Poskytuje bezpečnostní ochranu koncových zařízení, jako jsou počítače, mobilní telefony a další, před kybernetickými hrozbami.

Ochrana v prostředí cloudu: Zabezpečení cloudových služeb proti různým hrozbám, včetně neoprávněného přístupu a úniku dat.

Decepce a pasti pro kybernetické útočníky (Deception a Honeypots): Tato strategie vytváří falešné cíle a informace s cílem přitáhnout a odhalit potenciální útočníky.

SIEM (Security Information and Event Management) systémy: jsou klíčovými nástroji pro sledování bezpečnostních metrik a generování reportů v informačních systémech. Tyto systémy zpracovávají bezpečnostní události v informačních systémech a umožňují organizacím monitorovat a analyzovat potenciální hrozby a incidenty. Moderní SIEM systémy nabízejí širokou škálu nástrojů pro efektivní sledování a analýzu bezpečnostních událostí. Níže byl sepsán seznam nástrojů, které lze u moderních SIEM systémů nalézt (Micosoft):

Zpracování událostí (Event Processing): Zpracování a sběr dat z různých zdrojů v reálném čase, včetně bezpečnostních událostí, logů, síťového provozu a dalších.

Analýza událostí (Event Analysis): Analýza a hodnocení událostí a aktivit s cílem identifikovat podezřelé vzory a anomálie, které by mohly naznačovat bezpečnostní incidenty.

Ukládání a archivace dat (Data Storage and Archiving): Ukládání a archivace zpracovaných dat a událostí pro pozdější vyšetřování, analýzu a audity.

Korelace událostí (Event Correlation): Sledování a korelace událostí z různých zdrojů a kontextů, aby bylo možné identifikovat souvislosti a složitější bezpečnostní hrozby.

Detekce hrozeb (Threat Detection): Identifikace a detekce známých a neznámých hrozeb pomocí pravidel, algoritmů strojového učení a heuristik.

Dashboardy a vizualizace (Dashboards and Visualization): Vytváření vizuálních přehledů, dashboardů a reportů pro sledování bezpečnostní situace a prezentaci dat.

Správa incidentů (Incident Management): Správa a dokumentace bezpečnostních incidentů, včetně jejich sledování, eskalace a řešení.

Integrace a spolupráce (Integration and Collaboration): Možnost integrace s dalšími bezpečnostními nástroji a platformami a podpora spolupráce mezi bezpečnostními týmy.

Audity a compliance (Auditing and Compliance): Monitorování a hodnocení souladu s bezpečnostními standardy a předpisy pomocí auditů a reportů.

Automatizace (Automation): Automatizace opakujících se úloh a odpovědí na bezpečnostní události pomocí skriptů, pravidel a workflow.

3.3.1 Porovnání SIEM systémů

V následující podkapitole bylo prozkoumáno několik běžně používaných SIEM systémů a provedeno jejich porovnání (jeden z výchozích bodů, o které se opírá praktická část).

3.3.1.1 Splunk SIEM

Splunk SIEM tak jako ostatní systémy funguje jako univerzální platforma s neomezeným potenciálem a nabízí základní sadu funkcí Splunk Enterprise, kterou lze kdykoli rozšířit prostřednictvím modulárních aplikací. (ALEF)

Funkce Splunk SIEM

Sběr událostí: SPLUNK umožňuje sběr, indexaci a ukládání událostí z různých zdrojů, včetně logů, síťového provozu, aplikací, endpointů a cloudových služeb.

Detekce hrozeb: Platforma poskytuje pokročilé techniky detekce hrozeb a anomálií, včetně pravidel, strojového učení a analýzy behaviorálních vzorů.

Korelace událostí: SPLUNK umožňuje korelaci událostí z různých zdrojů a kontextů, což umožňuje identifikovat související události a potenciální hrozby.

Upozorňování a ovládací panely: Platforma nabízí funkce pro vytváření výstrah, grafů, řídicích panelů a sestav, které umožňují efektivně sledovat bezpečnostní metriky a přijímat informovaná rozhodnutí.

Analýza chování: S využitím strojového učení dokáže Splunk SIEM optimalizovat bezpečnostní operace odhalováním problémů, urychlením vyšetřování, snížením složitosti a zlepšením reakce na útoky.

Škálovatelnost a flexibilita: Splunk SIEM je moderní platforma pro zpracování velkých objemů dat, kterou lze škálovat tak, aby vyhovovala různým případům použití v

oblasti zabezpečení v různých prostředích nasazení, jako je cloud, lokální nebo hybridní nastavení. (Comodo)

Compliance: SPLUNK podporuje správu souladu s předpisy a standardy, včetně generování auditních reportů a sledování dodržování bezpečnostních předpisů.
Automatizace a orchestrace: Platforma umožňuje automatizaci a orchestraci bezpečnostních operací a odpovědí na incidenty, což zvyšuje efektivitu a rychlost reakce na bezpečnostní události.

Cloud-native: SPLUNK je navržen tak, aby byl plně kompatibilní s cloudovými prostředími a mohl efektivně zpracovávat data z cloudových služeb.

Nevýhody Splunk SIEM

Vysoké náklady: Implementace a provoz SPLUNK SIEM může být finančně náročný, zejména pro menší organizace s omezeným rozpočtem. Licenční poplatky, školení personálu a infrastrukturní náklady mohou být vysoké.

Složitá implementace: Instalace a konfigurace SPLUNK SIEM může být složitá a vyžadovat pokročilé technické znalosti. To může znamenat, že nasazení může trvat delší dobu.

Vysoké požadavky na hardware: Pro optimální výkon a škálovatelnost je zapotřebí výkonný hardware, což může zvýšit náklady na infrastrukturu a provoz.

Náročná správa a údržba: Pro udržení optimálního provozu je nutná pravidelná správa a údržba platformy, což může vyžadovat vysoký stupeň odborných znalostí a časovou investici.

Omezená podpora: Podpora ze strany SPLUNK může být omezená nebo nákladná, což může vést k potížím při řešení problémů a otázek.

Vysoký objem dat: Pokud není infrastruktura správně dimenzována, může SPLUNK produkovat velké množství dat, což může ztížit analýzu a reakci na bezpečnostní hrozby.

Komplexní uživatelské rozhraní: Uživatelské rozhraní SPLUNK SIEM může být složité a nepřehledné, což může zvyšovat náročnost práce uživatelům.

Závislost na dostupnosti internetu: Platforma může vyžadovat neustálé připojení k internetu, což může být omezující v prostředích s omezenou konektivitou. (Splunk)

3.3.1.2 **Graylog SIEM**

Graylog je open-source platforma pro sběr, analýzu a vizualizaci logovacích dat a událostí. Ačkoli není přímo označován za SIEM (Security Information and Event Management), mnoho organizací využívá Graylog k implementaci funkcí SIEM díky jeho schopnostem zpracování událostí a analýzy logů. Stručný popis Graylogu:

Funkce Graylog SIEM

Sběr logů: Graylog umožňuje sběr logů z různých zdrojů, včetně serverů, aplikací, zařízení sítě a dalších.

Indexace a ukládání dat: Data jsou indexována a ukládána pro rychlý a efektivní přístup a vyhledávání.

Analýza logů: Platforma umožňuje provádět rozsáhlé analýzy logovacích dat, identifikovat vzory a anomálie a zlepšit detekci hrozeb.

Vyhledávání a dotazování: Uživatelé mohou snadno vyhledávat a dotazovat data pomocí robustního dotazovacího jazyka a nástrojů pro vyhledávání.

Vizualizace dat: Graylog poskytuje možnosti vizualizace dat prostřednictvím interaktivních grafů, dashboardů a reportů, což umožňuje rychlou identifikaci trendů a anomálií.

Alerting: Uživatelé mohou nastavit upozornění a alarmy na základě určitých podmínek, což umožňuje rychlou reakci na bezpečnostní incidenty.

Integrace: Platforma podporuje integraci s dalšími bezpečnostními nástroji a platformami, což umožňuje komplexní bezpečnostní řešení.

Autentizace a autorizace: Graylog umožňuje správu uživatelů, rolí a přístupových práv, což zajišťuje bezpečný přístup k datům a funkcím platformy.

Auditní logy: Systém zaznamenává všechny změny a akce provedené uživateli, což umožňuje sledování a auditování činností.

Rozšiřitelnost: Graylog je rozšiřitelný pomocí různých doplňků a integrací, což umožňuje přizpůsobení platformy konkrétním potřebám organizace.

Nevýhody Graylog SIEM

Složitost implementace: Implementace Graylogu může být náročná, zejména pro organizace s menším technickým zázemím. Konfigurace a správa mohou vyžadovat znalosti z oblasti IT infrastruktury a bezpečnostních postupů.

Potřeba správy a údržby: Pro udržení optimálního provozu Graylogu je zapotřebí pravidelná správa a údržba. To může zahrnovat aktualizace, ladění výkonu a řešení problémů.

Školení personálu: Efektivní využití Graylogu vyžaduje, aby personál měl vhodné znalosti a dovednosti. Školení zaměstnanců může být nákladné a časově náročné.

Nároky na hardware a infrastrukturu: Pro provoz Graylogu je nutné mít dostatečně výkonný hardware a vhodně navrženou infrastrukturu. To může zvýšit náklady na pořízení a provoz.

Omezená podpora: I když existuje rozsáhlá komunita uživatelů Graylogu, profesionální podpora může být omezená v porovnání s komerčními SIEM řešeními.

Nedostatečné pokročilé funkce: V některých případech může Graylog postrádat některé pokročilé funkce, které jsou k dispozici v komerčních SIEM platformách.

Příklady funkcí které graylog neobsahuje:

- **Uživatelské a entity behavior analýza (UEBA)**: Tato funkce umožňuje identifikovat podezřelé chování uživatelů a dalších entit na základě vzorů a anomálií v jejich aktivitách a interakcích s informačními systémy.
- **Detekce pokročilých hrozeb (Advanced Threat Detection)**: Některá komerční SIEM řešení mají pokročilé algoritmy pro detekci složitých a pokročilých hrozeb, které mohou využívat strojové učení nebo umělou inteligenci.
- **Integrované nástroje pro reakci a správu incidentů**: Některé SIEM platformy nabízejí integrované nástroje pro správu bezpečnostních incidentů, které umožňují rychlou a koordinovanou reakci na bezpečnostní události.
- **Forenzní analýza**: Pokročilá forenzní analýza může být klíčová pro důkladné vyšetření bezpečnostních incidentů a identifikaci původu útoků. Některé SIEM platformy nabízejí rozšířené funkce pro forenzní analýzu.
- **Compliance Managemen**t: Funkce pro správu souladu a dodržování předpisů a standardů může být klíčová pro organizace působící v regulovaných odvětvích. Některé SIEM platformy mají vestavěné nástroje pro správu souladu.
- **Threat Intelligence Integration**: Některé komerční SIEM platformy poskytují integraci s hrozbami z bezpečnostních informačních zdrojů (threat intelligence feeds), což umožňuje lepší detekci známých hrozeb.
- **Podpora pro IoT a OT prostředí**: Vzhledem k rostoucímu využívání Internetu věcí (IoT) a operačních technologií (OT) může být podpora pro tyto prostředí

klíčová. Některé SIEM platformy mají specializované funkce pro monitorování a zabezpečení těchto prostředí.

Bezpečnostní rizika: Jakékoli IT řešení představuje potenciální riziko z hlediska bezpečnosti. Neodborně nakonfigurovaný Graylog může být zranitelný vůči útokům nebo zneužití.

Závislost na komunitě: Vývoj a podpora Graylogu jsou zčásti závislé na komunitě. To může znamenat, že některé funkce nebo problémy nemusí být rychle adresovány. (Graylog)

3.3.1.3 NetWitness SIEM

NetWitness SIEM je komplexní bezpečnostní platforma, která kombinuje detekci hrozeb, analýzu událostí, správu incidentů a reakci na bezpečnostní incidenty v jednom integrovaném řešení.

Funkce NetWitness SIEM

Sběr událostí a dat: Platforma sbírá události a data z různých zdrojů, včetně logů, síťového provozu, endpointů a cloudových služeb.

Analýza událostí: NetWitness SIEM provádí pokročilou analýzu událostí a dat, aby identifikoval podezřelé vzory a chování, které mohou naznačovat bezpečnostní hrozby.

Detekce hrozeb: Platforma využívá pokročilé techniky detekce hrozeb, včetně pravidel, strojového učení a threat intelligence, k identifikaci známých i neznámých hrozeb.

Integrovaná správa incidentů: NetWitness SIEM umožňuje efektivní správu bezpečnostních incidentů, včetně dokumentace událostí, sledování stavu incidentů a koordinace odpovědi týmu.

Rychlá reakce na incidenty: Platforma poskytuje nástroje pro rychlou identifikaci, analýzu a řešení bezpečnostních incidentů, včetně možnosti automatizace odpovědí na incidenty.

Vizualizace a reporting: NetWitness SIEM nabízí možnosti vizualizace dat a generování reportů pro sledování bezpečnostní situace a prezentaci výsledků analýz.

Integrace: Platforma je schopna integrovat se širokou škálou dalších bezpečnostních nástrojů a systémů, což umožňuje komplexní a integrované bezpečnostní řešení.

Compliance: NetWitness SIEM podporuje správu souladu s předpisy a standardy, včetně možnosti generování auditních reportů a sledování dodržování bezpečnostních předpisů.

Nevýhody NetWitness SIEM

Vysoké náklady: Implementace a provoz platformy NetWitness SIEM může být finančně náročná, zejména pro menší organizace s omezeným rozpočtem.

Složitost implementace: Instalace a konfigurace NetWitness SIEM může být složitá a vyžadovat pokročilé technické znalosti. To může znamenat, že nasazení může trvat delší dobu.

Náročná správa a údržba: Pro udržení optimálního provozu je zapotřebí pravidelná správa a údržba, což může vyžadovat znalosti z oblasti IT infrastruktury a bezpečnostních postupů.

Potřeba školení personálu: Efektivní využití NetWitness SIEM vyžaduje, aby personál měl vhodné znalosti a dovednosti. Školení zaměstnanců může být nákladné a časově náročné.

Vysoká míra komplexity: Platforma může být velmi komplexní a obsáhlá, což může způsobit potíže při používání a porozumění všem funkcím a možnostem.

Omezená podpora: I když platforma může nabízet podporu, může být omezená v porovnání s jinými SIEM řešeními nebo komerčními poskytovateli podpory.

Závislost na dostupnosti internetu: Pokud je síťové připojení nedostupné, může to omezit nebo znemožnit přístup k některým funkcím platformy.

Sklon ke zbytečnému generování falešných pozitivních výsledků: Pokud není správně nakonfigurován, může NetWitness SIEM generovat mnoho falešně pozitivních výsledků, což může zvyšovat časové nároky na analýzu a reakci na bezpečnostní události. (NetWitness)

3.3.1.4 ArcSight SIEM

ArcSight SIEM je integrovaná platforma pro správu informací a událostí v oblasti bezpečnosti, která poskytuje organizacím nástroje pro sběr, analýzu, monitorování a reakci na bezpečnostní události a hrozby

ArcSight má také vlastní SOAR (Security Orchestration, Automation, and Response), které umožňuje bezpečnostním týmům automatizaci, playbooky, incident management a SOC (Security Operations Center) analýzy a mnoho dalších. (Microfocus)

Funkce ArcSight SIEM

Detekce hrozeb: Platforma poskytuje nástroje pro detekci hrozeb a anomálií pomocí pravidel, strojového učení a threat intelligence, což umožňuje organizacím identifikovat potenciální rizika a bezpečnostní incidenty.

Normalizace a kategorizace událostí: ArcSight SIEM sbírá, normalizuje a kategorizuje veškeré události z bezpečnostních zařízení a sítě pro lepší viditelnost a analýzu hrozeb

Uložení dat a jejich prohledávání: ArcSight Logger umožňuje automatizované hlášení souladu a správu logů s kapacitou uložení až 42TB dat. (S, 2023)

Správa incidentů: ArcSight SIEM umožňuje správu bezpečnostních incidentů včetně dokumentace událostí, sledování stavu incidentů, koordinace odpovědi týmu a postupů pro řešení incidentů.

Vizualizace a reporting: Platforma poskytuje možnosti vizualizace dat a generování reportů pro sledování bezpečnostní situace, prezentaci výsledků analýz a dodržování compliance.

Integrace: ArcSight SIEM je schopen integrovat se širokou škálou dalších bezpečnostních nástrojů a systémů, což umožňuje komplexní a integrované bezpečnostní řešení.

Compliance: Platforma podporuje správu souladu s předpisy a standardy, včetně možnosti generování auditních reportů a sledování dodržování bezpečnostních předpisů.
Škálovatelnost a výkon: ArcSight SIEM je navržen tak, aby zvládal zpracování velkých objemů dat a událostí, což umožňuje organizacím monitorovat a chránit své prostředí bezpečnostních událostí rychle a efektivně.

Nevýhody ArcSight SIEM

Vysoké náklady: ArcSight SIEM může být finančně náročným řešením, jak z hlediska licenčních poplatků, tak i nákladů na implementaci, školení personálu a údržbu.

Složitost implementace a konfigurace: Implementace ArcSight SIEM může být složitá a vyžaduje pokročilé technické znalosti. Konfigurace a ladění mohou vyžadovat čas a odborné know-how.

Náročná správa a údržba: Pro udržení optimálního provozu je nutná pravidelná správa a údržba platformy, což může vyžadovat vysoký stupeň odborných znalostí a časovou investici.

Potřeba školení personálu: Efektivní využití ArcSight SIEM vyžaduje, aby personál měl vhodné znalosti a dovednosti. Školení zaměstnanců může být nákladné a časově náročné.

Komplexní uživatelské rozhraní: Uživatelské rozhraní ArcSight SIEM může být složité a nepřehledné, což může ztížit práci uživatelům a zvýšit čas potřebný k naučení se používat platformu.

Omezená podpora: Podpora ze strany poskytovatele může být omezená nebo nákladná, což může vést k potížím při řešení problémů a otázek.

Výkonové požadavky: Pro provoz ArcSight SIEM je zapotřebí dostatečně výkonného hardwaru a infrastruktury, což může zvýšit náklady na pořízení a provoz.

Závislost na dostupnosti internetu: Platforma může vyžadovat neustálé připojení k internetu, což může být omezující v prostředích s omezenou konektivitou.

Zpracování falešně pozitivních událostí: Pokud není správně nakonfigurována, může ArcSight SIEM generovat mnoho falešně pozitivních výsledků, což může zvýšit pracovní zátěž týmu zodpovědného za správu bezpečnosti. (Microfocus)

3.3.1.5 **LogRythm SIEM**

LogRhythm SIEM je integrovaná platforma pro správu informací a událostí v oblasti bezpečnosti (SIEM), která umožňuje organizacím sběr, analýzu, monitorování a reakci na bezpečnostní události a hrozby.

LogRhythm SIEM zahrnuje technologie UEBA (User and Entity Behavior Analytics), SOAR (Security Orchestration, Automation and Response) a NDR (Network Detection and Response), které pomáhají v detekci a odpovědi na útoky a zlepšení bezpečnosti sítě.

Funkce LogRythm SIEM

Sběr a normalizace událostí: LogRhythm SIEM umožňuje sběr a normalizaci událostí a dat z různých zdrojů, včetně logů, síťového provozu, aplikací a endpointů.

Detekce hrozeb: Platforma poskytuje pokročilé techniky detekce hrozeb a anomálií, včetně pravidel, strojového učení a threat intelligence, což umožňuje identifikaci podezřelých aktivit a potenciálních bezpečnostních incidentů.

Analýza událostí: LogRhythm SIEM provádí analýzu událostí a dat, aby identifikoval podezřelé vzory a chování, což umožňuje organizacím reagovat na bezpečnostní události včas.

UEBA (User and Entity Behavior Analytics): Tato technologie pomáhá v detekci a odpovědi na útoky, analýze chování uživatelů a entit a zlepšení bezpečnosti sítě.

SOAR (Security Orchestration, Automation and Response): Tato technologie umožňuje automatizaci a orchestraci bezpečnostních procesů, čímž se zlepšuje rychlost a efektivita odpovědí na útoky.

NDR (Network Detection and Response): Tato technologie umožňuje detekci a odpověď na útoky na síti, analýzu sítě a zlepšení bezpečnosti sítě.

Vizualizace a reporting: LogRhythm SIEM nabízí možnosti vizualizace dat a generování reportů pro sledování bezpečnostní situace, prezentaci výsledků analýz a dodržování compliance.

Compliance: LogRhythm SIEM podporuje správu souladu s předpisy a standardy, včetně možnosti generování auditních reportů a sledování dodržování bezpečnostních předpisů.

Nevýhody LogRythm SIEM

Vysoké náklady: Implementace a provoz LogRhythm SIEM může být finančně náročná, zejména pro menší organizace s omezeným rozpočtem.

Složitost implementace: Instalace a konfigurace LogRhythm SIEM může být složitá a vyžadovat pokročilé technické znalosti. To může znamenat, že nasazení může trvat delší dobu.

Náročná správa a údržba: Pro udržení optimálního provozu je nutná pravidelná správa a údržba platformy, což může vyžadovat vysoký stupeň odborných znalostí a časovou investici.

Potřeba školení personálu: Efektivní využití LogRhythm SIEM vyžaduje, aby personál měl vhodné znalosti a dovednosti. Školení zaměstnanců může být nákladné a časově náročné.

Komplexní uživatelské rozhraní: Uživatelské rozhraní LogRhythm SIEM může být složité a nepřehledné, což může ztížit práci uživatelům a zvýšit čas potřebný k naučení se používat platformu.

Omezená podpora: Podpora ze strany poskytovatele může být omezená nebo nákladná, což může vést k potížím při řešení problémů a otázek.

Výkonové požadavky: Pro provoz LogRhythm SIEM je zapotřebí dostatečně výkonného hardwaru a infrastruktury, což může zvýšit náklady na pořízení a provoz.

Závislost na dostupnosti internetu: Platforma může vyžadovat neustálé připojení k internetu, což může být omezující v prostředích s omezenou konektivitou.

Možnost falešně pozitivních událostí: Neadekvátní konfigurace může vést k nadměrnému generování falešně pozitivních událostí, což může zvyšovat časové nároky na analýzu a reakci na bezpečnostní události. (LogRythm)

3.3.1.6 IBM Qradar SIEM

IBM QRadar SIEM je komplexní platforma pro správu informací a událostí v oblasti bezpečnosti, která poskytuje organizacím nástroje pro sběr, analýzu, monitorování a reakci na bezpečnostní události a hrozby.

Funkce IBM Qradar SIEM

Sběr událostí: QRadar umožňuje sběr a agregaci událostí z různých zdrojů, včetně logů, síťového provozu, aplikací a bezpečnostních zařízení.

Detekce hrozeb: Platforma poskytuje pokročilé nástroje pro detekci hrozeb a anomálií, včetně pravidel, analýzy behaviorálních vzorů a využití threat intelligence.

Korelace událostí: QRadar umožňuje korelaci událostí z různých zdrojů a kontextů, což umožňuje identifikovat související události a potenciální hrozby.

Analýza událostí: Platforma provádí hloubkovou analýzu událostí a dat, aby identifikovala podezřelé aktivity a pomohla organizacím lépe porozumět bezpečnostnímu stavu svých sítí.

Správa incidentů: QRadar poskytuje nástroje pro správu bezpečnostních incidentů, včetně prioritizace, dokumentace a sledování stavu incidentů.

Vizualizace a reporting: Platforma nabízí vizualizaci dat a generování reportů, což umožňuje sledovat bezpečnostní události a prezentovat výsledky analýz.

Integrace: QRadar je schopen integrovat se širokou škálou dalších bezpečnostních nástrojů a systémů, což umožňuje komplexní a integrované bezpečnostní řešení.

Compliance: Platforma podporuje správu souladu s předpisy a standardy, včetně generování auditních reportů a sledování dodržování bezpečnostních předpisů.

Automatizace a orchestrace: QRadar umožňuje automatizaci a orchestraci bezpečnostních operací a odpovědí na incidenty, což zvyšuje efektivitu a rychlost reakce na bezpečnostní události.

Nevýhody IBM Qradar SIEM

Vysoké náklady: Implementace a provoz IBM QRadar SIEM může být finančně náročný, zejména pro menší organizace s omezeným rozpočtem. Licenční poplatky, školení personálu a infrastrukturní náklady mohou být vysoké.

Složitá implementace: Instalace a konfigurace IBM QRadar SIEM může být složitá a vyžadovat pokročilé technické znalosti. To může znamenat, že nasazení může trvat delší dobu.

Vysoké požadavky na hardware: Pro optimální výkon a škálovatelnost je zapotřebí výkonný hardware, což může zvýšit náklady na infrastrukturu a provoz.

Náročná správa a údržba: Pro udržení optimálního provozu je nutná pravidelná správa a údržba platformy, což může vyžadovat vysoký stupeň odborných znalostí a časovou investici.

Omezená podpora: Podpora ze strany IBM může být omezená nebo nákladná, což může vést k potížím při řešení problémů a otázek.

Vysoký objem událostí: Pokud není infrastruktura správně dimenzována, může QRadar produkovat velké množství událostí, což může ztížit analýzu a reakci na skutečné bezpečnostní hrozby.

Komplexní uživatelské rozhraní: Uživatelské rozhraní IBM QRadar SIEM může být složité a nepřehledné, což může zvyšovat náročnost práce uživatelům.

Závislost na dostupnosti internetu: Platforma může vyžadovat neustálé připojení k internetu, což může být omezující v prostředích s omezenou konektivitou.

Nedostatečná integrace: I přes schopnost integrace s dalšími nástroji může být integrace s některými specifickými systémy nebo aplikacemi obtížná. (IBM)

Obecné předpoklady SIEM systému

Na základě průzkumu SIEM systémů lze konstatovat, že nejen zde porovnané systémy mají v základu stejný předpoklad funkcí, výhod a nevýhod a odlišují je především jednotlivé nadstandardní funkce a cena, která pro firmy hraje častokrát nejvyšší roli.

3.4 Postupy pro implementaci bezpečnostních systémů

3.4.1 Analýza struktury informačních systémů

Proces začíná úvodní analýzou struktury informačních systémů v organizaci (firmě), kde je plánováno bezpečnostní systémy nasadit. Na základě analýzy tohoto problému byly identifikovány následující vhodné kroky analýzy informačních systémů.

Identifikace aktiv a kritických informací: Zjištění, jaké jsou hlavní aktiva a kritické informace ve firmě, jako jsou databáze zákazníků, obchodní tajemství, finanční informace a další. Určení, co je pro firmu nejcennější, pomůže určit priority v bezpečnosti.

Posouzení hrozeb a zranitelností: Analýza existujících hrozeb a zranitelností, kterým je firma vystavena. To zahrnuje možné útočníky, typy útoků a slabá místa v síti, aplikacích a procesech.

Hodnocení současných bezpečnostních opatření: Zhodnocení aktuálních bezpečnostních opatření a postupů, které firma používá. To zahrnuje firewally, antivirové programy, šifrování, autentizaci a další.

Posouzení právních a regulačních požadavků: Zjištění, jaké jsou právní a regulační požadavky v oblasti kybernetické bezpečnosti pro daný sektor nebo jurisdikci. Například GDPR v Evropě nebo HIPAA v oblasti zdravotnictví v USA.

Analýza lidských zdrojů: Zohlednění lidského faktoru ve firmě. To zahrnuje školení zaměstnanců v oblasti bezpečnosti, politiky přístupu k informacím, pravidla pro vytváření silných hesel a další.

Stanovení bezpečnostních cílů: Definování konkrétních cílů, kterých chce firma dosáhnout implementací kybernetického bezpečnostního systému. Tyto cíle by měly být měřitelné a zaměřené na ochranu důležitých aktiv a minimalizaci rizik.

Zhodnocení finančních zdrojů: Posouzení dostupných finančních prostředků a zdrojů, které jsou k dispozici pro implementaci bezpečnostních opatření. To pomůže určit rozpočet a prioritizovat investice v bezpečnosti.

Riziková analýza: Provedení rizikové analýzy, která identifikuje hlavní rizika a jejich potenciální dopady na firmu. To pomůže prioritizovat bezpečnostní opatření a plánovat strategie pro jejich řízení.

3.4.2 Navržení bezpečnostní architektury

Po analýze následuje krok navržení bezpečnostní architektury, která bude odpovídat potřebám a požadavkům firmy. Jednotlivými kroky návrhu bezpečnostní architektury jsou:

Perimetrická ochrana: Navržení strategie ochrany perimetru sítě pomocí firewallů, brán VPN, ochranných zařízení pro přenos dat a dalších technologií. Zabezpečení externího přístupu je klíčové pro ochranu interních systémů.

Segmentace sítě: Rozdělení sítě na logické segmenty s různými úrovněmi důvěryhodnosti a přístupovými právy. To pomůže minimalizovat šíření útoků a zvýší odolnost sítě.

Šifrování: Zahrnutí šifrování dat do architektury, zejména pro přenos citlivých informací přes veřejné sítě nebo ukládání dat na disk. To zabezpečí citlivé informace před neoprávněným přístupem.

Ochrana proti malwaru: Zahrnutí antivirových programů, antimalwarové brány a dalších nástrojů pro detekci a odstraňování malwaru ze sítě a systémů.

Správa identit a přístupu: Implementování správy identit a přístupu (IAM) pro efektivní správu uživatelských účtů, oprávnění a autentizaci. To pomůže minimalizovat riziko neoprávněného přístupu k citlivým datům.

Monitorování a detekce: Zahrnutí systémů monitorování a detekce útoků (IDS/IPS), které sledují síťový provoz a identifikují podezřelé aktivity nebo anomálie. To umožní rychlou reakci na potenciální hrozby.

Zálohování a obnova dat: Navrhnutí strategie zálohování a obnovy dat, která zabezpečí, že citlivé informace budou chráněny a zároveň budou k dispozici v případě potřeby obnovení po havárii nebo útoku.

Ochrana koncových zařízení: Zahrnutí ochrany koncových zařízení pomocí antivirových programů, osobních firewallů, správy mobilních zařízení (MDM) a dalších technologií. Koncová zařízení jsou často cílem útoků a jejich ochrana je klíčová.

Odpověď na incidenty: Navrhnutí plánu pro reakci na incidenty (IRP), který určí postupy pro identifikaci, hodnocení a reakci na bezpečnostní incidenty. To zahrnuje také plán komunikace s interními a externími zúčastněnými stranami.

Pravidelní revize a aktualizace: Zahrnutí pravidel a postupů pro pravidelnou revizi a aktualizaci bezpečnostní architektury, aby byla odpovídajícím způsobem chráněna vaše firma před novými hrozbami a zranitelnostmi.

3.4.3 Výběr bezpečnostních nástrojů

Následuje krok výběru bezpečnostních nástrojů a technologií. Zde je doporučeno postupovat následovně:

Průzkum trhu: Provedená průzkumu trhu a vyhledání různé bezpečnostních nástrojů a technologií, které splňují potřeby a požadavky firmy. Existuje mnoho různých poskytovatelů a produktů na trhu, které nabízejí širokou škálu funkcí a možností.

Vyhodnocení funkcí a vlastností: Pečlivé vyhodnocení funkcí a vlastností jednotlivých bezpečnostních nástrojů a technologií vzhledem k potřebám firmy. Zvážení jejich schopnosti detekce hrozeb, výkonu, možností konfigurace a integrace s existujícími systémy.

Porovnání nákladů: Porovnání nákladů spojenými s jednotlivými bezpečnostními nástroji a technologiemi vzhledem k jejich funkčnosti a výhodám. Ujištění se, že zvolené nástroje a technologie jsou cenově dostupné a ve shodě s rozpočtem firmy.

Zohlednění bezpečnostních standardů: Zajištění, že vybrané bezpečnostní nástroje a technologie splňují příslušné bezpečnostní standardy a požadavky, které jsou pro průmysl

nebo jurisdikci relevantní. To může zahrnovat například standardy ISO 27001, NIST nebo další.

Zkoušení a hodnocení: Vyhledání možnosti vyzkoušení a vyhodnocení vybraných bezpečnostních nástrojů a technologií, k získání zkušenosti s jejich funkcionalitou a efektivitou. To může zahrnovat bezplatné zkušební verze, demoverze nebo referenční příběhy zákazníků.

3.4.4 Implementace bezpečnostních systémů

Po zvolení vhodných bezpečnostních systémů přichází na řadu jejich implementace

Rozvrh implementace: Vytvoření časového rozvrhu implementace, který obsahuje stanovení konkrétních termínů pro jednotlivé fáze a aktivity implementace. Zvažte realistické časové odhady a přizpůsobte rozvrh podle potřeb a omezení firmy.

Zodpovědnosti a role: Určená zodpovědností a rolí jednotlivých členů týmu, kteří budou zapojeni do implementace bezpečnostních systémů. Jasné definování, kdo je odpovědný za jednotlivé úkoly a rozhodování.

Detailní kroky a postupy: Detailní popsání kroků a postupů, které budou použity k implementaci jednotlivých bezpečnostních opatření. To zahrnuje instalaci a konfiguraci hardware a software, nastavení politik a pravidel, a další,

Instalace bezpečnostních systémů: Hardware, jako jsou firewally, routery, IPS/IDS zařízení apod., je třeba je fyzicky nainstalovat do sítě a zapojit je do elektrického proudu. Následuje instalace potřebného softwaru pro správu a konfiguraci bezpečnostních zařízení. To může zahrnovat operační systémy, správcovské konzole, antivirové programy, firewally a další dle zvoleného řešení. Po instalaci softwaru je třeba provést konfiguraci bezpečnostních zařízení podle stanovených bezpečnostních politik a požadavků firmy. To zahrnuje nastavení síťových pravidel, ochranných mechanismů, autentizačních metod a dalších.

3.4.5 Ověření bezpečnostních systémů

Poté přichází na řadu otestování a ověření nainstalovaných bezpečnostních systémů:

Plánování testování: Nejprve je důležité plánovat testování a stanovit jasný cíl a rozsah testů. Identifikování důležitých funkcí a vlastností systému, které budou testovány, a určení, kdo bude provádět testování a jaké nástroje budou použity.

Provedení testů funkcionality: Testování by mělo zahrnovat ověření funkcionality jednotlivých komponent bezpečnostního systému, jako jsou firewall, antivirový software, systémy detekce a prevence útoků (IDS/IPS), a další. To zahrnuje ověření, zda systémy správně blokují nežádoucí provoz, detekují a oznamují potenciální hrozby a další.

Testování výkonu: Testování výkonu má za cíl zjistit, jak efektivně systém zpracovává zátěž a reaguje na různé podmínky provozu. To může zahrnovat testování rychlosti a spolehlivosti detekce, odezvy na přenos dat a další.

Testování zranitelností: Provedení testování zranitelností k identifikaci potenciálních slabých míst a nedostatků v bezpečnostním systému. To může zahrnovat skenování síťových zařízení, webových aplikací a dalších systémů na nalezení možných bezpečnostních chyb.

Simulace útoků: Simulujte různé typy útoků a scénářů, abyste ověřili, jak dobře váš bezpečnostní systém dokáže reagovat na hrozby a útoky v reálném čase. To může zahrnovat simulaci útoků jako je phishing, ransomware, útoky na aplikace a další.

Hodnocení výsledků: Po dokončení testování zhodnocení výsledků a identifikace případných nedostatků a slabin v bezpečnostním systému. Priotizování zjištěných problémů a určení, jaké kroky budou podniknuty k jejich řešení.

Revize a aktualizace: Na základě výsledků testování provedení případných úprav a aktualizací v bezpečnostním systému. To může zahrnovat úpravy konfigurace, instalaci aktualizací a další.

Dokumentace: Ujištění se, že všechny výsledky testování a provedené úpravy jsou důkladně zdokumentovány pro budoucí referenci a revize. To zahrnuje záznamy o testech, zjištěných chybách, provedených změnách a další.

3.4.6 Školení zaměstnanců

Následujícím krokem je proškolení zaměstnanců, kteří s novými systémy budou pracovat.

Identifikace školicích potřeb: Identifikování specifické školicí potřeby zaměstnanců v oblasti kybernetické bezpečnosti. Zvážení jejich úroveň znalostí a dovedností v této oblasti a zaměření se na klíčové oblasti, které je třeba pokrýt.

Plánování školení: Vytvoření plánu školení, který určuje obsah, formát a rozsah školení. Zvážení různých metod školení, jako jsou prezentace, workshopy, online kurzy, simulace útoků a další.

Zajištění školicích zdrojů: Zajištění potřebných zdrojů a materiálů pro školení zaměstnanců, včetně vzdělávacích materiálů, prezentací, testovacích scénářů a dalších.

Vzdělávání o bezpečnostních hrozbách: Poskytnutí zaměstnancům školení o různých typech kybernetických hrozeb, jako jsou phishing, malware, útoky na sociální inženýrství a další. Vysvětlení zaměstnancům, jak tyto hrozby fungují a jak se jim vyhnout.

Osvědčené postupy a politiky: Seznámení zaměstnanců s osvědčenými postupy a interními bezpečnostními politikami, které platí ve firmě. To zahrnuje pravidla pro vytváření silných hesel, politiky přístupu k datům, postupy pro zálohování a šifrování dat a další.

Používání bezpečnostních nástrojů: Učená zaměstnanců, jak správně používat instalované bezpečnostní nástroje a technologie, jako jsou antivirové programy, firewally, systémy detekce a prevence útoků a další. Poskytnutí jim praktických návodů a instrukcí pro správné používání těchto nástrojů.

Simulace a cvičení: Provádění simulací a cvičení, která umožní zaměstnancům praktické procvičení svých dovedností v oblasti kybernetické bezpečnosti. To může zahrnovat simulace útoků, falešné phishingové kampaně, testy vědomostí a další.

Evaluace a zpětná vazba: Po skončení školení provádění evaluaci úspěšnosti školení a získávání zpětné vazby od zaměstnanců. To umožní zhodnotit úroveň pochopení a připravenosti zaměstnanců v oblasti kybernetické bezpečnosti a případně upravit budoucí školicí programy.

3.4.7 **Monitorování a správa**

Po těchto krocích přichází konečně jejich funkce monitorování a správy. Tento proces probíhá takto:

Sledování síťového provozu: Používají se specializované nástroje pro sledování síťového provozu a monitorování aktivit v síti. Tyto nástroje zaznamenávají a analyzují provoz, který prochází sítí, a identifikují podezřelé nebo neobvyklé aktivity.

Detekce bezpečnostních incidentů: S pomocí systémů detekce a prevence útoků (IDS/IPS), správních systémů bezpečnostních událostí (SIEM) a dalších nástrojů se sledují a detekují možné bezpečnostní incidenty, jako jsou pokusy o neoprávněný přístup, malware, phishing a další.

Analýza a vyhodnocení: Detekované bezpečnostní události jsou analyzovány a vyhodnoceny z hlediska jejich závažnosti a potenciálního dopadu na bezpečnostní postavení firmy. To zahrnuje ověření a klasifikaci událostí, aby bylo možné určit, zda se jedná o skutečný bezpečnostní incident.

Reakce na incidenty: Pokud je detekován bezpečnostní incident, provádí se rychlá reakce na jeho potlačení a minimalizaci škod. To může zahrnovat izolaci postižených systémů, blokování útočníků, obnovu dat ze záloh a další opatření podle definovaného bezpečnostního plánu.

3.4.8 **Revize a aktualizace**

Posledním krokem implementace bezpečnostních systémů je pak jejich pravidelná revize a aktualizace. To je prováděno následovně:

Plánování revizí: Stanovení pravidelného plánu revizí a aktualizací, který definuje frekvenci a rozsah revizí. Plán by měl zahrnovat hodnocení bezpečnostních postupů, procesů a technologií, včetně plánů reakce na incidenty, politik a procedur.

Sběr dat a informací: Sběr relevantních dat a informací, které budou použity k hodnocení kybernetického bezpečnostního prostředí firmy. To může zahrnovat záznamy o bezpečnostních událostech, výsledky externích auditů, informace o nových hrozbách a zranitelnostech, a zpětnou vazbu od zaměstnanců a dalších zúčastněných stran.

Analýza výsledků: Provedení důkladné analýzy získaných dat a informací k identifikaci případných nedostatků, oblastí pro zlepšení a potřeby aktualizací. Zaměření se na klíčové oblasti, jako jsou zranitelnosti, bezpečnostní politiky, postupy reakce na incidenty a aktualizace softwaru a hardwaru.

Identifikace opatření: Na základě analýzy identifikování konkrétních opatření a kroků, které budou přijaty k zlepšení kybernetické bezpečnosti firmy. To může zahrnovat aktualizace politik a procedur, implementaci nových bezpečnostních nástrojů a technologií, dodatečné školení zaměstnanců a další.

Implementace změn: Implementace identifikovaných změn a aktualizací v souladu s definovanými postupy a plánem. Ujištění se, že změny jsou pečlivě otestovány a dokumentovány před jejich nasazením do produkčního prostředí.

Školení zaměstnanců: Poskytnutí školení zaměstnancům o nových bezpečnostních postupech, politikách a technologiích, které byly implementovány jako součást revizí a aktualizací. Ujištění se, že zaměstnanci jsou se změnami plně obeznámeni a schopni je efektivně využívat.

Monitorování a zpětná vazba: Monitorování dopadů provedených změn a získání zpětné vazby od zaměstnanců a dalších zúčastněných stran. Ujištění se, že změny dosahují očekávaných výsledků a případné upravení postupů podle zjištěných potřeb.

Průběžná revize a aktualizace: Průběžné revidování a aktualizování bezpečnostních postupů, procesů a technologií v souladu s novými hrozbami, změnami v prostředí firmy a zkušenostmi získanými během provozu. Udržování tohoto procesu jako kontinuální cyklus, který umožňuje neustálé zlepšování kybernetické bezpečnosti firmy.

3.5 Zhodnocení nákladů a očekávaných výnosů

Posouzení nákladů a předpokládaných výnosů v oblasti kyberbezpečnosti je klíčovým faktorem pro efektivní správu bezpečnosti informačních technologií v organizaci. Tento proces umožňuje identifikovat investice do bezpečnostních opatření, které přinášejí optimální hodnotu a ochranu před kybernetickými hrozbami.

Náklady spojené s kyberbezpečností zahrnují investice do fyzického a softwarového vybavení, školení zaměstnanců, monitorovacích nástrojů a dalších bezpečnostních opatření. Je nutné zohlednit nejenom počáteční náklady, ale i provozní a údržbové náklady systémů.

Očekávané výnosy spojené s investicemi do kyberbezpečnosti zahrnují snížení rizika kybernetických útoků, ochranu citlivých informací, udržení důvěryhodnosti a reputace organizace a minimalizaci finančních ztrát způsobených kybernetickými incidenty. Důležité je též zohlednit potenciální výnosy z dodržování regulačních požadavků a normativních standardů.

3.6 Posouzení souvislosti mezi bezpečností a produktivitou

Vztah mezi bezpečností a produktivitou v kybernetických systémech představuje klíčovou souvislost v dnešní digitální krajině. Ochranná opatření a bezpečnostní strategie sehrávají klíčovou úlohu při ochraně informací, sítí a systémů před kybernetickými hrozbami, ale jejich implementace může mít výrazný dopad na efektivitu pracovních procesů. Zajištění bezpečnosti vyžaduje čas a investice, což může potenciálně ovlivnit pracovní výkonnost. Používání silných šifrovacích algoritmů, pravidelné aktualizace softwaru, školení zaměstnanců a monitorování bezpečnostních incidentů mohou vyžadovat od pracovníků dodatečné úsilí a čas.

Naopak, kvalitní kybernetická bezpečnost může podporovat produktivitu tím, že minimalizuje riziko přerušení provozu způsobeného kybernetickými útoky. Bezpečné prostředí umožňuje organizaci zaměřit se na své podnikání a inovace bez obav o ztrátu citlivých informací, které by mohly narušit konkurenceschopnost a obchodní kontinuitu.

Vyvážený přístup k řízení bezpečnosti a produktivity je klíčem k úspěchu v kybernetickém prostředí. To zahrnuje nejen technologická opatření, ale také budování bezpečnostní kultury a vhodných politik. Cílem je dosáhnout synergického efektu, kde bezpečnost podporuje produktivitu a naopak, což nakonec posiluje celkový výkon organizace v digitální éře.

4 Vlastní práce

4.1 Vytvoření a analýza firmy

Pro praktickou část jsem se rozhodl si vytvořit příkladovou firmu, která poslouží jako objednavatel zřízení bezpečnostních systémů.

4.1.1 Vytvoření firmy

Popis firmy: XYZ je malá právnická firma specializující se na poskytování právních služeb pro jednotlivce i malé podniky. Jejich právníci mají bohaté zkušenosti v různých právních oblastech a poskytují klientům individuální a profesionální péči.

Oblast činnosti: Poskytování právních služeb, poradenství v oblasti práva, právní zastoupení, sestavování smluv a dokumentů.

Zákazníci: Jednotlivci, malé a střední podniky, kteří potřebují právní pomoc v různých oblastech, jako jsou rodinné právo, občanské právo, právo pracovní a obchodní právo.

Zaměstnanci:

1. **Právníci:**
    - Právníci jsou klíčovými členy týmu a mají odpovědnost za poskytování právních služeb klientům. Mezi jejich hlavní úkoly patří právní poradenství, příprava smluv a dokumentů, právní zastoupení v soudních sporech a řešení právních otázek.
2. **Koncipienti:**
    - Koncipienti podporují právníky ve vykonávání jejich práce. Jejich úkoly mohou zahrnovat výzkum právních otázek, přípravu dokumentů, komunikaci s klienty a správu právních záležitostí.
3. **Administrativní personál:**
    - Administrativní personál zajišťuje běžné administrativní úkoly v kanceláři, jako je příjem a rozdělování pošty, plánování schůzek a událostí, správa dokumentů a účetnictví.
4. **Stážisté:**

- Stážisté jsou studenti práva nebo absolventi právnických fakult, kteří získávají praktické zkušenosti v oboru. Pod dohledem zkušených právníků mohou stážisté provádět výzkum právních otázek, připravovat dokumenty, asistovat právníkům v přípravě na jednání a získávat cenné praktické dovednosti.

Pracovní stanice zaměstnanců:

1. **Právníci:**

- Pevné pracovní stanice: Právníci mají své pevné pracovní stanice v kancelářích LegaConsult, vybavené stolními počítači, monitory, klávesnicemi a myšmi. Tyto stanice jim poskytují stabilní pracovní prostředí pro práci na dlouhodobých projektech a právních případech.
- Přenosné pracovní stanice: Kromě pevných pracovních stanic mohou právníci mít také přenosné pracovní stanice ve formě notebooků nebo tabletů. Tyto zařízení jim umožňují pracovat na cestách, v soudní síni nebo mimo kancelář, aniž by omezovali jejich produktivitu.

2. **Koncipienti:**

- Pevné pracovní stanice: Koncipienti mohou mít také své pevné pracovní stanice v kancelářích, kde mají přístup k počítačům, tiskárnám a dalším kancelářským zařízením pro vykonávání svých úkolů.
- Přenosné pracovní stanice: Stejně jako právníci mohou mít i Koncipienti přenosné pracovní stanice ve formě notebooků nebo tabletů pro práci na cestách a mimo kancelář.

3. **Administrativní personál:**

- Pevné pracovní stanice: Administrativní personál má své pevné pracovní stanice v administrativních prostorách kanceláří, kde mají přístup k počítačům, tiskárnám, telefonům a dalším kancelářským zařízením.

- Přenosné pracovní stanice: Pokud je to nezbytné, může mít administrativní personál přístup k přenosným pracovním stanicím, které jim umožňují pracovat mimo kancelář, například při organizaci událostí nebo schůzek mimo pracoviště.

4. **Stážisté:**

- Pro stážisty jsou vyhrazeny určené pracovní stanice, které jsou sdíleny mezi více stážisty v závislosti na jejich směnách.
- Tyto pracovní stanice jsou vybaveny stolními počítači nebo notebooky, stejně jako standardní pracovní stanice, ale budou mít možnost rychlého přihlášení a odhlášení pro různé uživatele.
- Na sdílených pracovních stanicích budou stážisté moci pracovat s dokumenty uloženými v cloudovém úložišti, aby byla zajištěna snadná spolupráce a přístup k sdíleným zdrojům.
- Stážisté budou informováni o jejich přidělených směnách a pracovních stanicích prostřednictvím interního kalendáře nebo rezervačního systému.

4.1.2 **Analýza firmy**

Následujícím krokem vycházejícím z teoretické části je analýza firmy.

Inventarizace aktiv:

1. **Fyzická aktiva:**
    - Kancelářské prostory:
        - Č. 101: Kancelář právníka A.
        - Č. 102: Kancelář právníka B.
        - Č. 103: Kancelář koncipienta A.
        - Č. 104: Kancelář koncipienta B.
        - Č. 105: Kancelář koncipienta C a prostor pro stážisty.
        - Č. 106: Kancelář administrativního personálu.
    - Konferenční místnost: Pro jednání s klienty.
    - Právní knihovna: Obsahuje knihy, právní časopisy a zákonné sbírky.
    - Vybavení kanceláří: Stoly, židle, skříně, tiskárny, skenery, telefony.
2. **Technologická aktiva:**
    - Počítačové vybavení:

        - 10 x stolní počítač pro právníky a koncipienty.
        - 10 x notebook pro administrativní personál a stážisty.
    - Servery:
        - Server pro ukládání důležitých informací (offline): Uchovává citlivé právní dokumenty a data klientů, nepřipojen k internetu pro zajištění maximální bezpečnosti.
        - Server pro ukládání běžných dat (online): Dostupný přes internet pomocí VPN, slouží pro sdílení dokumentů a dat mezi zaměstnanci, přístupný i mimo kancelář.
3. **Ostatní aktiva:**
    - Právní software: Licencovaný software pro správu případů a dokumentů.
    - Komunikační technologie: Telefonní systém, e-mailové služby, videokonferenční vybavení.
    - Bezpečnostní zařízení: Firewally, antivirový software, šifrování dat, VPN systém pro vzdálený přístup.

Hrozby:

1. **Kybernetické útoky:**
    - Útoky na síťovou bezpečnost: Hacker může napadnout síť prostřednictvím malware, phishingu nebo jiných technik, aby získal neoprávněný přístup k citlivým informacím.
    - DoS útoky: Útočník může provést DoS (Denial of Service) útok na servery, což by mohlo způsobit výpadek služeb a narušení provozu firmy.
2. **Ztráta dat:**
    - Fyzická poškození: Požár, povodeň nebo jiné přírodní katastrofy mohou způsobit fyzické poškození serverů a jiného zařízení, což může vést ke ztrátě důležitých dat.
    - Technické selhání: Selhání hardwaru nebo softwaru může způsobit ztrátu dat nebo nedostupnost služeb, což může negativně ovlivnit práci firmy.
3. **Sociální inženýrství:**
    - Podvodníci mohou využít sociální inženýrství k získání citlivých informací, jako jsou hesla nebo přístupové údaje, od zaměstnanců.

Zranitelnosti:

1. **Nedostatečná síťová bezpečnost:**
    - Nedostatečné zabezpečení sítě může zanechat firmu otevřenou různým kybernetickým hrozbám, včetně útoků na síťové zařízení, phishingu a malware.
2. **Nedostatečná záloha dat:**
    - Firma nezajišťuje pravidelnou a spolehlivou zálohu dat, citlivé informace tak mohou být vystaveny riziku ztráty v případě havárie nebo jiné události.
3. **Nedostatečné školení zaměstnanců:**
    - Zaměstnanci absolvovali školení o postupech při zaházení s citlivými informacemi při svém nástupu. Jejich znalosti však nebyly a nejsou nadále testovány, a další školení již firma neorganizuje.
    - Zaměstnanci tak jsou zranitelní vůči kybernetickým hrozbám, jelikož nejsou správně školeni v oblasti kybernetické bezpečnosti.

Hodnocení současných bezpečnostních opatření:

1. **Chybějící SIEM systém (Security Information and Event Management):**
    - Chybějící SIEM systém znamená, že firma nemá centralizovaný mechanismus pro sběr, analýzu a reakci na události z různých bezpečnostních zdrojů v síti. Tím pádem může být obtížné identifikovat a reagovat na hrozby a incidenty včas.
2. **Používání pouze antiviru:**
    - Antivirový software je důležitým prvkem ochrany proti známým malwarům, ale je omezený ve svých schopnostech detekce nových a pokročilých hrozeb. Používání pouze antiviru může znamenat, že firma je zranitelná vůči pokročilým útokům, které antivirový software nemusí detekovat.
3. **Chybějící IDS (Intrusion Detection System):**
    - Chybějící IDS znamená, že firma nemá mechanismus pro detekci neoprávněného nebo podezřelého síťového provozu. To může znamenat, že útočníci mohou provádět neoprávněné aktivity v síti bez detekce.
4. **Pouze softwarové firewally:**

- Používání pouze softwarových firewalů může být omezené ve srovnání s hardwarovými firewally. Softwarové firewally mohou být náchylné k různým útokům, jako jsou přetížení a obcházení. Hardwarové firewally poskytují obvykle lepší výkon a ochranu.

5. **Chybějící webový aplikační firewall:**
   - Chybějící webový aplikační firewall znamená, že firma nemá ochranu pro webové aplikace proti různým typům útoků, jako jsou SQL injection, cross-site scripting (XSS) a další. To může znamenat, že webové aplikace mohou být zranitelné a snadno zneužitelné útočníky.
6. **Externí správa bezpečnostních opatření:**
   - Firma může outsourcuje správu svých bezpečnostních opatření externím poskytovatelem služeb.
   - Závislost na externím správci znamená menší kontrolu nad bezpečnostními opatřeními a potřebu pečlivě vybrat spolehlivého a důvěryhodného poskytovatele.

Posouzení právních a regulačních požadavků:

Na základě teoretické části lze konstatovat, že firma musí splňovat:

1. **GDPR (Obecné nařízení o ochraně osobních údajů):**
   - GDPR je evropské nařízení, které reguluje ochranu osobních údajů občanů EU, a je povinné pro všechny subjekty, které zpracovávají osobní údaje těchto občanů. To zahrnuje i právnické firmy.
   - Firma musí dodržovat principy ochrany osobních údajů, zajišťovat transparentnost ve zpracování osobních údajů, a zajistit, že mají dostatečné bezpečnostní opatření k ochraně těchto údajů.
2. **Zákon o kybernetické bezpečnosti:**
   - V České republice platí zákon o kybernetické bezpečnosti, který stanoví požadavky na zabezpečení informačních systémů a ochranu informací. Firma je povinna dodržovat tyto požadavky a zajišťovat bezpečnost svých informačních systémů a dat.

- To zahrnuje implementaci bezpečnostních opatření, správu rizik, školení zaměstnanců v oblasti kybernetické bezpečnosti a povinnost hlášení incidentů týkajících se kybernetické bezpečnosti.

3. **Evropské směrnice o kybernetické bezpečnosti:**
   - Vedle zákona o kybernetické bezpečnosti může firma být také povinna dodržovat evropské směrnice a normy týkající se kybernetické bezpečnosti. Tyto směrnice mohou obsahovat další požadavky na ochranu informačních systémů a informací.
   - Zajištění souladu s těmito směrnicemi může vyžadovat dodatečné opatření, jako je certifikace bezpečnosti, audity nebo pravidelné revize bezpečnostních postupů.

Analýza lidských zdrojů:

Strategie řízení lidských zdrojů: Je důležité zajistit, aby zaměstnanci měli přístup k pravidelnému školení a profesnímu rozvoji, aby si udrželi své dovednosti a znalosti aktuální.

Personální obsazení: Firma má různorodý tým zaměstnanců, včetně právníků, koncipientů, administrativního personálu a stážistů. Tým je rozložen tak, aby pokryl potřeby právních služeb a administrativní podpory.

Žádný interní bezpečnostní tým či zaměstnanec: Firma nemá svůj interní bezpečnostní tým, a tak ztrácí plnou kontrolu nad bezpečnostními opatřeními prováděnými externím poskytovatelem.

Definování bezpečnostních cílů:

1. **Zvýšení kontroly nad bezpečnostními operacemi:** Hlavním cílem je získat větší kontrolu nad bezpečnostními operacemi a procesy, což umožní firmě lépe chránit svá aktiva a data před hrozbami kybernetického prostředí.
2. **Zlepšení ochrany citlivých informací:** Firma si klade za cíl zlepšit ochranu svých citlivých informací, včetně osobních údajů klientů a interních dokumentů. Interní správa bezpečnostních opatření umožní firmě lépe identifikovat a reagovat na potenciální rizika a zranitelnosti.

3. **Posílení odpovědnosti a transparentnosti:** Převzetí správy bezpečnostních opatření zpět do vlastních rukou umožní firmě posílit svou odpovědnost za bezpečnostní opatření a transparentnost procesů. To zahrnuje pravidelnou kontrolu a audit bezpečnostních postupů a větší transparentnost v komunikaci s klienty a partnery ohledně bezpečnostních opatření.
4. **Snížení závislosti na externích poskytovatelích:** Firma si klade za cíl snížit svou závislost na externích poskytovatelích a posílit svou interní kapacitu pro řízení a ochranu kybernetické bezpečnosti. Tím se sníží riziko spojené s potenciálními nedostatky nebo ztrátou kontroly nad bezpečnostními procesy.
5. **Zvýšení efektivity a účinnosti:** Interní správa bezpečnostních opatření by měla firmě umožnit lépe reagovat na aktuální hrozby a rychleji implementovat nové bezpečnostní opatření a technologie. To zvýší celkovou efektivitu a účinnost bezpečnostních procesů.

Zohlednění finančních zdrojů:

Rozpočet se pak bude dělit především do:

1. **Nákup technologií a nástrojů:**
    - Nákup bezpečnostních technologií a nástrojů, jako jsou firewally, antivirové programy, systémy monitorování a detekce hrozeb, SIEM systémy, a další.
    - Náklady na licencování softwaru a případné hardwarové vybavení.
2. **Školení zaměstnanců:**
    - Financování školení zaměstnanců v oblasti kybernetické bezpečnosti, aby získali potřebné dovednosti a znalosti pro správu bezpečnostních opatření.
    - Školení může zahrnovat certifikované kurzy, workshopy, školení na pracovišti a další formy vzdělávání.
3. **Nábor zaměstnanců:**
    - Případné náklady spojené s náborem nových zaměstnanců, kteří budou odpovědní za správu bezpečnostních opatření.
4. **Externí konzultace a odborné služby:**
    - Případné náklady spojené s externími konzultacemi a odbornými službami, pokud firma potřebuje poradenství nebo pomoc při implementaci bezpečnostních opatření.

4.2 Navržení bezpečnostní architektury

Perimetrická ochrana:

1. **Firewall:**
    - Nasazení síťového firewallu jako první linie obrany na hranici sítě firmy.
2. **Intrakční detekce/prevenční systém (IDS/IPS):**
    - Implementace IDS/IPS systému.
3. **Antivirový a antimalwarový software:**
    - Instalace antivirového a antimalwarového softwaru na všech koncových zařízeních a serverech v síti.
4. **Segmentace sítě:**
    - Rozdělení interní sítě na segmenty a zavedení pravidel pro komunikaci mezi nimi. Oddělení síťového provozu klientů od interních serverů pomocí VLAN (Virtual LAN) a firewall pravidel.
5. **VPN (Virtual Private Network):**
    - Nasazení VPN pro zabezpečené vzdálené připojení zaměstnanců a externích uživatelů.
6. **Bezpečnostní politiky a pravidla:**
    - Stanovení a vynucování bezpečnostních politik a pravidel pro přístup k síti a datům. Například vyžadování silných hesel, pravidelné změny hesel, a omezení přístupu k citlivým informacím na základě role zaměstnance.

4.3 Výběr bezpečnostních nástrojů a technologií

Průzkum trhu:

Firewally:

1. **Cisco ASA (Adaptive Security Appliance):**
    - Cisco ASA je jedním z předních firewallů na trhu, nabízející komplexní ochranu sítě a dat. Poskytuje pokročilé funkce, jako je inspekce stavu, hluboká inspekce paketů a podpora VPN.
2. **Palo Alto Networks Next-Generation Firewall:**

- Palo Alto Networks nabízí firewally další generace s pokročilými funkcemi jako je aplikační identifikace a kontrola, prevence hrozeb a integrovaná správa bezpečnostní politiky.

3. **Fortinet FortiGate:**
   - Fortinet FortiGate je široce používaný firewall s pokročilými funkcemi jako je IPS (Intrusion Prevention System), SSL/TLS inspekce a správa SD-WAN (Software-Defined Wide Area Network).
4. **Check Point Next Generation Firewall:**
   - Check Point je dalším významným hráčem na trhu s firewally, který nabízí širokou škálu funkcí, včetně aplikovaného bezpečnostního intelligence, detekce a prevence hrozeb a rozšířené správy.
5. **Juniper Networks SRX Series Services Gateways:**
   - Juniper Networks poskytuje řadu firewallů SRX, které kombinují pokročilou síťovou ochranu s výkonem a škálovatelností. Tyto firewally nabízejí také rozšířené funkce pro VPN a SD-WAN.
6. **SonicWall Next-Generation Firewall:**
   - SonicWall je známým poskytovatelem firewallů další generace s funkcemi jako je pokročilá detekce hrozeb, kontrola aplikací a ochrana proti ransomwaru.

IDS/IPS:

1. **Cisco Firepower NGIPS (Next-Generation IPS):**
   - Cisco Firepower NGIPS je výkonný IPS s pokročilými funkcemi, jako je detekce a prevence síťových hrozeb, analýza chování a automatická blokace útoků.
2. **Palo Alto Networks Threat Prevention:**
   - Threat Prevention od společnosti Palo Alto Networks je částí jejich platformy Next-Generation Firewall a nabízí pokročilou detekci a prevenci hrozeb na síťové úrovni.
3. **Fortinet FortiGate Intrusion Prevention System:**
   - FortiGate IPS od společnosti Fortinet je součástí jejich integrovaného bezpečnostního řešení a poskytuje rozšířenou detekci a prevenci hrozeb s vysokým výkonem.

4. **Check Point Intrusion Prevention System:**
    - Check Point IPS nabízí komplexní ochranu proti širokému spektru hrozeb, včetně známých i neznámých útoků, s pokročilými funkcemi jako je threat emulation a threat extraction.
5. **Snort:**
    - Snort je open-source IDS/IPS systém s širokou podporou komunitou a flexibilní konfigurací. Nabízí detekci hrozeb na základě signatur i analýzy chování.
6. **Suricata:**
    - Suricata je další open-source IDS/IPS systém s vysokým výkonem a možností detekce hrozeb pomocí různých technik, včetně signatur, protokolové analýzy a detekce anomálií.

Antiviry a Antimalware software:

1. **Symantec Endpoint Protection:**
    - Symantec Endpoint Protection je široce používaný antivirový a antimalwarový software s pokročilými funkcemi, jako je detekce a prevence hrozeb na základě chování, ochrana proti ransomware a integrovaná správa.
2. **McAfee Endpoint Security:**
    - McAfee Endpoint Security poskytuje komplexní ochranu pro koncové zařízení s funkcemi jako je detekce hrozeb na základě chování, kontrola aplikací, ochrana e-mailů a webového prohlížeče.
3. **Kaspersky Endpoint Security:**
    - Kaspersky Endpoint Security je známý svou efektivní detekcí a prevencí různých typů hrozeb, včetně malware, ransomware, phishingových útoků a dalších.
4. **Bitdefender GravityZone Business Security:**
    - Bitdefender GravityZone Business Security je oblíbeným řešením pro malé a střední podniky, které poskytuje efektivní ochranu proti hrozbám jako jsou viry, spyware, trojské koně a škodlivé webové stránky.
5. **Trend Micro Apex One:**

- Trend Micro Apex One je integrovaný bezpečnostní software, který nabízí ochranu proti známým i neznámým hrozbám pomocí pokročilých technologií, včetně analýzy chování a sandboxování.

6. **ESET Endpoint Security:**
   - ESET Endpoint Security je dalším populárním antivirovým a antimalwarovým řešením s vysokým výkonem a širokou funkcionalitou, včetně ochrany před malware, ransomware, phishingem a spamem.

VPN:

1. **Cisco AnyConnect Secure Mobility Client:**
   - Cisco AnyConnect je vysoce škálovatelné řešení, které poskytuje bezpečné a snadné připojení k firemní síti z různých zařízení a platforem. Nabízí pokročilé funkce správy, včetně možnosti centralizované konfigurace a monitoringu.
2. **Palo Alto Networks GlobalProtect:**
   - GlobalProtect od společnosti Palo Alto Networks je integrální součástí jejich Next-Generation Firewall platformy a poskytuje bezpečné připojení k firemní síti z různých míst a zařízení. Nabízí pokročilé bezpečnostní funkce a možnosti správy.
3. **Fortinet FortiClient:**
   - FortiClient je integrované bezpečnostní řešení od společnosti Fortinet, které zahrnuje VPN funkce pro bezpečné připojení k firemním sítím. Poskytuje širokou škálu bezpečnostních funkcí, včetně ochrany proti hrozbám a správy zařízení.
4. **Check Point Endpoint Security VPN:**
   - Endpoint Security VPN od společnosti Check Point je součástí jejich integrované bezpečnostní platformy a poskytuje bezpečné připojení k firemní síti z různých zařízení a míst. Nabízí širokou škálu bezpečnostních funkcí a možností správy.
5. **OpenVPN Access Server:**
   - OpenVPN Access Server je snadno použitelné a škálovatelné řešení pro vytváření vlastních VPN pro firemní použití. Nabízí pokročilé bezpečnostní funkce a možnosti správy, včetně možnosti integrace s firemními systémy.

6. **Zscaler Private Access:**
    - Zscaler Private Access je cloudové řešení pro bezpečné připojení k firemním aplikacím a zdrojům. Nabízí pokročilou bezpečnostní ochranu a správu přístupu s možností integrace s firemními systémy a cloudovými službami.

SIEM:

Výběr SIEM systému probíhal na základě poznatků z teoretické části. Výsledky výběru jsou k nalezení v příslušné kapitole.

4.4 Následující kroky

Po dokončení předchozích kroků by následovaly kroky vycházející z kapitoly postupy pro implementaci bezpečnostních systémů a to tedy: Implementace bezpečnostních systémů, Ověření bezpečnostních systémů, Školení zaměstnanců, Monitoring a správa, Revize a správa.

5 Výsledky a diskuse

5.1 Výběr Softwarových produktů

5.1.1 Výběr Firewallu

V této části jsem za pomoci vícekriteriální analýzy a její bodovací metody s vahami vybíral nejvhodnější Firewall z navržených variant. Vybíráno bylo dle následujících kritérií.

Jméno	**Zabezpečení**	**Výkon**	**Kompatibilita**	**Funkce**	**Podpora**
Cisco ASA	8	8	10	9	10
Palo Alto	9	9	9	8	9
FortiGate	8	8	8	8	8
Check Point	8	8	8	8	8
Juniper	7	7	7	7	7
SonicWall	7	7	7	7	7
Váhy:	0,25	1/6	1/6	0,25	1/6

Tabulka 1 Bodové ohodnocení vybraných Firewallů

Bodovací metoda	**Bodovací metoda s vahami**
45	8,91667
44	8,75
40	8
40	8
35	7
35	7

Tabulka 2 Výsledek vícekriteriální analýzy Firewallů

Z tabulky číslo 2 vyplývá, že jsem podle výsledků bodovacích metod zvolil firewall Cisco ASA

5.1.2 Výběr IDS/IPS

V tomto kroku jsem opět za pomoci vícekriteriální analýzy a její bodovací metody s vahami vybíral nejvhodnější IDS/IPS, váha kompatibility se oproti minulé volbě zvýšila, aby reprezentovala důraz na kompatibilitu vybíraného systému s již zvoleným Firewallem.

Jméno	Metody detekce	Kompatibilita	Výkon	Správa a monitorování	Podpora
Cisco Firepower	9	10	9	8	10
Palo Alto	9	8	9	9	9
Fortinet FortiGate	8	9	8	8	9
Check Point	8	7	8	8	8
Snort	7	8	7	6	7
Suricata	8	8	8	7	7
Váhy:	0,25	0,2	0,175	0,175	0,2

Tabulka 3 Bodové ohodnocení vybraných IDS/IPS

Bodovací metoda	Bodovací metoda s vahami
46	9,225
44	8,8
42	8,4
39	7,8
35	7,025
38	7,625

Tabulka 4 Výsledek vícekriteriální analýzy IDS/IPS

V tabulce číslo 4 lze najít opět výsledky bodovacích metod. Díky těmto výsledkům jsem zvolil jako IDS/IPS Cisco Firepower.

5.1.3 Výběr antivirového software

Následně jsem vybíral antivirový software, váha kompatibility opět trochu vzrostla v návaznosti na předchozí kroky.

Jméno	Zatížení systému	Aktualizace	Detekční účinnost	Kompatibilita	Podpora
Symantec	7	8	8	9	8
McAfee	8	9	9	9	9
Kaspersky	7	8	9	8	8
Bitdefender	9	9	9	9	9
Trend Micro	8	8	8	8	8
ESET	8	8	8	8	7
Váhy:	0,125	0,25	0,25	0,225	0,15

Tabulka 5 Bodové ohodnocení vybraných Antivirů

Bodovací metoda	Bodovací metoda s vahami
40	8,1
44	8,875
40	8,125
45	9
40	8
39	7,85

Tabulka 6 Výsledek vícekriteriální analýzy Antivirů

V tabulce číslo 6 lze nalézt výsledky bodovacích metod použitých k získání vhodného software. Vybral jsem tak byl díky nejlepšímu výsledku Bitdefender.

5.1.4 Výběr VPN

Jméno	Bezpečnost	Výkon a spolehlivost	Kompatibilita	Podpora	Správa
Cisco AnyConnect	9	9	10	9	8
Palo Alto	9	9	8	8	8
Fortinet FortiClient	8	8	8	7	7
Check Point	8	8	8	7	7
OpenVPN	7	8	8	5	7
Zscaler	9	9	8	8	9
Váhy:	0,33	0,15	0,33	0,09	0,09

Tabulka 7 Bodové ohodnocení vybraných VPN

Bodovací metoda	Bodovací metoda s vahami
45	9,213333
42	8,456667
38	7,793333
38	7,793333
35	7,28
43	8,54667

Tabulka 8 Výsledek vícekriteriální analýzy VPN

V tabulce 9 jsou výsledky analýzy VPN software. Nejlepší výsledek vykazuje Cisco AnyConnect a proto jsem ho vybral jako vhodné k použití.

5.2 Výběr SIEM systému

V návaznosti na předchozí vybraný software jsem nakonec vybíral SIEM, který bude z ostatních systémů data sbírat, analyzovat, korelovat a dále s nimi pracovat.

Jméno	Funkce	Kompatibilita	Complience	Analýza událostí
Splunk	9	9	9	9
Graylog	8	7	8	8
NetWitness	9	9	9	9
ArcSight	9	9	9	9
LogRythm	9	8	8	8
IBM Qradar	9	9	9	9
Váhy:	0,25	0,5	0,1	0,15

Tabulka 9 Bodové ohodnocení vybraných SIEM systémů

Bodovací metoda	Bodovací metoda s vahami
36	9
31	7,5
36	9
36	9
33	8,25
36	9

Tabulka 10 Výsledek vícekriteriální analýzy SIEM systémů

V tabulce 9 se nachází bodové ohodnocení jednotlivých SIEM systémů zmíněných v teoretické části. Největší váhu má pak kompatibilita reprezentující ostatní již zvolené systémy (software).

V tabulce 10 jsou pak výsledky bodovacích metod. Z výsledků jsem vyvodil závěr, že firmě doporučuji zvolit buďto: Splunk, Netwitness, ArcSight, nebo IBM Qradar. Může se zde nabízet otázka, proč v žádné z analýz není uvedena jako kritérium cena i když je v teoretické části několikrát zmíněna jako častokrát nejdůležitější kritérium. Cena SIEM systémů bývá většinou nastavena každému zákazníku na míru. A díky tomu, že má firma je fiktivní, nelze pro ni získat reálnou odhadovou cenu.

6 Závěr

6.1 Shrnutí cílů

Hlavním cílem této práce bylo představit, jak monitorovat sít a jak implementovat bezpečnostní systémy do firmy

Dílčími cíli pak byly vytvoření příkladové firmy, analýza firmy, navržení bezpečnostní architektury, výběr bezpečnostních nástrojů a technologií, implementace a otestování

6.2 Zhodnocení dosažených výsledků.

V práci jsem dosáhl veškerých stanovených cílů, které přináší náhled do problematiky implementace bezpečnostních systémů. Analyzoval jsem postupy implementace těchto systémů a následně je aplikoval v praktické části.

Celkově lze konstatovat, že implementace bezpečnostních systémů do firemního prostředí je nezbytným krokem pro ochranu firemních aktiv a udržení konkurenceschopnosti v dnešním digitálním prostředí. Avšak úspěšná implementace vyžaduje nejen technologická opatření, ale také aktivní zapojení celé organizace a udržitelnou investici do kybernetické bezpečnosti.

7 Seznam použitých zdrojů

§ 4 Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), str. [Systém ASPI]. Wolters Kluwer. 2336-517X.
ALEF. SPLUNK. [Online] [Citace: 29. 10 2023.] https://www.alef.com/cz/splunk.c-214.html.
Comodo. WHAT IS SPLUNK USED FOR? [Online] [Citace: 29. 10 2023.] https://www.comodo.com/is-splunk-a-siem.php.
ENISA. 2022. [Online] 3. Listopad 2022. [Citace: 21. 10 2023.] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
Graylog. Graylog Documentation. [Online] [Citace: 10. 11 2023.] https://go2docs.graylog.org/5-2/home.htm.
IBM. IBM Documentation. [Online] [Citace: 24. 11 2023.] https://www.ibm.com/docs/en/qsip/7.5.
LogRythm. Logrythm Documentation. [Online] [Citace: 22. 11 2023.] https://docs.logrhythm.com/.
Micosoft. Co je to SIEM. [Online] [Citace: 28. 10 2023.] https://www.microsoft.com/cs-cz/security/business/security-101/what-is-siem.
Microfocus. ArcSight Documentation. [Online] [Citace: 20. 11 2023.] https://www.microfocus.com/documentation/arcsight/#gsc.tab=0.
—. ArcSight Enterprise Security Manager. [Online] [Citace: 15. 11 2023.] https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm.
Microsoft. Co je kybernetický útok? *https://www.microsoft.com/.* [Online] [Citace: 16. 10 2023.] https://www.microsoft.com/cs-cz/security/business/security-101/what-is-a-cyberattack.
N. Ú. K. I. B. 2022. https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [Online] 2022. [Citace: 15. Říjen 2023.]
N.Ú.K.I.B. 2023. https://www.aspi.cz/. *Minimální bezpečnostní standard. Verze 1.2, platná ke dni 14. února 2023.* [Online] 14. 2 2023. [Citace: 16. 10 2023.] https://www.aspi.cz/products/lawText/7/302132/1/2?vtextu=N%C3%9AKIB#lema3.
NetWitness. NetWitness Resources. [Online] [Citace: 12. 11 2023.] https://www.netwitness.com/resources/.
S, Viswanath V. 2023. What is ArcSight. [Online] 3. Duben 2023. [Citace: 20. 11 2023.] https://mindmajix.com/what-is-arcsight.
Splunk. Splunk Resources. [Online] [Citace: 5. 11 2023.] https://www.splunk.com/en_us/resources.html.
The Hacker News. 2023. [Online] 10. Duben 2023. [Citace: 24. 10 2023.] https://thehackernews.com/2023/04/top-10-cybersecurity-trends-for-2023.html.
Trellix. 2023. The Cyberthreat Report. *https://www.trellix.com.* [Online] Červen 2023. [Citace: 20. 10 2023.] https://www.trellix.com/advanced-research-center/threat-reports/jun-2023/.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek