Aplikace pro analýzu rizik v kybernetické a informační bezpečnosti

Petr Diviš

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Petr Diviš**
Osobní číslo:	**L21568**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Aplikace pro analýzu rizik kybernetické a informační bezpečnosti**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do dané problematiky.
2. Seznamte se s aplikacemi pro analýzu rizik v kybernetické a informační bezpečnosti.
3. Proveďte komparaci dostupných aplikací se zaměřením na jejich funkcionalitu.
4. Na základě předchozích zjištění navrhněte vlastní aplikaci.

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

Seznam doporučené literatury:

1. KOLOUCH, Jan a Pavel BAŠTA. *Cyber Security.* Praha. CZ.NIC, 2019. ISBN 978-80-88168-34-8.
2. SANTOS, Henrique M. D. *Cyberserity: A Practical Engineering Approach.* Boca Raton: CRC Press, 2022. ISBN 978-0-367--25242-7.
3. SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* Brno:CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 3.5.2024

Jméno a příjmení studenta: Petr Diviš

.....
podpis studenta

ABSTRAKT

Bakalářská práce se věnuje aplikacím pro analýzu rizik v kybernetické a informační bezpečnosti. Teoretická část obsahuje základní teoretická východiska dané problematiky. Popisuje informační a komunikační technologie, řízení rizik, ale i datové modelování při navrhování informačního systému.

Praktická část se zabývá seznámením s aplikacemi pro analýzu rizik a jejich následnou komparací. V závěru práce je zpracován konceptuální datový model aplikace pro analýzu rizik v kybernetické a informační bezpečnosti.

Klíčová slova: Analýza rizik, Aplikace, Kybernetická bezpečnost, Kybernetické hrozby.

ABSTRACT

The bachelor thesis focuses on applications for risk analysis in cyber and information security. The theoretical part contains the basic theoretical background of the issue. It describes information and communication technologies, risk management, as well as data modelling in information system design.

The practical part deals with the introduction to applications for risk analysis and their subsequent comparison. The thesis concludes with a conceptual data model of an application for risk analysis in cyber and information security.

Keywords: Applications, Cyber security, Cyber threats, Risk analysis.

Tímto bych rád poděkoval vedoucímu mé bakalářské práce Ing. Petru Svobodovi, Ph.D., za užitečné rady a konstruktivní připomínky, které mi velmi pomohly při psaní a finalizaci bakalářské práce.

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

OBSAH

ÚVOD

Informační systémy se staly nepostradatelným nástrojem pro chod mnoha procesů v dnešním světě. Jejich vliv se dotýká prakticky všech oblastí lidské činnosti, od podnikání a průmyslu po vzdělání a státní správu. Informační systémy slouží k zefektivnění procesů, optimalizaci, nebo zlepšení komunikace. Rozšiřování informačních systémů přineslo rizika, které mohou ohrozit jejich integritu. Tyto hrozby zahrnují kybernetické útoky, které mohou mít podobu malwaru, phishingových útoků, nebo krádeži informací. Podstatnou část tvoří i chyby uživatelů informačních systémů, kdy při nedbalosti, nebo úmyslném jednání mohou vést k únikům dat, nebo nevědomé infikování systému viry. Technické selhání lze také považovat za hrozbu, kdy dojde k hardwarové, nebo softwarové poruše, což může zapříčinit nedostupnost dat, nebo narušení fungování informačního systému.

Ochrana informačních systémů před kybernetickými útoky, chybami uživatelů a technickými selháními je komplexní proces, který vyžaduje implementaci technických i organizačních opatření. Technická opatření zahrnují firewally, antivirové a antispyware programy, případně systémy detekce a prevence vniknutí do systému. Mezi technická opatření patří také aplikace pro analýzu rizik. Aplikace pro analýzu rizik slouží k identifikaci, analýze a hodnocení rizik kybernetické bezpečnosti, což vede k implementaci adekvátních opatření pro zmírnění rizik. Důležitá jsou ovšem i organizační opatření, jako je politika informační bezpečnosti, která definuje pravidla a postupy pro používání informačních systémů. Dále také řízení přístupu, které určuje, kdo má přístup k jakým datům a systémům.

V oblasti informační bezpečnosti se neustále objevují nové trendy, na které je nutné reagovat, a které je nutné brát v úvahu při ochraně informačních systémů. Rostoucí sofistikovanost kybernetických útoků, nárůst útoků na cloudové systémy, nebo nutnost chránit data v mobilních zařízeních jsou oblasti, kterým je potřeba věnovat zvýšenou pozornost.

Hlavním cílem bakalářské práce je návrh konceptuálního datového modelu aplikace pro analýzu rizik v kybernetické a informační bezpečnosti. K dosažení hlavního cíle slouží tři dílčí cíle. Prvním dílčím cílem je pojednat o souvisejících teoretických východiscích řešené problematiky. Druhý dílčí cíl je seznámit se s metodologií tvorby datového modelu. Třetí dílčí cíl je provést komparaci vybraných aplikací pro analýzu rizik.

Za účelem splnění cílů této bakalářské práce bylo využito komparace, která je v práci použita pro komparaci již existujících aplikací. Popis je v práci použit pro seznámení s procesem tvorby datových modelů. Dedukce slouží v práci jako základ pro stanovení teoretického

rámce, který vychází z obecných principů a konceptů řízení kybernetických rizik a modelování dat. Analýza je v práci využita k hodnocení shromážděných dat o aplikacích pro analýzu rizik. Indukce je využita v práci k identifikaci vztahů mezi aplikacemi pro analýzu rizik. Deskripce je v práci použita u řízení rizik a syntéza je využita v závěru práce.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

V posledním desetiletí došlo k výraznému rozvoji digitálních technologií, což vedlo k rozvoji kybernetické bezpečnosti. Její význam lze pochopit jako ochranu digitálních systémů a dat před kybernetickými hrozbami. Tyto hrozby mohou mít vážné dopady na ekonomiku, bezpečnost státu a společnost. Kybernetická bezpečnost hraje také podstatnou roli v ochraně práv a svobod jednotlivců v kyberprostoru. Kybernetickou bezpečnost nelze v současné době ignorovat, ani brát na lehkou váhu. Je to důležitá oblast, která má zásadní dopad na řadu organizací a jednotlivců. Proto je třeba jí věnovat dlouhodobý a systematický přístup. (Kolouch et al., 2019)

Kyberprostor je virtuální prostor, který je vytvářen za pomocí počítačových systémů a síťových technologií. Vzájemná komunikace systémů v kyberprostoru se provádí za pomocí TCP/IP protokolu. Kyberprostor je dynamický a neustále se vyvíjí, protože se přidávají nové systémy a technologie. (Kolouch et al., 2019)

Kybernetické hrozby se v posledních letech stupňují. Je to způsobeno rozsáhlou digitalizací, při které se mnoho tradičních hrozeb přesouvá do kyberprostoru. Dochází zde také k prolínání různých hrozeb a k hybridizaci bezpečnostního prostředí. Všechny tyto hrozby jsou komplexní a mohou mít vážné důsledky. Mohou narušit důvěru veřejnosti ve stát, stabilitu země a demokratické uspořádání. Aby stát mohl účinněji ochránit kyberprostor, musí porozumět těmto hrozbám. To znamená že musí mít přístup k relevantním informacím a musí být schopen je analyzovat. (Česká republika, 2020)

Systém zajišťování kybernetické bezpečnosti v České republice je komplexní a zahrnuje mnoho různých subjektů. Každý subjekt má svou roli a přispívá k zabezpečení kyberprostoru různými způsoby, které jsou dány jeho působností a aktivitami. Vrcholným orgánem, který je odpovědný za zajišťování národní bezpečnosti, a tedy i za řízení a funkčnost systému zajišťování kybernetické bezpečnosti, je vláda České republiky. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je hlavním orgánem České republiky odpovědným za kybernetickou bezpečnost. Jeho působnost je stanovena zákonem o kybernetické bezpečnosti a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti. NÚKIB má na starost ochranu kritické informační infrastruktury a dalších důležitých informačních a komunikačních systémů. Za tímto účelem zřídil vládní CERT, který poskytuje subjektům služby v oblasti kybernetické bezpečnosti. NÚKIB také zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti. Je národním kontaktním bodem pro koordinaci

výzkumu a vývoje a významně se podílí na vzdělávání a osvětě v této oblasti. (Česká republika, 2020)

Informace je třeba chránit před neoprávněným přístupem, změnou, nebo zničením po celou dobu jejich existence. To platí pro informace v jakékoli formě, ať už jsou uloženy, přenášeny, nebo používány. Stupeň ochrany by měl být přizpůsoben důležitosti informací. Proto je nezbytné, aby ke každé informaci byl přiřazen vlastník odpovědný za její utajení a za určení osob nebo subjektů, kterým je povolen přístup, a úrovně přístupu, kterou získají. Pro ochranu dat před nežádoucím zveřejněním, změnou a vymazáním se využívají tři metody. (Šulc, 2018)

Data at rest

Pro zajištění bezpečnosti dat v úložišti je důležité, aby k nim měl přístup pouze ten, kdo je k tomu oprávněn. Toho lze dosáhnout řízeným přístupem, který definuje kdo má k datům přístup a jak s nimi může nakládat. Citlivá data by měla být šifrována, aby nemohla být z úložiště odcizena ani poškozena. V případě, že by se útočník pokusil data zničit, je důležité je zálohovat a archivovat v geograficky vzdálené lokalitě. Narušení integrity dat lze zabránit podepisováním dat, nebo vytvářením kontrolních součtů. Pokud se data již nepotřebují, je důležité je bezpečně zlikvidovat, aby je útočník nemohl snadno obnovit. (Šulc, 2018)

Data in motion

Během přenosu dat může dojít k jejich úniku, poškození nebo ztrátě. Aby se tomu zabránilo, je důležité data během přenosu zabezpečit. Jedním z nejdůležitějších opatření je šifrování dat. Šifrování data zakódovává tak, aby je bylo možné přečíst pouze s příslušným klíčem. To chrání data před neoprávněných přístupem. Dalším opatřením je číslování zpráv, které umožňuje sledovat pořadí zpráv a zabránit jejich záměně. Pro ochranu před nežádoucími změnami lze data podepsat, což umožňuje identifikaci zfalšované, nebo upravené zprávy. (Šulc, 2018)

Data in use

Největším rizikem pro data jsou uživatelé, kteří je vytvářejí a používají. Uživatelé mají k datům legitimní přístup, který však mohou zneužít. Proto je důležité monitorovat jejich aktivity v systému. Uživatel potřebuje oprávnění k tomu, aby mohl s daty pracovat. V některých případech však může mít přístup k datům, aniž by k nim měl mít oprávnění pokud k nim přistupuje prostřednictvím aplikace. Aby se zabránilo úniku dat, měla by být monitorována

aktivita uživatelů v systému. Bezpečnostní audity by měly zachytávat podezřelé chování, jako je například neoprávněný přístup k datům, změna dat a jejich zneužití. (Šulc, 2018)

2 INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE

Informační a komunikační technologie (ICT) představují soubor nástrojů a systémů, které tvoří základ moderní výpočetní techniky. Jejich cílem je zefektivnit způsob, jakým lidé pracují s informacemi a daty, ať už je vytváření, zpracovávají, nebo sdílejí. Informační a komunikační technologie zahrnují všechna zařízení, síťové komponenty a aplikace, které umožňují lidem a organizacím komunikovat v digitálním světě. Svět ICT je rozsáhlý a dynamický. Skládá se z široké škály technologií, které umožňují komunikaci, sdílení data a propojení na globální úrovni. Mezi ně patří jak zavedené technologie, které jsou známé a používané denně, tak i nově vznikající technologie. (Awati a Pratt, 2023)

2.1 Informační technologie

Mezi informační technologie patří hardware a software. Technické a programové vybavení se vzájemně doplňuje. (Awati a Rosencrance, 2021)

Hardware označuje všechny fyzické součásti analogového nebo digitálního počítače. Termín hardware odlišuje hmotné aspekty počítačového zařízení od softwaru, který se skládá z programů a instrukcí. Software řídí funkčnost hardwaru a udává mu, co má dělat a kdy má dané instrukce provést. Počítačové komponenty se dělí na vnitřní a vnější. Obecně platí, že vnitřní komponenty jsou nezbytné pro základní chod počítače, zatímco vnější komponenty slouží k rozšíření jeho funkcí. (Awati a Rosencrance, 2021)

Vnitřní komponenty spolupracují na zpracování a ukládání instrukcí z programů a operačního systému. Patří mezi ně základní deska, která nese procesor a další nezbytné komponenty. Funguje jako centrální uzel pro propojení všech součástí. Procesor je mozek počítače, který zpracovává a vykonává instrukce z programů. Jeho frekvence určuje výkon a efektivitu. Paměť RAM slouží jako dočasné úložiště pro rychlý přístup k datům používaných programy. Po vypnutí počítače se data z RAM vymažou. Pevný disk je fyzické úložiště pro trvalé i dočasné datové soubory, jako jsou programy, operační systém, soubory zařízení atd. Optické jednotka umožňuje číst a zapisovat data na optická média, jako jsou CD a DVD. SSD disk je moderní úložiště založené na flash paměti, které je rychlejší a odolnější než klasické pevné disky. Chladič pomáhá odvádět teplo z komponent, aby se zabránilo jejich přehřátí a poškození. Grafická karta zpracovává grafická data a umožňuje zobrazovat obraz na monitoru. U náročnějších úloh doplňuje a odlehčuje procesor. Síťový adaptér, nazývaná také karta síťového rozhraní (NIC) umožňuje počítači připojit se k síti. Jedná se o desku plošných spojů, nebo čip, který obvykle podporuje připojení k síti Ethernet. Mezi další typy

vnitřních komponentů patří porty USB, napájecí zdroj, tranzistory a čipy. (Awati a Rosencrance, 2021)

Software je soubor instrukcí, dat a programů, které řídí chod počítače a plní zadané úkoly. Představuje protiklad hardwaru, který zahrnuje fyzické komponenty počítače. Software je obecný pojem pro aplikace, skripty a programy spustitelné v zařízení. Dřívější software byly vyvíjeny pro konkrétní počítače a prodávány v sadě s hardwarem, na kterém fungovaly. V 80. letech 20. století se software začal šířit na disketách a později na CD a DVD. V dnešní době se většina programů kupuje a stahuje online. Software lze najít na internetových stránkách prodejců, nebo poskytovatelů aplikačních služeb. Mezi nejčastěji používané typy softwaru patří následujících 5 typů:

Aplikační software, který je nejběžnějším typem softwaru. Jedná se o soubor počítačových programů, které plní specifické funkce pro uživatele, ať už přímo, nebo v interakci s jinými aplikacemi. Aplikace může fungovat samostatně, nebo se skládat z více programů, které spolupracují na dosažení požadovaného výsledku. (Rosencrance, 2021)

Systémový software představuje klíčovou součást fungování počítače. Jedná se o programy, které zajišťují chod aplikačního softwaru a hardwarových komponentů. Systémový software slouží jako koordinátor, řídí vzájemnou spolupráci hardwaru a softwaru a vytváří platformu pro bezproblémový chod všech typů programů. Operační systém je stěžejním příkladem systémového softwaru. Plní funkci řídícího centra, dohlíží na chod všech ostatních programů v počítači. Mezi další důležité typy systémového softwaru patří Firmware, překladače počítačových jazyků a systémové nástroje. (Rosencrance, 2021)

Tabulka 1 – Komparace Systémového a Aplikačního SW (Rosencrance, 2021)

Vlastnosti	**Systémový software**	**Aplikační software**
Účel	Řídí základní funkce počítače a umožňují běh aplikačního SW	Vykonává specifické funkce pro uživatele
Příklady	Operační systém, ovladače zařízení, firmware	Grafické programy, webové prohlížeče
Typ jazyka	Nízko úrovňový jazyk (assembler)	Vysoko úrovňový jazyk (Java, Python)
Interakce s hardwarem	Přímá interakce s HW	Nepřímá interakce s HW
Uživatelské rozhraní	Obvykle nemá uživatelské rozhraní	Má uživatelské rozhraní, se kterým uživatel pracuje
Přístup uživatele	Uživatel nemá obvykle přímý přístup	Uživatel má přímý přístup a aktivně ho používá
Závislost	Aplikační SW závisí na systémovém SW	Systémový SW nezávisí na aplikačním SW

Software ovladačů, známý také jako ovladače zařízení je nedílnou součástí systémového softwaru. Jeho úkolem je zajišťovat plynulou komunikaci mezi operačním systémem a hardwarem, čímž umožňuje periferním zařízení a komponentů, plnit jejich specifické funkce. Každé zařízení vyžaduje pro svou správnou funkci alespoň jeden ovladač. (Rosencrance, 2021)

Middleware je software, který slouží jako most mezi různými vrstvami softwaru. Zprostředkovává komunikaci mezi aplikačním a systémovým softwarem a také mezi různými typy aplikačního softwaru. Middleware umožňuje například systému Microsoft Windows komunikovat s aplikacemi Excel a Word. Umožňuje odeslat požadavek na vzdálenou práci z aplikace v počítači s jedním operačním systémem do aplikace v počítači s jiným operačním systémem. Middleware umožňuje také novějším aplikacím pracovat se staršími. (Rosencrance, 2021)

Programovací software je nepostradatelný pomocník programátorů. Slouží k psaní a vývoji softwaru. Nabízí sadu nástrojů, které usnadňují a zefektivňují práci vývojářů. Mezi funkce programovacího softwaru patří psaní kódu, vývoj programů a testování. (Rosencrance, 2021)

2.2 Typy počítačových sítí

Počítačové sítě představují soubor počítačů a dalších zařízení, která se vzájemně propojují a sdílejí informace. Taková infrastruktura, ať už kabelová nebo bezdrátová umožňuje uživatelům bezproblémově komunikovat a sdílet data. Uživatelé tak mohou přistupovat k informacím a službám na jiných počítačích v síti, nebo sdílet informace a služby s ostatními uživateli. Počítačové sítě se vyskytují v široké škále velikostí a konfigurací a to od malých sítí, do kterých patří domácí a kancelářské sítě, přes středně velké sítě, do kterých patří školní a firemní sítě až po velké sítě jako je internet. (Nováček, 2023)

Počítačové sítě se dělí do pěti hlavních kategorií podle jejich rozlehlosti:

- Osobní síť (PAN) – Představuje typ počítačové sítě zaměřený na krátkodosahovou a nenáročnou komunikaci v okruhu maximálně desítek metrů. Slouží k propojení osobních zařízení, jako jsou chytré telefony, tablety, notebooky a stolní počítače s dalšími periferními zařízeními. (Yasar, 2022)
- Lokální síť (LAN) – Je typ počítačové sítě, který propojuje zařízení v omezené geografické oblasti, jako je domácnost, kancelářská budova, nebo školní areál. V praxi se jedná o skupinu vzájemně propojených zařízení, zahrnující počítače, servery, tiskárny a síťová úložiště. Propojení probíhá buď pomocí kabelů, nebo bezdrátově pomocí Wi-Fi. (Nováček, 2023)
- Metropolitní síť (MAN) – Jedná se o typ počítačové sítě, který pokrývá rozsáhlejší oblast, typicky v rámci jednoho města, nebo obce. Slouží k propojení lokálních sítí (LAN) a umožňuje tak sdílení dat a komunikaci v rámci většího celku. (Wright, 2021)
- Rozsáhlá síť (WAN) – Představuje typ počítačové sítě, která propojuje zařízení v rozsáhlé geografické oblasti. V praxi se jedná o propojení sítí LAN a MAN pomocí vysokorychlostních komunikačních kanálů, které bývají založeny na optických kabelech, nebo satelitním spojení. (Scarpati, 2023)

- Globální síť (GAN) – Představuje typ počítačové sítě, která propojuje zařízení v celosvětovém měřítku. Tyto sítě využívají satelitní technologie, nebo vysokorychlostní podmořské kabely k překonání velkých vzdáleností a zajištění bezproblémového propojení. (Nováček, 2023)

Počítačové sítě lze rozdělit podle přenosového média na drátové sítě a bezdrátové sítě. Drátové sítě se dále dělí podle jejich materiálu na:

- Koaxiální kabel – Je složen z vnitřního vodiče obklopeného vnějším krytem. Tato struktura umožňuje efektivní přenos velkých objemů dat vysokou rychlostí (Nováček, 2023).
- Měděný kabel – Je typ kabelu, jehož jádro tvoří vodiče z mědi, která se vyznačuje vynikající vodivostí a odolností. Kabel se dále dělí na nechráněnou kroucenou dvojlinku (UTP), která se používá v domácnostech a kancelářích a sítěnou kroucenou dvojlinku (STP), která je odolnější proti rušení, a proto ideální pro přenos citlivých dat. (Nováček, 2023)
- Optický kabel – Odlišuje se od běžných kabelů tím, že k přenosu dat využívá světlo namísto elektrického signálu. Světlo putuje vlákny z průhledného materiálu, obvykle skla nebo plastu, které je vedou s minimálním úbytkem. Tato technologie umožňuje dosahovat velmi vysokých rychlostí a bezkonkurenční spolehlivosti. (Nováček, 2023)

Datové signály mohou cestovat bezdrátově za pomocí elektromagnetických vln. Zařízení se k síti mohou připojit bezdrátově, bez nutnosti používání kabelů. Bezdrátové sítě se dělí na:

- Wi-Fi – Je bezdrátová technologie, která k odesílání dat používá rádiové vlny. Používá dvě hlavní frekvenční pásma: 2,4 GHz a 5 GHz. První pásmo má delší dosah, ale je náchylnější k rušení. Druhé pásmo má kratší dosah, ale je rychlejší a méně náchylné k rušení. (Nováček, 2023)
- Bluetooth – Umožňuje bezdrátové propojení elektronických zařízení. Funguje podobně jako WiFi, ale má kratší dosah vzdálenosti a nižší spotřebu energie. (Nováček, 2023)

Počítačové sítě se rozlišují podle uspořádání jejich vzájemného propojení, neboli topologie. Sítě Peer-to-peer představují model, ve kterém všechny počítače (uzly) spolupracují rovnocenně. Není zde žádný centrální server, který by řídil provoz a ukládání dat. Jednotlivé uzly

si tak předávají data a úkoly mezi sebou bez potřeby zprostředkovatele. Klient-server je princip fungování sítí, kde jeden nebo více počítačů slouží jako server. Ostatní počítače v síti pak vystupují jako klienti. Klienti se připojují k serveru a žádají o data nebo služby. Server jim následně poskytuje požadované informace nebo funkce. Tento model se běžně používá v organizacích a institucích, kde je důležitá silná centralizace a kontrola přístupu k datům. (Yasar, Gillis, 2023)

Počítačové sítě lze dělit podle vlastnictví na:

- Veřejné sítě – Jsou vlastněny a provozovány nezávislými organizacemi, nebo vládou (např. internet.)
- Soukromé sítě – Jsou vlastněny a provozovány jednou organizací pro interní potřeby, příkladem je firemní síť.
- Hybridní sítě – Kombinují prvky veřejných a soukromých sítí. Příkladem je připojení soukromé sítě k internetu. (Nováček, 2023)

Počítačové sítě se dělí podle bezpečnosti na:

- Sítě s vysokou bezpečností – Jsou konstruovány s cílem chránit citlivá data před neoprávněným přístupem, zneužitím a krádeží. Často se uplatňují v kritických oblastech, jako je bankovnictví, státní správa, armáda nebo zdravotnictví. Mezi hlavní prvky zabezpečení patří Firewally, šifrování, autentizace a další bezpečnostní prvky. (Nováček, 2023)
- Sítě s normální bezpečností – Slouží k ochraně běžných dat před neoprávněným přístupem. Nachází se v běžných podnikových aplikacích a v domácnostech. Mezi prvky zabezpečení patří Firewally a další základní bezpečnostní prvky. (Nováček, 2023)
- Sítě s nízkou bezpečností – Nekladou důraz na ochranu dat před neoprávněným přístupem. Používají se v nekritických aplikacích a testovacích prostředcích. Obvykle neobsahují žádné, nebo jen minimální bezpečnostní prvky. (Nováček, 2023)

2.3 Data a Internetový protokol

Data jsou jakékoli sdělení, poznatky, nebo pojmy, které jsou převedeny do formátu, se kterými dokáže pracovat počítač. To zahrnuje i programy, které počítači dávají instrukce, co má dělat. Data lze chápat jako zachycené skutečnosti, mezi které patří čísla, události, grafy,

mapy, transakce a tvoří základní stavební jednotku informací. Z pohledu počítače jsou data jakékoli prvky s informační hodnotou, které jsou jím zpracovány. Data se obvykle uchovávají v ucelených souborech, které se liší typem (textové, obrazové, binární). Zpracováním dat vznikají informace, které lze dále využít. Informace jsou zpracovaná data, která jsou užitečná pro příjemce. To znamená, že ne všechna data se nutně stávají informacemi. Teprve když data dostanou kontext a stanou se srozumitelnými, tak je lze označit jako informaci. (Kolouch, 2017)

Internetový protokol slouží na internetu k odesílání dat mezi počítači. Funguje jako sada pravidel, která řídí, jak se data rozdělí na menší části, tzv. pakety a jak se tyto pakety doručí do cílového počítače. Každý počítač připojený k internetu má jedinečnou IP adresu. Tato adresa funguje jako identifikační číslo a umožňuje vzájemnou komunikaci. Jedním z nejdůležitějších transportních protokolů je TCP (Transmission Control Protocol). Porot se IP často označuje také jako TCP/IP. TCP zajišťuje spolehlivou komunikaci mezi počítači. Při posílání a příjímání dat se informace rozdělí na menší části nazývané pakety. Tyto pakety obsahují adresy odesílatele i příjemce. Každý paket se nejprve odešle na tzv. bránu. Brána přečte cílovou adresu v paketu a předá ho další bráně v daném směru. Tento proces se opakuje, dokud jedna brána nerozpozná, že paket patří do sítě, kterou spravuje. Pak ho předá přímo cílovému počítači, jehož adresa je v paketu uvedena. Data se při odesílání rozdělí na pakety, které se mohou posílat přes internet různými cestami. To znamená, že pakety mohou dorazit do cíle v jiném pořadí, než v jaké byly odeslány. O jejich správné seřazení se stará jiný protokol, tzv. protokol řízení přenosu. Internetový protokol se stará pouze o doručení paketů, nezajišťuje jejich pořadí. (Kerner, 2021)

2.4 IP a MAC adresa

IP adresa, neboli adresa internetového protokolu je jedinečný číselný kód, který slouží k identifikaci zařízení, nebo sítě v internetové síti. IP adresu obvykle přiděluje poskytovatel internetových služeb při připojení k internetu. (Kerner, 2021)

Nejrozšířenější verzí protokolu IP je IPv4, který nabízí 32bitový systém adres rozdělený do čtyř částí. Hlavní výhodou IPv4 je snadná implementace a rozšířenost. Nevýhodou je omezený adresní prostor a problém s možným vyčerpáním adres IPv4. (Kerner, 2021)

Protokol IPv6 definuje 128bitový adresový prostor, čímž nabízí podstatně větší kapacitu než protokol IPv4. Adresa IPv6 se skládá z osmi částí. Hlavní předností protokolu je velká dostupnost adresního prostoru. Mezi nevýhody se řadí komplexnost daná rozsáhlým adresním prostorem. Pro správce sítí bývá náročné jej monitorovat a spravovat. (Kerner, 2021)

IP adresy se podle přístupu dělí na:

- Soukromé IP adresy – Všechna zařízení v domácí či firemní síti disponují tzv. soukromou IP adresou. Tyto adresy nejsou viditelné z internetu a slouží pouze pro komunikaci uvnitř dané sítě. Mezi zařízení s privátními IP adresami patří počítače, tablety, chytré telefony, chytré televizory a tiskárny. (Yasar, 2023)
- Veřejné IP adresy – Poskytovatelé internetového připojení přidělují routeru veřejnou IP adresu. Ta umožňuje routeru komunikovat s internetem a s jinými externími sítěmi. Veřejná IP adresa je platná pro celou síť, takže všechna zařízení sdílející jedno internetové připojení budou mít stejnou veřejnou IP adresu. (Yasar, 2023)

Podle způsobu přidělení se rozlišují:

- Dynamické IP adresy – Dynamická IP adresa se neustále mění. Při každém připojení k internetu se zařízení automaticky přidělí nová adresa z fondu IP adres, které vlastní poskytovatel internetových služeb. Poskytovatelé tak šetří náklady a usnadňují si správu sítě. Dynamické IP adresy nabízí také bezpečnostní výhodu, jelikož pro hackery je obtížnější proniknout do zařízení, jehož IP adresa se neustále mění. (Yasar, 2023)
- Statické IP adresy – Statická IP adresa se na rozdíl od dynamické po přidělení nikdy nemění. Většina uživatelů a firem statickou IP nepotřebuje. Statická IP adresa je nezbytná pro firmy, které provozují vlastní webové servery, protože zaručuje, že webové stránky a e-mailové adresy serveru budou vždy dostupné na stejné adrese. (Yasar, 2023)
- IP adresy webových stránek – IP adresy webových stránek se dělí na sdílené a dedikované IP adresy. Sdílená IP adresa je adresa, kterou používá více webových stránek najednou. Většinou ji využívají malé firmy, které spoléhají na spravované hostingové služby. Tyto služby se starají o technickou stránku provozu webových stránek. Dedikovaná IP adresa je jedinečná adresy, která je pevně svázána s jednou webovou

stránkou. Na rozdíl od sdílené IP adresy, kterou používá více webů najednou, dedikovaná adresa zajišťuje maximální kontrolu a stabilitu pro jednu webovou stránku. (Yasar, 2023)

MAC adresa (Media Access Control) je unikátní 12místný kód ve formátu hexadecimálních čísel, který je přidělen každému zařízení připojenému k síti. MAC adresa slouží jako jedinečný identifikátor daného zařízení. Adresa bývá přidělena výrobcem a lze ji nalézt na síťové kartě daného zařízení. MAC adresa je součástí datového spoje v modelu OSI (Open Systems Interconnection). Vkládá se do hlavičky každého datového rámce a slouží k identifikaci odesílatele a příjemce dat v síti. Každé síťové zařízení má vlastní MAC adresu. To znamená, že zařízení s více rozhraními, např. notebook s Ethernetem a Wi-Fi bude mít i více MAC adres. (Yasar, 2022)

Tabulka 2 – Komparace MAC a IP adresy (Yasar, 2022)

Vlastnost	**MAC adresa**	**IP adresa**
Funkce	Identifikace síťových zařízení v lokálním měřítku	Identifikace síťových zařízení na internetu v globálním měřítku
Možnost změny	Nelze změnit	Lze kdykoli změnit
Název	Někdy nazývaná fyzická adresa	Někdy nazývaná logická adresa
Způsob přidělení	Zakódováno do zařízení při výrobě	Přiděleno zařízení pomocí softwarové konfigurace

3 ŘÍZENÍ RIZIK

Existuje mnoho způsobů, jak se vypořádat s riziky v oblasti informační bezpečnosti. Většina organizací ale začíná určením zodpovědné osoby za tuto oblast. Dále se zavádí základní bezpečnostní opatření, a to jak organizační, tak technická. Tato opatření by měla implementovat všechny organizace bez ohledu na jejich velikost, zaměření či obor činnosti. Dalším krokem je analýza rizik a návrh strategie pro jejich zvládnutí. To obvykle zahrnuje implementaci dalších bezpečnostních opatření, ať už organizačních či technologických. Zavedená bezpečnostní opatření by měla být pravidelně revidována a analyzována. V případě zjištění nesouladu s požadavky je nutné včas a adekvátně reagovat. (Smejkal, Sokol a Kodl, 2019)

Pro oblast informační bezpečnosti se doporučuje postupovat dle normy ISO/IEC 27001. Katalog organizačních a technických bezpečnostních opatření v normě ISO/IEC 27002 slouží jako zdroj pro výběr relevantních kroků. Tyto normy shrnují osvědčené postupy a vhodná opatření v oblasti informační bezpečnosti. Dodržování norma ISO/IEC 27001 pomáhá organizacím neopomenout žádnou z 11 klíčových oblastí informační bezpečnosti:

- Bezpečnostní politika.
- Organizace bezpečnosti.
- Klasifikace a řízení aktiv.
- Bezpečnost lidských zdrojů.
- Fyzická bezpečnost a bezpečnost prostředí.
- Řízení komunikací a řízení provozu.
- Řízení přístupu.
- Nákup, vývoj a údržba informačního systému.
- Zvládání bezpečnostních incidentů.
- Řízení kontinuity činnosti organizace.
- Soulad s požadavky. (Smejkal, Sokol a Kodl, 2019)

Manažer bezpečnosti řídící se normou ISO/IEC 27001 by měl pro implementaci systému managementu bezpečnosti informací provést následující kroky:

- Určení rozsahu a hranic systému managementu bezpečnosti informací (ISMS – Information Security Management Systém) a stanovit, které informace a aktiva spadají pod ISMS.
- Stanovit jednotný postup pro posuzování rizik, který povede k hodnocení, které bude vzájemně srovnatelné a v případě opakování povede ke stejným závěrům.
- Realizovat analýzu rizik, identifikovat a kvalifikovat aktiva, hrozby, zranitelnosti a výslední riziko.
- Zvolit optimální strategii pro zvládání rizik a na základě analýzy nákladů a přínosů vybrat adekvátní bezpečnostní opatření s definováním systémem pro měření jejich efektivity.
- Získat schválení managementu pro strategii zvládání rizik a zavedení vybraných bezpečnostních kroků.
- Vytvořit komplexní strategii pro zvládání rizik s ohledem na schválený přístup vedení.
- Implementovat vybraná bezpečnostní opatření, která efektivně sníží rizika na akceptovatelnou úroveň.
- Sepsat bezpečnostní politiku, standardy a směrnice reflektující identifikovaná rizika, zvolená opatření a cíle organizace.
- Posilovat bezpečnostní povědomí mezi zaměstnanci formou kurzů, školení a vzdělávacích aktivit.
- Průběžně monitorovat a hodnotit funkčnost zavedených opatření a navrhnout kroky pro jejich optimalizaci.
- Pravidelně opakovat analýzu rizik s ohledem na dynamické změny v prostředí.
- Realizovat interní audity pro kontrolu a zlepšování bezpečnostního systému.
- Zavádět inovativní a efektivnější opatření na základě analýzy rizik, interních auditů a hodnocení účinnosti jednotlivých kroků.
- Provádět průběžnou aktualizaci a optimalizaci jednotlivých postupů a navazujících dokumentů. (Smejkal, Sokol a Kodl, 2019)

3.1 Oblast působnosti

Zlepšování kybernetické bezpečnosti organizace představuje kontinuální proces, jehož úspěch závisí na jasné definovaném rozsahu. V počáteční fázi může organizace postrádat dostatečné zdroje nebo zkušenosti pro komplexní řešení kybernetické bezpečnosti. V takovém případě je vhodné se zaměřit na oblasti s nejvyšším vnímaným rizikem a postupně rozšiřovat rozsah dle dostupných zdrojů a rostoucích zkušeností. Důležité je, aby se omezené zdroje soustředily na skutečně rizikové oblasti. Proto je nezbytné formálně a s důrazem na širokou škálu názorů definovat oblasti s nejvyšším rizikem. (Clark, Hakim, 2017)

3.2 Aktiva

V oblasti kybernetické bezpečnosti se termín informační aktiva používá pro označení všech informačních zdrojů organizace, které je nutné chránit před kybernetickými útoky. Patří sem datové zdroje, software, hardware, sítě, nástroje a i méně hmatatelné aspekty jako pověst a postavení na trhu. Organizace kritické infrastruktury sdílí běžná informační aktiva s jinými typy firem, ale také disponují specifickými aktivy, jako jsou procesní zařízení a řídící systémy. Rozsah systému kybernetické bezpečnosti se definuje určením, která informační aktiva budou zahrnuta, a která ne. V ideálním případě je vhodné chránit co nejvíce aktiv, avšak v praxi je nutné zohlednit i náklady a efektivitu, pro organizace, které se s kybernetickou bezpečností teprve seznamují, je vhodné začít s projektem zaměřeným na nejkritičtější rizika a postupně rozšiřovat chráněná aktiva. Informační aktiva v kontextu kybernetické bezpečnosti podléhají různým bezpečnostním požadavkům. Mezi nejdůležitější patří důvěrnost (ochrana před neoprávněných přístupem), integrita (ochrana před neautorizovanými změnami) a dostupnost (zajištění nepřetržitého přístupu pro oprávněné uživatele). (Clark, Hakim, 2017)

Aktiva lze rozdělit do dvou kategorií:

Primární/hlavní aktiva organizace – Zahrnují informace a procesy, které jsou klíčové a nezbytné pro dosažení cílů. Jedná se o hlavní zdroje hodnoty organizace, které ji odlišují od konkurence a umožňují jí fungovat. (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

Podpůrná aktiva – Jsou nedílnou součástí informačního systému a zajišťují fungování hlavních aktiv organizace. Bez podpůrných aktiv by hlavní aktiva nemohla existovat, nebo fungovat správně. (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

Hlavní a podpůrná aktiva jsou vzájemně propojená. Proto rizika identifikovaná u podpůrných aktiv mohou negativně ovlivnit i hlavní aktiva organizace. Z tohoto důvodu je nezbytné správně identifikovat vztahy mezi aktivy a porozumět jejich důležitosti pro organizaci. Nesprávné posouzení důležitosti aktiva může vést k nesprávnému posouzení dopadů souvisejících s rizikem. Dále také může ovlivnit pochopení pravděpodobnosti zvažovaných hrozeb. (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

3.3 Důvěrnost

Důvěrnost informačního aktiva spočívá v tom, že k němu mají přístup pouze osoby oprávněné vlastníkem aktiva. Mezi příklady informačních aktiv s požadavkem na důvěrnost patří obchodní tajemství, údaje o klientech a personální data. Důvěrnost uložených dat lze zajistit šifrováním. Šifrovat se dá jak soubor, databáze, tak i celý disk. Mezi nástroje pro šifrování patří BitLocker, který je integrovaný do operačního systému Windows a podporuje šifrovací standard AES (Advanced Encryption Standard) s délkou klíče 128 a 256 bitů. Čím delší je klíč, tím obtížnější je prolomení šifry. Důvěrnost dat během přenosu lze chránit pomocí protokolů pro šifrování dat, jako je IPsec (Internet Protocol Security. IPsec je sada internetových protokolů (IP) pro zabezpečení komunikace, která zajišťuje ověřování a šifrování každého paketu IP v rámci komunikační relace. (Clark, Hakim, 2017)

3.4 Integrita

Integrita aktiva je ohrožena, pokud dojde k jeho neoprávněné změně. Například informace v databázi se mohou znehodnotit náhodným poškozením nebo úmyslným zásahem neoprávněných osob. Bez ohledu na příčinu, je ochrana neporušenosti informačních aktiv před neoprávněnými nebo nechtěnými změnami klíčovou součástí kybernetické bezpečnosti. Zachování neporušenosti aktiv u zdroje je možné zavedením řízení přístupu, procesů a konfigurace. Během přenosu dat lze neporušenost zajistit pomocí hashovacích algoritmů, nebo cyklických algoritmů redundanční kontroly pro detekci poškození. (Clark, Hakim, 2017)

3.5 Dostupnost

Dostupnost informačního aktive je definována jako možnost oprávněných osob získat spolehlivé a aktuální informace o daném aktivu. V praxi se k zajištění dostupnosti dat používají různé technologie, například redundantní pole disků, které kombinuje více disků do jednoho logického celku. I v případě selhání jednoho disku tak data zůstávají dostupná. Počítačové sítě a systémy se skládají z mnoha komponent, které musí spolupracovat, aby byla zajištěna

dostupnost dat pro oprávněné uživatele. Základním cílem kybernetické bezpečnosti je chránit důvěrnost, integritu a dostupnost informačních aktiv. (Clark, Hakim, 2017)

3.6 Hrozby

Hrozby pro kybernetickou bezpečnost organizace, která se týká jejich aktiv, mohou mít různé zdroje. Základní rozdělení rozlišuje dvě hlavní kategorie, do kterých patří hrozby pocházející od lidského faktoru a hrozby nelidského původu. Hrozby pocházející od lidského faktoru pak mohou pocházet z různých zdrojů. Jednat se může o interní hrozby od zaměstnanců organizace, nebo externí hrozby osob mimo organizaci. Lidské zdroje hrozeb lze rozdělit do skupin na základě kritérií, jako je přístup k aktivům, dovednosti a motivace. Například hrozby od administrativních pracovníků se liší od hrozeb pracovníků IT. Důvodem je odlišný přístup k aktivům a rozdílné dovednosti. Proto může organizace rozdělit skupinu zaměstnanci na obecné zaměstnance a zaměstnance IT. Seskupení zdrojů hrozeb usnadňuje posuzování a zvládání rizik. (Clark, Hakim, 2017)

3.7 Rizika

Riziko lze definovat jako událost, která může negativně ovlivnit dosažení stanovených cílů. Závažnost rizika je určena pravděpodobností, že dané riziko nastane a rozsahem negativních dopadů. (Refsdal, Solhaug a Stølen, 2015)

Pro každé identifikované riziko může organizace vyhodnotit škálu potenciálních reakcí:

Akceptace – K akceptaci rizika dochází v situaci, kdy organizace dojde k závěru, že neexistují efektivní a finančně dostupné metody snížení pravděpodobnosti výskytu dané události, nebo zmírnění jejích dopadů. V takovém případě se organizace rozhodne akceptovat zbylé riziko. (Clark, Hakim, 2017)

Vyhýbání se rizikům – Pro skutečné vyhnutí se riziku je obvykle nezbytné transformovat fungování organizace tak, aby se dané riziko vůbec neprojevilo. Může se jednat například o ukončení specifické aktivity z důvodu nepřijatelně vysokého rizika. (Clark, Hakim, 2017)

Ošetření/zmírnění rizik – Základ kybernetické bezpečnosti spočívá v ošetření a zmírnění rizik. Toho se dosahuje implementací kontrolních mechanismů, které buď snižují pravděpodobnost, nebo dopad kybernetické hrozby. V ideálním případě se kombinují oba přístupy, čímž se celkové riziko pro dané aktivum dostává do mezí tolerance dané organizace. (Clark, Hakim, 2017)

Převod rizika – Jedná se o běžný koncept, který se vyskytuje v pojištění. V tomto případě se pojišťovna za poplatek zavazuje, že v případě pojistné události vyplatí pojištěnému finanční kompenzaci. Tento princip lze s jistými omezeními aplikovat i v oblasti kybernetické bezpečnosti. Přenos rizika může zmírnit dopad kybernetické hrozby, ale neřeší všechna rizika. U organizací kritické infrastruktury je důležité chránit jak hmotná tak i nehmotná aktiva, jako je dobré jméno a reputace. (Clark, Hakim, 2017)

Tabulka 3 – Stupnice hodnocení rizik (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

Úroveň rizika	**Hodnocení rizika**	**Popis**
Nízké	Přijatelné tak, jak je	Riziko lze přijmou bez dalších opatření.
Střední	Snesitelné pod kontrolou	Provedení kontroly z hlediska managementu rizik, stanovení činností v rámci neustálého zlepšování ve střednědobém a dlouhodobém horizontu.
Vysoké	Nepřijatelné	V krátkodobém horizontu přijmou opatření ke snížení rizika. Zvážit odmítnutí aktivity, pokud není možné riziko adekvátně snížit.

3.8 Metody posuzování technických zranitelností

K odhalení slabých míst v informačním systému lze využít preventivní přístupy, jako je testování daného systému a to v závislosti na důležitosti systému informačních a komunikačních technologiích a dostupných zdrojích. Testovací metody zahrnují automatický nástroj pro skenování zranitelnosti, testování a hodnocení bezpečnosti, penetrační testování a přezkoumání kódu. (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

Automatický skener zranitelností se používá k prohledání skupiny počítačů, nebo sítě za účelem nalezení známých zranitelných služeb. Mezi příklady zranitelných služeb patří systémy umožňující anonymní přenos souborů, nebo přeposílání zpráv pomocí aplikace Sendmail. Některé z potenciálních zranitelností a služeb, které automatický skener najde nemusí ve skutečnosti představovat hrozbu v kontextu daného systému. Důvodem je hodnocení potenciálních zranitelností bez ohledu na specifické prostředí a požadavky daného webu. (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

Testování a hodnocení bezpečnosti je další metodou, kterou lze využít k odhalení slabých míst v systému ICT v rámci procesu posuzování rizik. Spočívá ve vytvoření a realizaci testovacího plánu, který zahrnuje testovací skripty, postupy a očekávané výsledky. Cílem testování bezpečnosti je ověřit efektivnost bezpečnostních mechanismů systému ICT v reálném provozním prostředí. Smyslem je zajistit, aby implementovaná opatření odpovídala schválené bezpečnostní specifikaci pro software a hardware, a aby byla v souladu s bezpečnostní politikou organizace. (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

Penetrační testování může sloužit jako doplňková metoda k revizi bezpečnostních opatření a k ověření zabezpečení různých aspektů systému ICT. Pokud se penetrace provede v rámci procesu posuzování rizik, umožní posoudit odolnosti systému ICT proti záměrným pokusům o obejití jeho ochrany. Cílem penetračního testování je prověřit systém ICT z pohledu potenciálního útočníka a odhalit případná selhání v jeho ochranných mechanismech. Analýza zdrojového kódu představuje nejdetailnější metodu odhalení zranitelností. (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023)

4 DATOVÉ MODELOVÁNÍ PŘI NAVRHOVÁNÍ APLIKACE

Data představují klíčový zdroj pro fungování informačního systému. Jejich struktura, kvalita a komplexnost ovlivňují efektivitu jak informačních technologií, tak i projektů informačních systémů. Z tohoto důvodu je nezbytné, aby při tvorbě datových modelů věnovali mimořádnou pozornost jak management, tak i systémoví analytici. Data a algoritmy tvoří základ informačního systému. Modelování dat a algoritmů tak představuje samotnou podstatu modelování informačního systému. (Kaluža a Kalužová, 2012)

Životní cyklus vývoje informačního systému má následující strukturu:

1. Identifikace a výběr projektů – v této fázi se definuje potřeba nového systému, požadavky uživatelů, obchodní cíle a priority vývoje.
2. Zahájení a plánování projektů – v této fázi se detailně specifikují jednotlivé projekty, určí se tým pro řešení problémů, potřebné zdroje a časový harmonogram dalšího postupu. Vedení organizace schvální realizaci projektů.
3. Analýza současného stavu – provádí se kritická analýza stávajícího informačního systému s cílem identifikovat jeho nedostatky a možnosti zdokonalení. Poznatky z analýzy se porovnávají s požadavky uživatelů a analyzuje se stav využití informačních technologií. Formulují se alternativy návrhu nového řešení.
4. Návrh (projektování) nového řešení – v této fázi se vytváří nový systém, navrhují se nové struktury, vstupní formuláře a výstupní sestavy, dialogy, algoritmy a programové řešení. Někdy se rozlišuje mezi logickým a fyzickým návrhem. Logický návrh je nezávislý na technologické platformě, zatímco fyzický návrh je úzce spjat s programovaným a hardwarovým prostředím.
5. Zavedení (implementace) nového řešení – provádí se testování programů, instalace konečné verze softwaru, finalizace dokumentace, školení uživatelů, zkušení provoz systému a jeho předání k běžnému provozu.
6. Údržba systému – systém se upravuje v důsledku změny vnějších podmínek, odstraňují se skryté závady a zlepšují se jeho funkce. (Kaluža a Kalužová, 2012)

Datové modelování se řadí do třetí a čtvrté fáze, tedy do analýzy a návrhu. V rámci analýzy současného stavu se stanový výchozí datový model a jeho konkretizace v tzv. logické podobě proběhne v etapě návrhu nového řešení. Je důležité zdůraznit, že datové modelování

nezahrnuje všechny činnost týkající se dat v rámci vývoje informačního systému. Mimo oblast datových modelů stojí návrhy vstupních formulářů, výstupních sestav, řešení chybových reportů, číselníků atd. Zdroje informací pro datové modelování vznikají již v raných fázích etapy analýzy současného stavu při mapování datových toků, kdy jsou identifikovány vedle datových toků i jejich úložiště v nejrůznějších formách: v souborech, databázích a archivech. (Kaluža a Kalužová, 2012)

Vědecké obory, které se rychle rozvíjejí, se potýkají s nejednotností terminologie. Platí to i pro oblast modelování dat. Běžně používané pojmy bývají interpretovány různě. Existují dva hlavní přístupy k tomuto pojmu, přičemž někteří autoři ho používají volně bez bližšího definování. První přístup chápe datový model jako nástrojový koncept. Definuje ho jako formální systém s objekty, pravidly integrity a operátory. Odmítá chápat model jako strukturu dat. Druhý přístup vnímá datový model jako strukturu modelující konkrétní systém. Definuje ho jako souhrn konceptů pro popis množiny dat a operací pro manipulaci s nimi. Z hlediska praktického modelování dat je vhodnější druhý přístup. Datový model je pak abstrakcí, odrazem reálného světa z pohledu vývojáře, který realizuje cíle projektu. (Kaluža a Kalužová, 2012)

4.1 Víceúrovňový přístup k modelování dat

Realita, kterou se vývojář zabývá, je modelována pomocí abstrakce. Abstrakce zohledňuje cíl modelu a zachycuje v něm podstatné rysy reality, zatímco ostatní ignoruje. Různé cíle vyžadují různé abstrakce. Každá abstrakce je ale ovlivněna myšlenkovou koncepcí, takže k podobnému výsledku lze dojít různými cestami. Preferovat určitou koncepci jen proto, že ji někdo nejlépe zná a o jiných má jen mlhavé znalosti, je nevědecké. V praxi vítězí co nejjednodušší a nejefektivnější cesta. (University of Bristol, 2024)

4.2 Tříúrovňová koncepce

Tříúrovňová koncepce datového modelování zahrnuje sémantickou, konceptuální a logickou úroveň procesu.

Sémantická úroveň

Základní vrstvou modelování je sémantická úroveň, která odráží modelovanou realitu. Prvky reality relevantní pro vyvíjený systém budou označovány jednoduše jako typy objektů. Tato vrstva se zaměřuje výhradně na strukturu typů objektů. Každý typ objektu musí být popsán slovně. Jedná se o první zachycení reality, kdy se abstrahují nepodstatné rysy a modelují se

pouze podstatné prvky – typy objektů. V tomto stadiu není zaručen další vývoj identifikovaného typu objektu: může zaniknout, splynout s jiným typem objektu, nebo se rozdělit do více navazujících prvků modelu. (Kaluža a Kalužová, 2012)

Konceptuální úroveň

Konceptuální úroveň modelování vychází ze specifikované struktury typů objektů. Z hlediska formy popisu i použitých prvků navazuje na zavedenou praxi E-R modelů a diagramů tříd. Jedná se o grafické znázornění struktury entit (tříd) a vztahů mezi nimi. V případě trojvrstvé koncepce modelování tato struktura vzniká transformací odpovídajících typů objektů sémantického modelu. (Agar, 2021)

Logická úroveň

Třetí úroveň představuje logické modelování, které je úzce spjato s konkrétní databázovou koncepcí. Na základě dosavadního vývoje můžeme rozlišovat následující databázové koncepce:

- Hierarchická.
- Síťová.
- Relační.
- Objektová.
- Objektově relační. (Agar, 2021)

Fyzická úroveň

Fyzický datový model představuje finální podobu datového fondu, která je implementována v konkrétním databázovém systému. Vychází z logického datového modelu vytvořeného správci a vývojáři databáze a dále jej rozvíjí s ohledem na specifické technologie a požadavky daného prostředí. (Microsoft, 2024)

4.3 Sémantický datový model

Koncept umožňuje prozkoumání informací v informačním systému strukturou relevantní pro daný systém. Strukturované modely pomáhají analytikům s dotazováním přirozeným způsobem, podobně jako při kladení otázek o fungování systému. Efektivní modely jsou snadno použitelné a pochopitelné, čímž usnadňují práci s daty a abstrahují od komplexnosti datové struktury. (ORACLE, 2024)

Metoda abstrakce hraje klíčovou roli při tvorbě datových modelů. Cílem modelování v této oblasti je identifikovat a strukturovat relevantní koncepty, které odrážejí specifika kybernetických hrozeb a jejich dopadů. Jak ale tyto koncepty nalézt? Zásadní je důkladné prozkoumání oblasti zájmu, a to jak z obecného hlediska, tak i v detailech. To zahrnuje analýzu typů kybernetických útoků, zranitelných systémů, potenciálních cílů a dalších relevantních faktorů. Datový model se nezaměřuje na individuální incidenty, ale na obecné kategorie a jejich vlastnosti. Například místo modelování specifických malware vzorků se model zaměří na obecné vlastnosti malware, jako jsou typ šíření, funkce, cíl a detekovatelnost.

Mezi tři typy abstrakce, které lze specifikovat při sémantickém a konceptuálním modelování, patří klasifikace, agregace a generalizace.

Klasifikace hraje klíčovou roli při identifikaci a pochopení aktiv, která je nutné chránit. Pomocí klasifikace lze systematicky roztřídit aktiva do kategorií na základě jejich vlastností, jako jsou typ aktiva, citlivost dat, hodnota aktiva a kritičnost pro fungování informačního systému. (Kaluža a Kalužová, 2012)

Agregace slouží k seskupování aktiv do logických celků na základě společných vlastností a funkcí. To umožňuje zjednodušit a zefektivnit analýzu rizik a implementaci bezpečnostních opatření. (Kaluža a Kalužová, 2012)

Generalizace představuje proces abstrakce, který umožňuje definovat vztahy mezi různými typy kybernetických hrozeb. To umožňuje shromažďovat a analyzovat data z různých zdrojů a identifikovat trendy a vzorce, které by mohly vést k potenciálním kybernetickým útokům. Uvedené tři typy abstrakce na sobě nejsou závislé. Z praktického hlediska se při tvorbě datového modelu uplatňují primárně abstrakce klasifikace a agregace. Ty slouží k definování struktury datových typů sémantického modelu včetně jejich komponent na základě analýzy požadavků na vstupní data. (Kaluža a Kalužová, 2012)

4.4 Formy analýzy datových požadavků

Získávání vstupních dat pro analýzu rizik kybernetické bezpečnosti je klíčové pro pochopení hrozeb, kterým informační systém čelí, a pro zavedení efektivních kontrol. Existuje několik základních metod, které lze použít k identifikaci a analýze požadovaných dat:

- Rozhovorem vývojáře s uživateli systému.
- Rozborem písemných materiálů.
- Dotazníky.

- Pozorováním. (Kaluža a Kalužová, 2012)

Vzhledem k důkladnosti a systematičnosti mají první dvě formy analýzy zásadní význam pro tvorbu datových modelů.

Dotazníková metoda slouží spíše jako doplňkový a volitelný nástroj pro sběr dat v analýze rizik kybernetické bezpečnosti. Její hlavní nevýhodou je absence interaktivní interakce mezi tazatelem a respondentem, která umožňuje hlubší prozkoumání daného tématu. I sebepečlivěji vypracovaný dotazník nedokáže předvídat všechny rozdíly a detaily v odpovědích respondentů, čímž omezuje možnosti následného zkoumání. Využití dotazníků se tak hodí spíše do úvodní fáze analýzy. Hlavní předností dotazníkové metody je nízká cena v případě dotazování velkého počtu respondentů. To z ní dělá vhodný nástroj pro rychlé shromáždění obecných informací od široké skupiny respondentů. Pro hlubší a detailnější analýzu rizik je však nutné dotazníkovou metodu kombinovat s jinými metodami sběru dat, jako jsou rozhovory, analýza písemných materiálů a pozorování. (Kaluža a Kalužová, 2012)

Metoda pozorování umožňuje sledovat chování uživatelů v reálném pracovním prostředí. Nabízí tak cenný vhled do toho, jak uživatelé skutečně pracují s daným systémem a jaká rizika kybernetické bezpečnosti s sebou jejich chování nese. Z praktického hlediska se jedná o doplňkovou formu sběru dat z důvodu vysoké časové náročnosti, vyšší nákladnosti, nižší spolehlivosti a obtížnosti získání komplexního přehledu. (Kaluža a Kalužová, 2012)

Rozhovory systémových analytiků s uživateli systému vedou k popisu zkoumané reality v přirozené řeči. Tyto rozhovory jsou samozřejmě řízené a sledují cíle projektu, čímž se snaží odhalit skutečné potřeby uživatelů. Hlavní výhodou volného popisu a neomezené možnosti charakterizace jakéhokoli pozorovaného jevu je jeho přirozenost. Nespornou předností rozhovoru je osobní kontakt tazatele a respondenta, který zaručuje zodpovězení všech otázek. Tazatel má možnost dodatečně vysvětlit otázky. Mezi nevýhody rozhovorů patří jejich časová náročnost a s tím spojená nákladnost. Tazatel se také musí vypořádat s tendencí některých respondentů odpovídat tak, jak si myslí, že tazatel chce slyšet. (Indeed, 2022)

Skupinový rozhovor představuje specifickou formu sběru dat v rámci analýzy rizik kybernetické bezpečnosti. Na rozdíl od individuálního rozhovoru probíhá se skupinou respondentů ve stejném čase. Tato metoda přináší řadu výhod i nevýhod, které je nutné zvážit při jejím výběru. Mezi hlavní výhody skupinového rozhovoru patří vzájemné objasňování odpovědí a formulace rozdílných úhlů pohledu. Na druhou stranu mezi nevýhody se řadí zdrženlivost některých respondentů a náročnější plánování. (Kaluža a Kalužová, 2012)

Rozbor písemných materiálů představuje druhou základní metodu sběru vstupních dat pro sémantické modelování dat. Ve většině případů je tato analýza nepostradatelnou součástí celého procesu. Předmětem analýzy jsou veškeré dokumenty normativní nebo zavedené povahy, které z datového hlediska souvisejí s daným informačním systémem. Písemné materiály, které slouží jako vstupní data pro sémantické modelování dat, lze z hlediska způsobu analýzy rozdělit do několika kategorií:

- Textové materiály mezi které se řadí legislativní předpisy, normy, návody, vědecké články a publikace.
- Formuláře, které zahrnují klasické formuláře v papírové podobě, elektronické formuláře a dotazníky.
- Struktura dat v programech starších aplikací. (Kaluža a Kalužová, 2012)

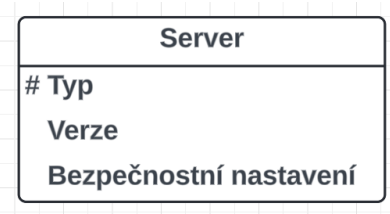
4.5 Konceptuální datový model

Vůbec první metodou v konceptuálním modelování dat byla metoda E-R diagramu prezentovaná poprvé v roce 1976. Ostatní pokusy implementovat jinou metodu se prakticky neujaly. V roce 1988 byla převzata metoda E-R standardizačním institutem ANSI jako standard. Postupně docházelo k jejímu zdokonalování tak, aby lépe postihovala modelované situace. Dnes je metoda E-R jednou ze dvou nejpoužívanějších ke konceptuálnímu modelování.
Druhou metodou je diagram tříd tvořící součást metodiky UML, který také prošel od svého vzniku v rámci UML v roce 1995 až do současnosti určitým vývojem. Původními autory UML jsou autoři pracující na zakázku firmy. Od první verze UML označované 0.8 byly postupně publikovány další až po současnou verzi 2.2. (Kaluža a Kalužová, 2012)

4.6 Základní konstrukty E-R diagramu

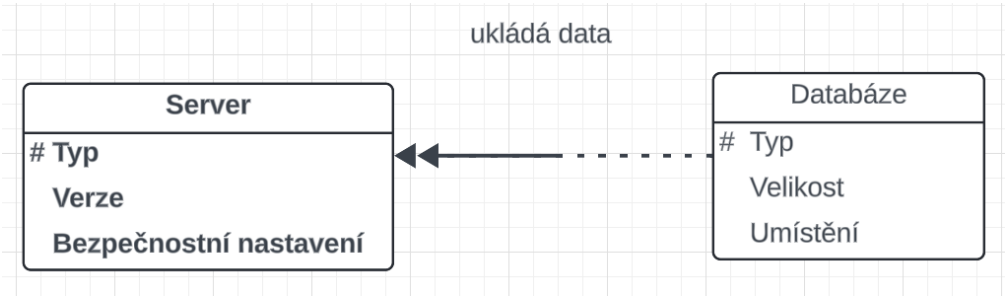
Návrh E-R diagramu spočívá v definování soustavy stavebních kamenů, tzv. konstruktů. Ačkoliv se ujednotilo pojmenování těchto konstruktů, jejich grafické znázornění se liší v závislosti na používaném softwaru. Některé modelovací nástroje se od teoretických doporučení značně odchylují a kombinují E-R diagramy s diagramy tříd (např. Gliffy od Gliffy, Inc. San Francisco, Edraw Max od EdrawSoft Hong Kong, SmartDraw od SmartDraw Software, LLC San Diego). E-R diagramy (Entity-Relationship Diagrams) jsou užitečným nástrojem pro modelování a analýzu rizik v kybernetické bezpečnosti. Umožňují graficky znázornit různé typy aktiv v informačním systému a jejich vzájemné vazby, čímž usnadňují pochopení a identifikaci potenciálních bezpečnostních slabin. (Silva, 2024)

Entita v kontextu kybernetické bezpečnosti představuje specifický prvek IT infrastruktury, jako je server, aplikace, síťové zařízení, databáze nebo uživatelský účet. Graficky je entita znázorněna jako obdélník s názvem v horní části a s výčtem relevantních atributů v dolní části. Název entity by měl být výstižný a vyjádřen podstatným jménem. Atributy pak specifikují vlastnosti a charakteristiky dané entity, které jsou důležité pro posouzení kybernetické bezpečnosti. Aplikace pro analýzu rizik v kybernetické bezpečnosti analyzují entity a jejich atributy z hlediska potenciálních hrozeb a zranitelností. Identifikují slabé stránky a navrhují nápravná opatření pro posílení celkové kybernetické odolnosti. Níže je uveden příklad E-R diagramu. Entita Server má atributy typ, verze a bezpečnostní nastavení. (Silva, 2024)



Obrázek 1 – Grafické vyjádření entity (Kaluža a Kalužová, 2012)

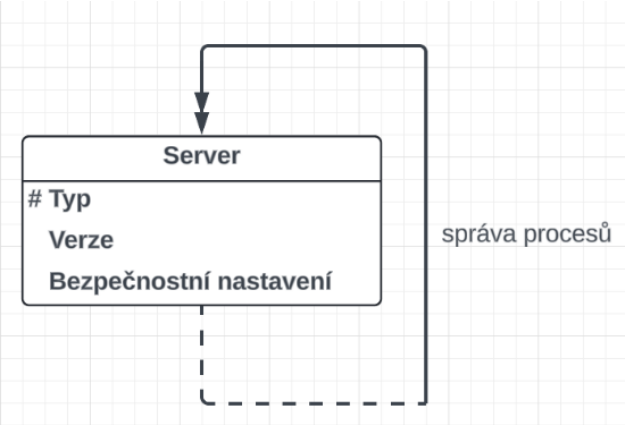
Vztah je druhý základní konstrukt E-R diagramu. Nejběžnější typ vztahu je asociativní vztah. Ten reprezentuje asociace jedné, nebo několika entit, například vztah „ukládá na“ přiřazuje entitu Databáze k entitě Server. Diagram ukazuje příklad asociativního vztahu mezi entitami Server a Databáze. Každá entita má své atributy jako jsou typ, verze, bezpečnostní nastavení, vlastník, velikost a umístění. Diagram ukazuje spojení entit za pomocí relační spojnice, která obsahuje také verbální popis. (Silva, 2024)



Obrázek 2 – Grafické vyjádření vztahu (Kaluža a Kalužová, 2012)

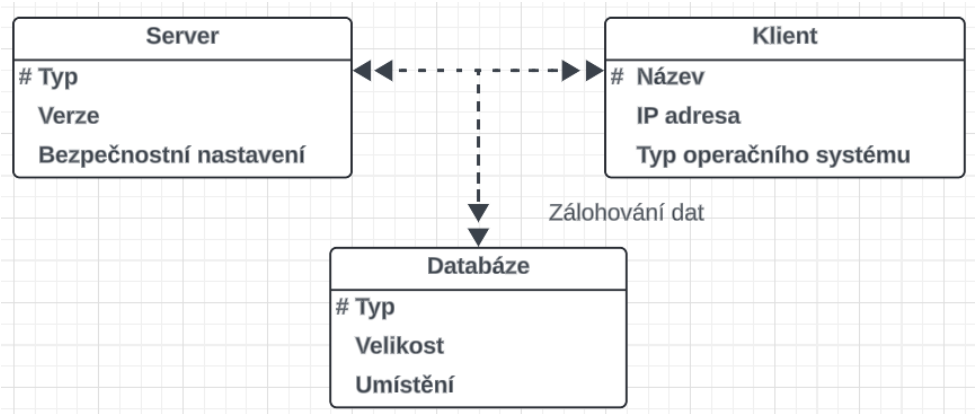
Každý asociativní vztah lze popsat třemi základními charakteristikami mezi které patří stupeň, kardinalita a volitelnost. Stupněm vztahu se rozumí počet entit propojených v jedné vazbě. Nejnižší je úroveň jedna, kdy se vazba váže pouze k jednomu objektu. Jedná se o jednoprvkovou, nebo také samostatnou vazbu. (Kaluža a Kalužová, 2012)

Analogicky vazba druhé úrovně, tedy mezi dvěma objekty, je párová. Vazba mezi třemi objekty je trojná. Instance párové vazby spojuje dvojici instancí zúčastněných objektů. Instance trojné vazby pak trojici instancí tří zúčastněných objektů. Podobně by bylo možné specifikovat vazbu čtvrté až n-té úrovně (tzv. n-prvkovou vazbu). Jejich praktický výskyt v datových modelech je však ojedinělý. (Silva, 2024)



Obrázek 3 – Jednoprvkový vztah (Kaluža a Kalužová, 2012)

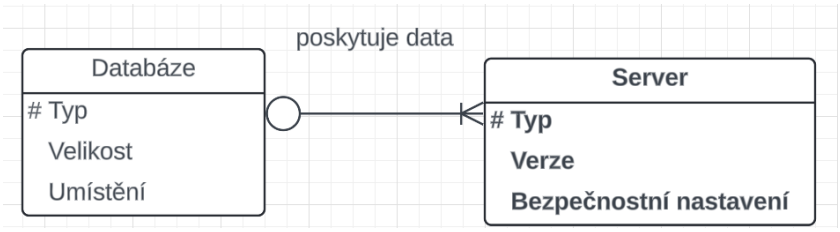
Kardinalita vztahu udává, kolikrát se prvky daného vztahu mohou vyskytnout v jednom případě. (Silva, 2024)



Obrázek 4 – Trojný vztah (Kaluža a Kalužová, 2012)

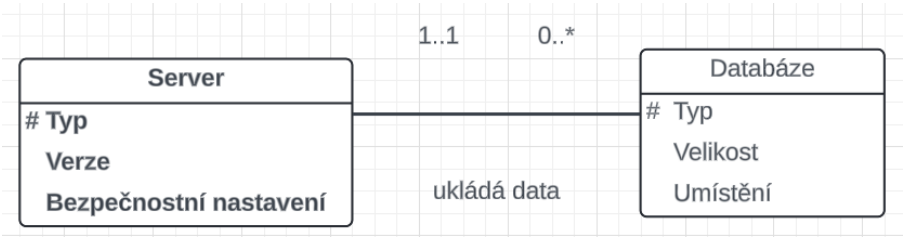
Kardinalita nabývá hodnot "jedna" (jediný výskyt) nebo "mnoho" (libovolný počet výskytů), případně se označuje obecně jako "n" nebo "m". To vede k třem základním typům vztahů: "jeden k jednomu" (1:1), "jeden k mnoha" (1: n) a "mnoho k mnoha" (m:n). Graficky se vztah "mnoho k mnoha" znázorňuje dvěma šipkami směřujícími k "mnoho"(viz obrázek grafické vyjádření vztahu – dvojitá šipka). V některých publikacích se pro „mnoho“ používá

„vraní stopa“. V dnešních publikacích a softwarových nástrojích se kardinalita vztahu vyjadřuje pomocí minimální a maximální kardinality zapsané ve tvaru $n_1..n_2$ (Silva, 2024). Například 1..1 znamená, že mezi dvěma entitami může existovat právě jeden vzájemný výskyt. 1..* znamená, že mezi entitami může existovat jeden nebo více vzájemných výskytů. Obecně může hodnota kardinality nabývat libovolné hodnoty z množiny kladných celých čísel, například 1..5, 10.. a tak dále. (Kaluža a Kalužová, 2012)



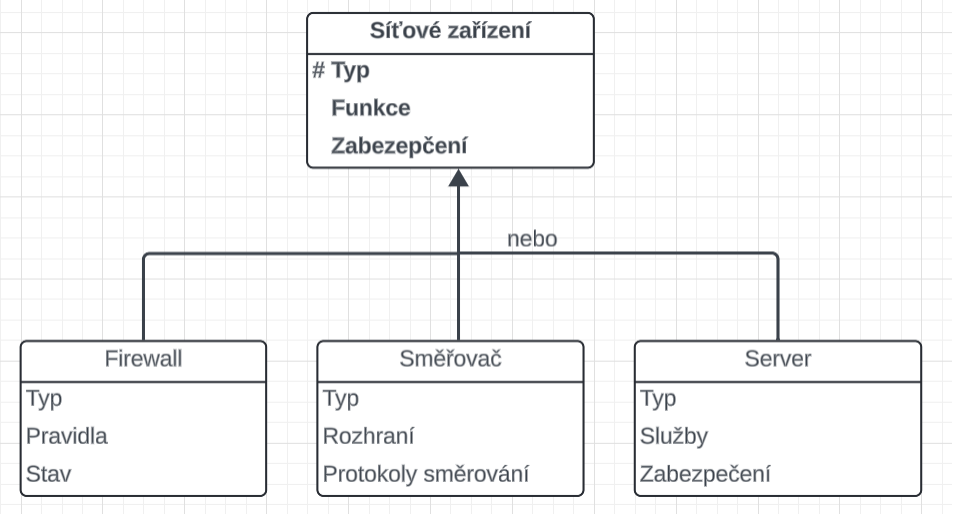
Obrázek 5 – Vraní stopa (Kaluža a Kalužová, 2012)

Třetí vlastností vztahu je volitelnost, která určuje, zda je vztah povinný, nebo volitelný pro danou entitu. Jinými slovy, volitelnost určuje, zda musí, nebo může existovat odpovídající entita pro každý výskyt vztahu. Graficky se volitelná účast vyznačí přerušovanou čarou, povinná plnou čarou. (Kaluža a Kalužová, 2012)



Obrázek 6 – Značení minimální a maximální kardinality (Kaluža a Kalužová, 2012)

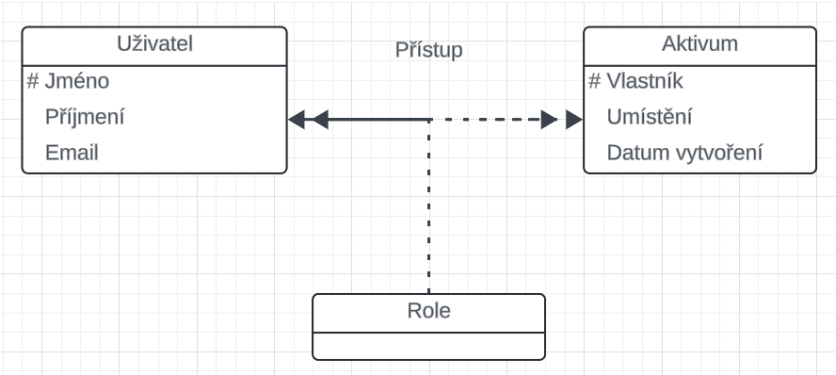
Druhým typem vztahu je tzv. generický vztah nazývaný též generalizace. V protikladu k němu se používá termín specializace. Entita E je generalizací skupiny entit E_1, E2, ..., En, pokud každý prvek z této skupiny je zároveň prvkem entity E. V praxi to znamená, že entita E (nazývaná také supertyp) sdružuje společné vlastnosti entit E_{12}, ..., En (nazývaných subtypy). Postup od obecného k specifickému (od definování nadřazené entity k podřazeným entitám) se nazývá specializace, opačný postup pak generalizace. (Kaluža a Kalužová, 2012)



Obrázek 7 – Generický vztah (Kaluža a Kalužová, 2012)

Supertyp zahrnuje subtypy, které se buď vzájemně vylučují, nebo se překrývají. Další charakteristikou generického vztahu je volitelnost, která určuje, zda každý prvek nadřazené kategorie musí (nebo nemusí) patřit do některé z podkategorií. (Kaluža a Kalužová, 2012)
Graficky se generický vztah znázorňuje tak, že spojnice vedoucí od podkategorií k nadřazené kategorii končí šipkou. Vzájemně se vylučující podkategorie se oddělují spojkou "nebo", zatímco překrývající se podkategorie spojkou "a". Povinnost (protiklad volitelnosti) se znázorňuje plnou čarou se šipkou na konci, zatímco volitelnost se znázorňuje čárkovanou čarou. (Kaluža a Kalužová, 2012)

Atribut je třetí konstrukt E-R diagramu. Vlastnost slouží k popisu základních charakteristik entity nebo vztahu. Mezi příklady patří jméno, příjmení a rodné číslo. Každá vlastnost má definované specifické hodnoty. (WATT, 2014)
V diagramech se vlastnosti obvykle zobrazují v dolní části značky entity. Existují i jiné způsoby zobrazení vlastností v ER diagramech, například pomocí propojených konektorů s uvedením názvů vlastností. Tato forma zobrazení však může u modelů s velkým počtem vlastností znepřehlednit diagram. (WATT, 2014)



Obrázek 8 – Vztahový atribut (Kaluža a Kalužová, 2012)

Volba tvaru značky entity se řídí počtem a délkou názvů vlastností. V případě delších názvů se doporučuje uvádět vlastnosti v samostatném seznamu. Vývojový diagram znázorňuje vztah Přístup mezi entitami Uživatel a Aktivum. S kardinalitou m:n je k nim přiřazen atribut Role. Většina atributů při modelování dat se řadí mezi jednoduché. To znamená že jsou tvořeny jedinou složkou a nabývají hodnot, které nelze dále rozložit. Mezi příklady jednoduchých atributů patří typ firewallu, velikost datového paketu a verze operačního systému. Jednoduché atributy se mohou označovat jako atomické. (Kaluža a Kalužová, 2012)
Kromě jednoduchých atributů existují i složené atributy, které se skládají z více částí se společným významem nebo využitím. Tyto atributy se dělí do dvou kategorií:

- Skupiny komponent – příkladem je IP adresa, název domény, nebo hlášení o události kybernetické bezpečnosti.
- Opakující se komponenty – například historie přihlášení uživatele a statistiky síťového provozu. (Kaluža a Kalužová, 2012)

V rámci tvorby sémantického modelu se v závislosti na specifické situaci může objevit typ objektu odpovídající skupinovému atributu. Při transformaci do konceptuálního modelu se u zbývajících skupinových atributů, a to zejména v případě sdílených domén může rovněž zavést nová entita. V ostatních případech a u atributů s opakujícími se komponentami ze zpracování provede při transformaci do logického datového modelu. Hodnotou atributu nemusí být pouze číselná nebo textová informace, ale i obrázek, video nebo zvuková nahrávka. Některé atributy reprezentují hodnotu, která se dá odvodit obvykle jednoduchou aritmetickou operací z jiných atributů, které nemusí patřit k téže entitě. Odvozené atributy se sice nezačleňují do struktury modelu, ale slouží jako informační zdroj pro algoritmické řešení. (Kaluža a Kalužová, 2012)

Doménu lze definovat jako soubor povolených hodnot, které se přiřazují jednomu nebo více atributům. Jinými slovy, doména určuje, jaké hodnoty daný atribut může nabývat. Příkladem domény může být doména úrovní oprávnění a doména typů protokolů. (Kaluža a Kalužová, 2012)

Klíč je jedním nebo několika atributy charakterizujícími výskyty dané entity. Pokud entitu identifikuje pouze jeden atribut, nazývá se jednoduchým klíčem. Pokud atribut neumožňuje jednoznačně identifikovat entitu, jedná se o sekundární klíč.

I je kandidátním klíčem entity E, pokud splňuje následující požadavky:

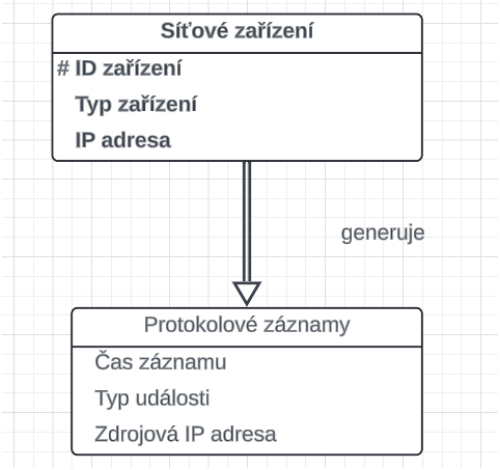
Požadavek jedinečnosti: žádné dva výskyty entity E nesmí mít stejnou hodnotu I.

Požadavek úplnosti: pokud se z I odstraní jakákoli část, požadavek jedinečnosti již nebude platný. (Kaluža a Kalužová, 2012)

Z vybraných kandidátních klíčů se stávají primární klíče entity, které slouží k její jednoznačné identifikaci. Kandidátní klíče, které nebyly zvoleny jako primární klíče, se nazývají alternativní klíče. Při výběru primárního klíče z kandidátních klíčů je vhodné se řídit následujícími principy:

- Kandidátní klíč s minimální množinou atributů.
- Kandidátní klíč, u něhož je změna hodnot nejméně pravděpodobná.
- Kandidátní klíč, u něhož existuje nejmenší pravděpodobnost, že v budoucnu ztratí svou jedinečnost.
- Kandidátní klíč s nejmenším počtem znaků (v případě textových atributů).
- Kandidátní klíč s nejmenší maximální hodnotou (u číselných atributů).
- Kandidátní klíč, který lze nejsnáze použít z hlediska uživatele. (Kaluža a Kalužová, 2012)

Primární klíč se graficky znázorňuje symbolem # umístěným před názvem atributu. Další možné způsoby označení primárního klíče jsou podtržení názvu atributu, nebo použití značky {PK}. Alternativní klíč se mezi ostatními atributy nijak zvlášť neoznačuje. Pořadí atributů v rámci entity, včetně primárního klíče, nemá žádný vliv na jejich význam. Z praktických důvodů se však atributy tvořící primární klíč obvykle uvádějí na prvním místě. V praxi vždy neplatí, že každá entita v konceptuálním modelu má definovaný svůj přirozený primární klíč nezbytný k identifikaci každého výskytu entity. Existují entity, jejichž primární klíč je závislý na klíčích jiných entit. (Yasar, 2022)



Obrázek 9 – Silná a slabá entita (Kaluža a Kalužová, 2012)

Síťové zařízení má svůj primární klíč, identifikátor síťového zařízení. Protokol síťového zařízení však obsahuje kromě údajů vztahujících se k celému síťovému zařízení také jednotlivé záznamy specifikující řadou údajů události a aktivity v síti. Údaje o záznamu síťového zařízení nemohou představovat atributy síťového zařízení, neboť jejich hodnoty se opakují v rámci téhož síťového zařízení a nejsou jedinečně identifikovatelné primárním klíčem síťového zařízení. Tvoří tedy zvláštní entitu. Každý záznam síťového zařízení má své časové razítko, které rozlišuje jednotlivé výskyty této entity, avšak záznamy nejsou schopny samostatné existence bez příslušného síťového zařízení. Síťové zařízení se stává tzv. silnou entitou a protokol síťového zařízení tzv. slabou entitou. (Yasar, 2022)

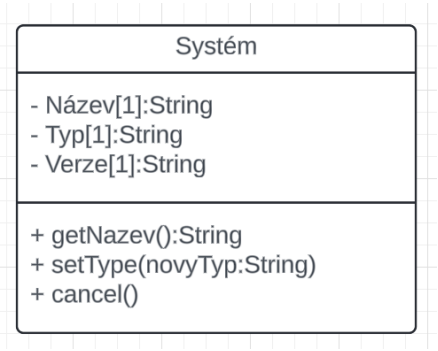
Silná entita se vyznačuje tím, že její existenci a jednoznačnou identifikaci zajišťuje výhradně její primární klíč, bez nutnosti závislosti na jiné entitě. Naopak u slabé entity neexistuje žádný vlastní atribut, který by ji dokázal jednoznačně identifikovat. K její identifikaci je nutné použít primární klíč jiné (silné) entity, na které je slabá entita existenčně závislá. V datovém modelu se slabá entita odlišuje od silné entity absencí primárního klíče. Vazba mezi slabou a silnou entitou se znázorňuje zdvojenou čarou. Volitelnost se vyznačuje čárkovanou čarou, kardinalita 1:n šipkou u slabé entity a kardinalita 1:1 bez šipky. (Yasar, 2022)

4.7 Základní konstrukty diagramu tříd

Vizualizace datových konceptů prošla značným vývojem, směřujícím k co nejvěrnějšímu zobrazení modelované reality. Hlavní odlišností mezi E-R diagramem a diagramem tříd je přítomnost operací, tedy algoritmické složky, v diagramu tříd. Metodika UML umožňuje

modelování tříd bez zahrnutí definice operací, čímž vzniká diagram velmi podobný E-R diagramu. (SourceMaking, 2024)

Třída je popis množiny objektů, které sdílí stejné vlastnosti – atributy a operace. Třída z hlediska modelování odpovídá konstruktu entita a jednotlivé objekty pak výskytům entit. Graficky se třída vyznačí obdélníkem se třemi částmi: jménem třídy, atributy a operacemi. (SourceMaking, 2024)

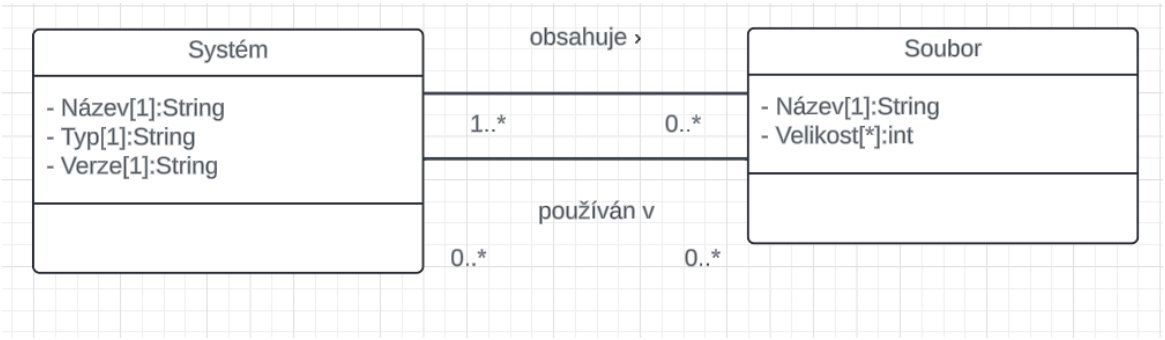


Obrázek 10 – Grafické vyjádření třídy (Kaluža a Kalužová, 2012)

Názvy tříd by měly být stručné a výstižné, aby co nejlépe odrážely podstatu objektů, které reprezentují. V případě potřeby lze uvést i další informace o třídě, jako je stav vývoje, jméno autora nebo číslo verze. Druhá část značky zahrnuje seznam vlastností, které patří objektům dané třídy. Tyto vlastnosti mohou zahrnovat i odkazy na vlastnosti nebo objekty jiných tříd. Podle metodiky UML je u každé vlastnosti v seznamu kromě jména možné specifikovat i další parametry, jako je datový typ, multiplicita a viditelnost. Datový typ určuje typ hodnoty, kterou vlastnost může nabývat (například String pro textové hodnoty, int pro celočíselné). Multiplicita definuje počet hodnot, které může vlastnost mít (uvádí se v hranatých závorkách za jménem atributu). Viditelnost určuje rozsah, v němž je atribut přístupný (například soukromá v rámci třídy – symbol "-" před jménem vlastnosti, veřejná v rámci celého systému – symbol "+", chráněná v rámci generického vztahu – symbol "#"). (Kaluža a Kalužová, 2012)

Třetí část značky zahrnuje popis akcí, které objekty dané třídy dokáží provádět. Každá akce má své jméno a podobně jako vlastnosti může mít i další atributy, jako je viditelnost, seznam parametrů v závorkách za jménem a typ vrácené hodnoty, oddělený od jména dvojtečkou. Seznam parametrů definuje vstupní informace pro akci a typ vrácené hodnoty určuje její výstup. Kromě tříd, ke kterým jsou dynamicky přiřazovány objekty, je možné definovat i třídy bez objektů. Jejich seznam vlastností a akcí slouží obvykle k opakovanému použití v jiných třídách. Takové třídy se nazývají abstraktní. Vztah mezi objekty v daném kontextu

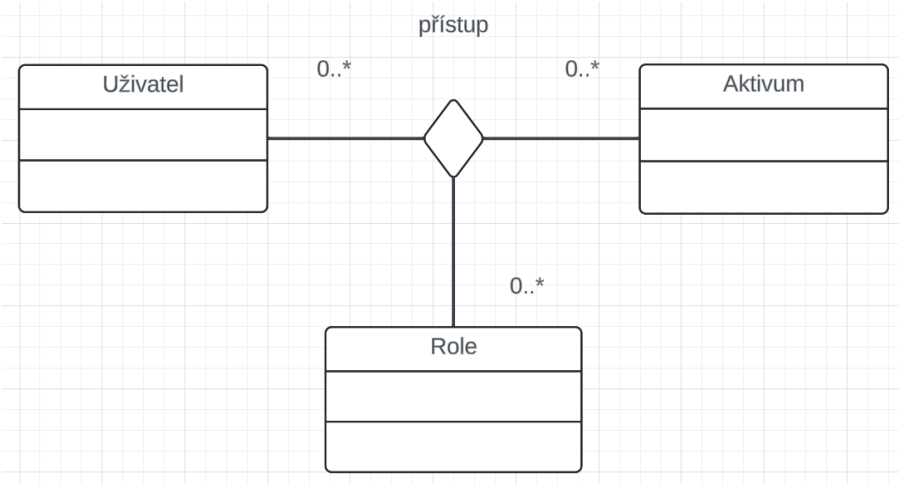
lze přirovnat k asociacím v E-R diagramu. Asociace propojuje objekty a je charakterizována svým názvem, které je obvykle vyjádřeno slovesem. (Kaluža a Kalužová, 2012)



Obrázek 11 – Asociace v diagramu tříd (Kaluža a Kalužová, 2012)

Asociace bývá doprovázena "směrníkem", který určuje, jak ji interpretovat. Například asociace obsahuje má směrník naznačující interpretaci systém obsahuje soubor, čte se tedy zleva doprava. Samozřejmě je možné zvolit i pravidlo, že pokud má být asociace interpretována běžným způsobem zleva doprava, směrník není nutný. Graficky je asociace znázorněna spojnicí mezi značkami příslušných tříd. Mezi dvěma entitami může existovat více než jedna asociace. Toto lze chápat i jako více rolí, které může jedna asociace zastávat. Vztah s asociacemi může mít různé vlastnosti: kardinalitu (multiplicitu), řazení, modifikovatelnost a další. Kardinalita vyjadřuje počet entit ve vzájemném vztahu a označuje se intervalem na obou stranách asociace: n..m, kde n a m nabývají hodnot od 0 do * (symbol * značí mnoho). Řazení znamená, že entity na dané straně asociace budou seřazeny, například podle hodnoty určitého atributu. (Kaluža a Kalužová, 2012)

Modifikovatelnost určuje, zda je vztah mezi entitami neměnný, nebo zda jej lze změnit (zrušit). Neměnnost se označuje {frozen}, opak neměnnosti (možnost změny) se výslovně neoznačuje. Jednoprvková asociace se označuje stejně jako u E-R diagramu spojnicí ve stavu smyčky. Trojná a další (n-tá) asociace se graficky vyznačuje pomocí diamantu v průsečíku spojnic. (Kaluža a Kalužová, 2012)



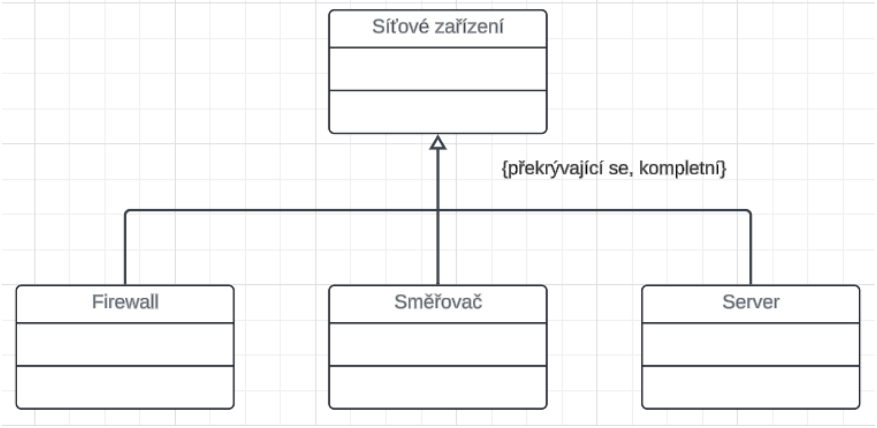
Obrázek 12 – Ternární asociace (Kaluža a Kalužová, 2012)

Vztahové atributy se modelují pomocí asociační třídy, která je s danou asociací propojena. Asociační třída slouží k ukládání a správě atributů vztahu.

Generický vztah, zahrnující supertřídy a subtřídy, se graficky znázorňuje hierarchickým uspořádáním. Princip dědičnosti umožňuje subtřídám zdědit vlastnosti (atributy a operace) supertříd. To umožňuje široké využití abstraktních tříd, které definují společné vlastnosti bez konkrétních objektů. (Kaluža a Kalužová, 2012)

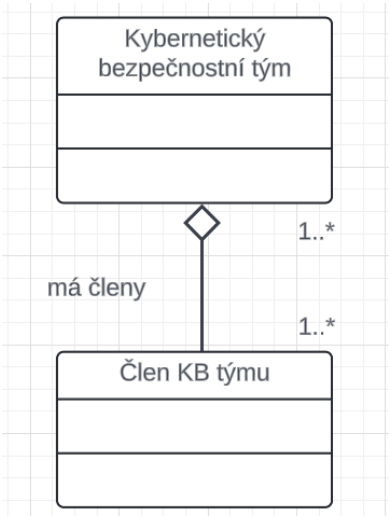
Subtřídy se buď definují jako redefinice supertřídy s vlastními výskyty, nebo se rozlišují specifickou vlastností (atributem, operací) supertřídy. Subtřídy ve vztahu mohou být překrývající se nebo nepřekrývající se. Mohou být také kompletní (nezahrnují žádné další subtřídy) nebo nekompletní (výčet subtříd není úplný). Kompletnost odpovídá konceptu volitelnosti v E-R diagramu. V praxi to znamená, že existují čtyři možnosti, které se graficky znázorňují u spojnice vztahu následovně:

- {překrývající se, kompletní},
- {nepřekrývající se, nekompletní},
- {překrývající se, nekompletní},
- {nepřekrývající se, kompletní}. (Kaluža a Kalužová, 2012)



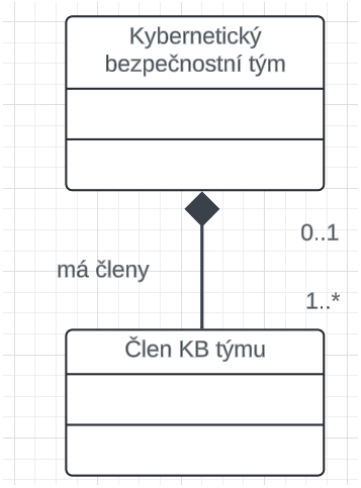
Obrázek 13 – Generický vztah v diagramu tříd (Kaluža a Kalužová, 2012)

Agregace představuje třetí typ vztahu a vyjadřuje hierarchii tříd v rámci komplexu, nazývaného agregace. Slouží k modelování celků (agregátů) složených z částí. (Canhasi, 2023)



Obrázek 14 – Agregační vztah (Kaluža a Kalužová, 2012)

Typickým příkladem agregace je kusovník, který popisuje strukturu montovaného celku z jednotlivých komponent. Dalším příkladem může být hierarchie složená z nadřazených a podřízených prvků. Agregace může být chápána jako specifický typ asociace, a proto na ni lze aplikovat principy vlastností asociace, jako je multiplicita, modifikovatelnost a role. (Canhasi, 2023)



Obrázek 15 – Kompoziční vztah (Kaluža a Kalužová, 2012)

Kompozice, někdy nazývaná silná agregace, je specifickým typem agregace. Vyjadřuje závislost životního cyklu částí na životním cyklu celku. Části v kompozici jsou vnořené objekty, které nemohou být součástí jiných tříd. Graficky se kompozice odlišuje od agregace plným diamantem. Diskuze o základních stavebních kamenech modelu tříd – třídách a jejich vzájemných vazbách – položila základy metodiky konceptuálního modelování. Na rozdíl od E-R diagramů není v tomto případě nutné explicitně zdůrazňovat primární klíč. Jeho důležitost je oslabena automatickou jedinečnou identifikací objektů pomocí čísla OID. Díky tomu se atributy tříd stávají rovnocennými. (Canhasi, 2023)

5 DÍLČÍ ZÁVĚR

Teoretická část práce se zabývala koncepty informačních a komunikačních technologií, s důrazem na počítačové sítě, data a internetový protokol. Dále se věnovala problematice řízení rizik v informačních systémech, včetně oblasti působnosti, aktiv, důvěrnosti, integrity, dostupnosti, hrozeb a rizik. V závěru teoretické části byla představena metodika datového modelování při navrhování informačního systému, včetně víceúrovňového přístupu k modelování dat, tříúrovňové koncepce, sémantického datového modelu, analýzy datových požadavků, konceptuálního datového modelu a základních konstruktů E-R diagramu a diagramu tříd. Na základě představených datových modelů a metod je tak možné sestavit vlastní aplikaci pro analýzu rizik v informačních systémech.

II. PRAKTICKÁ ČÁST

6 APLIKACE PRO ANALÝZU RIZIK

Software pro řízení rizik pomáhá subjektům identifikovat, zmírňovat a napravovat rizika, což může vést ke zvýšení efektivity. Trh s řízením rizik prochází rychlou transformací od izolovaných nástrojů pro jednotlivé oblasti rizik k integrovaným platformám. Tyto platformy sjednocují funkce řízení rizik, dodržování předpisů, kybernetické bezpečnosti, IT a rizik třetích stran. Rostoucí počet a komplexnost rizik, kterým podniky čelí, zdůrazňuje důležitost řízení podnikových rizik (ERM – Enterprise Risk Management). Výdaje na nástroje pro řízení rizik a zajištění shody s předpisy v různých odvětvích se výrazně zvyšují. Vytvoření spolehlivé strategie a výběr správného ERM nástroje se tak stává klíčovým rozhodnutím pro ochranu před riziky.

6.1 OpenVAS

Greenbone Community Edition (GCE) se skládá z platformy s integrovanými službami. Je vyvinuta v rámci komerční produktové řady Greenbone Enterprise. GCE vznikla jako komunitní projekt s názvem OpenVAS a je primárně vyvíjena a distribuována společností Greenbone. Architektura GCE se dělí do tří hlavních částí:

- Spustitelné aplikace skeneru, které spouštějí testy zranitelnosti proti cílovým systémům.
- Greenbone Vulnerability Management Daemon.
- Greenbone Security Assistant (GSA) společně s Greenbone Security Assitant Daemon. (Greenbone AG, 2024)

Greenbone Vulnerability Management Daemon (GVMD) – Známý také jako Greenbone Security Assistant, je centrální služba, která integruje základní skenování zranitelností do komplexního řešení pro správu zranitelností. GVMD řídí skener OpenVAS pomocí protokolu Open Scanner Protocol. GVMD dále nabízí vlastní protokol Greenbone Management Protocol ve formátu XML. Spravuje také databázi SQL, která slouží jako centrální úložiště konfiguračních data výsledků skenování. GVMD zajišťuje správu uživatelů, včetně nastavení oprávnění pomocí skupin a rolí. Součástí služby je i interní systém pro spouštění naplánovaných úloh a dalších událostí. (Greenbone AG, 2024)

Greenbone Security Assistant (GSA) – Je webové rozhraní, které umožňuje uživateli řídit skenování a prohlížet informace o zranitelnostech. Jedná se o hlavní bod interakce pro uživatele. GSA se připojuje ke GVMD prostřednictvím webového serveru Grennbone Security

Assistant Daemon a poskytuje plnohodnotnou webovou aplikaci pro správu zranitelností. Komunikace probíhá pomocí protokolu GMP (Grennbone Management Protocol), s nímž může uživatel komunikovat i přímo pomocí různých nástrojů. (Greenbone AG, 2024)

Skener OpenVAS – Hlavní skener OpenVAS představuje samostatný skenovací nástroj, který realizuje ověření zranitelnosti na cílových systémech. Za tímto účelem se spoléhá na průběžně aktualizované a komplexní zdroje, mezi které patří Greenbone Enterprise Feed a Grennbone Community Feed. Skener se skládá z dvou hlavních částí: ospd-openvas a openvas-scanner. Ovládání skeneru OpenVAS probíhá pomocí rozhraní OSP (Open Scanner Protocol. (Greenbone AG, 2024)

Skener Notus – Provádí skenování automaticky v rámci běžného provozu, bez nutnosti zásahu uživatele. Kvůli nízké systémové náročnosti dosahuje skener vyššího výkonu a umožňuje tak rychlejší skenování. Skener přebírá funkcionalitu všech lokálních bezpečnostních kontrol (LSC – Local Security Control) dříve realizovaných pomocí NASL (Nessus Attack Scripting Language). Notus skenuje software nainstalovaný na hostiteli a porovnává jej se seznamem zranitelného softwaru. Běžný skener OpenVAS spouští jednotlivé LSC skripty NASL jeden po druhém pro každý cílový počítač. Pro každý skript se porovnává seznam známých zranitelností s nainstalovaným softwarem. Celý proces se opakuje pro všechny LSC skripty. Skener Notus oproti tomu nejprve načítá seznam nainstalovaného softwaru, ale následně ho porovnává s komplexní databází zranitelností specifických pro daný operační systém skenovaného počítače. Tímto odpadá nutnost spouštět individuální LSC skripty, jelikož veškeré informace o zranitelném softwaru jsou soustředěny v jediném souhrnném seznamu a nejsou roztříštěny do mnoha NASL skriptů. (Greenbone AG, 2024)

Další software – Greenbone Vulnerability Management Tools (gvm tools) – slouží k dálkovému ovládání instalací Greenbone Community Edition a Greenbone Enterprise Appliances. Usnadňují přístup ke komunikačním protokolům GMP a OSP. Modul se skládá z interaktivních a neinteraktivních klientů. Pro interaktivní skriptování je přímo podporován programovací jazyk Python. Je však také možné vydávat vzdálené příkazy HMP/OSP bez programování v jazyce Python. (Greenbone AG, 2024)

V počátcích projektu OpenVAS se jednalo pouze o nástroj pro skenování zranitelností. Brzy poté vznikla společnost Greenbone s cílem poskytnout profesionální podporu pro skenování zranitelností. Greenbone převzala vedení vývoje OpenVAS, přidala další softwarové komponenty a transformovala OpenVAS v komplexní řešení pro správu zranitelností, a to při

zachování principů svobodného softwaru. Toto řešení později získalo název Greenbone Vulnerability Management, aby odráželo svůj původ a změny v identitě. Po vydání rámce OpenVAS 9 tak byly další verze pojmenovány GVM. (Greenbone AG, 2024)

6.2 Rapid7

InsightVM je zdroj bohatý na data, který může posílit ostatní soubor nástrojů od SIEM (Security Information and Event Management) a firewallů až po systémy ticketingu. InsightVM spojuje knihovnu znalostí společnosti Rapid7 o výzkumu znalostí z Nexpose, znalosti o exploitech z Metasploitu, globálních chování útočníků, data o skenování v rámci celého internetu, analýzu odhalení a reportování v reálném čase. InsightVM využívá konzoli Security Console, která slouží k lokálním skenování zranitelností a správě systému. Základní funkce této konzole jsou odhalování rizik, organizace zařízení a stanovování priorit nápravy. Kontrolou zabezpečení lze odhalit známé zranitelnosti, možnosti zneužití a nesrovnalosti s pravidly. Vytvářením skupin aktiv lze dosáhnout cíleného skenování. Výběrem z předdefinovaných šablon skenování (např. dodržování zásad CIS – Center for Internet Security Controls, nebo kompletní audit bez webového pavouka) je možné určit rozsah kontrol. InsightVM umožňuje upravování a vytváření vlastních šablon, které mohou efektivně vyhledávat zranitelnosti a kontrolovat dodržování zásad. Na základě plánů skenování se automatizuje proces skenování a pravidelného informování o jeho výsledcích. (Rapid7, 2024)

Skenovaný aktiva lze uspořádat do dynamických i statických skupin podle různých kritérií, jako je umístění, operační systém a vlastník. Pomocí systému značení v konzoli Security Console mohou být upravována skóre rizik a také stanovovány priority nápravy pro nejdůležitější aktiva. Filtrované vyhledávání aktiv umožňuje najít skenovaná aktiva na základě více než 40 jedinečných parametrů. Reporty z výsledků skenování jsou generovány tak, aby bylo možné zjištěné nedostatky napravit. K dispozici jsou předpřipravené šablony reportů i exporty dotazů SQL (Structured Query Language). Mezi nejpopulárnější šablony reportů patří Top Remedation, který souží k určení priorit oprav k největšímu snížení rizika. Dále také Report Trendy, který umožňuje analyzovat celkový počet zjištěných aktiv, zranitelností a zneužití v rámci datových rozsahů. (Rapid7, 2024)

Centrum pro kybernetickou bezpečnost (CIS) je nezisková organizace, která posiluje globální bezpečností postavení zprostředkováním cenného a důvěryhodného prostoru pro spolupráci mezi veřejným soukromým sektorem. CIS hraje klíčovou roli v utváření bezpečnostních politik a směřování na národní a mezinárodní úroveň. Správce politik zajišťuje kontrolu

dodržování referenčních hodnot CIS, včetně technických kontrolních pravidel a hodnot pro posílení síťových zařízení, operačních systémů, middlewaru a softwarových aplikací. Pro provádění těchto kontrol je nutná licence, která aktivuje funkci Správce politik a umožňuje kontrolu CIS. (Rapid7, 2024)

Příkazová kontrola je rozhraní v konzoli Security Console, které umožňuje zadávat příkazy pro vyvolání specifických operací. Pomocí tohoto nástroje lze zobrazit diagnostiku v reálném čase a nahlédnout do fungování konzole Security Console. (Rapid7, 2024)

Common Configuration Enumeration (CCE) je standardizovaný systém pro přidělování unikátních identifikátorů. Tento systém zajišťuje konzistentní identifikaci konfiguračních prvků v různých prostředích. CCE je implementováno v rámci shody s kritérii SCAP (Security Content Automation Protocol) pro Unauthenticated Scanner. (Rapid7, 2024)

Common Platform Enumeration (CPE) je systém pro identifikaci operačních systémů a softwarových aplikací. Jeho schéma pojmenování vychází z obecného formátu pro jednotné identifikátory zdrojů. CCE je součástí shody s kritérii SCAP pro produkt neautentizovaného skenování. (Rapid7, 2024)

Standard Common Vulnerabilities and Exposures (CVE) definuje jednotný způsob identifikace zranitelností v aplikacích. Usnadňuje tak sdílení informací o zranitelnostech mezi bezpečnostními produkty. CVE je součástí shody s kritérii SCAP pro produkt neautorizovaného skenování. (Rapid7, 2024)

Common Vulnerability Scoring Systém (CVSS) je univerzální systém pro hodnocení rizika zranitelností. CVSS je součástí shody s kritérii SCAP pro produkt neautorizovaného skenování. (Rapid7, 2024)

6.3 GFI LanGuard

GFI LanGuard slouží k spravování, udržování a ochraně koncových bodů v síti. GFI LanGuard poskytuje přehled o všech prvcích v síti, pomáhá s vyhodnocením, kde mohou být potenciální zranitelnosti a umožňuje jejich opravy. Nabízí snadno použitelné řešení pro správu záplat a audit sítě. GFI LanGuard disponuje schopností identifikovat více než 60 000 zranitelností. Provádí skenování zařízení, identifikuje a kategorizuje bezpečnostní zranitelnosti, doporučuje postup a poskytuje nástroje pro řešení problému. Graf indikátoru úrovně ohrožení poskytuje hodnocení stavu zranitelnosti skenovaných zařízení. Dále nabízí webové rozhraní pro vytváření zpráv pomocí zabezpečeného připojení (https). V případě rozsáhlých

sítí lze nainstalovat více instancí (lokalit) GFI LanGuard a pro centralizovaný přehled a souhrnné hlášení lze použít jedinou webovou konzoli. Reporty lze exportovat do různých formátů například PDF, HTML, XLS, XLSX, RTF a CSV. (Vaughan, 2024)

GFI LanGuard je vybaven databází hodnocení zranitelností, která zahrnuje standardy OVAL (Open Vulnerability and Assessment Language), které obsahují více než 11 500 kontrol a SANS Top 20. Databáze je průběžně aktualizována informacemi z BugTraq, SANS Corporation, OVAL a CVE. Funkce automatické aktualizace zajišťuje stálé obnovování systému o nově vydané aktualizace zabezpečení a kontroly zranitelností společnosti Microsoft. GFI LanGuard se integruje s více než 4 000 bezpečnostními aplikacemi, včetně antiviru, antispywaru, brány firewall, anti-phishingu, zálohovacího klienta, šifrování disků, prevence ztráty dat a řízení přístupu k zařízením. Poskytuje přehledy o stavu a seznamy aplikací pro okamžitou komunikaci, nebo sdílení souborů nainstalovaných v síti a upozorňuje na problémy, které vyžadují řešení, jako je spouštění aktualizací antiviru nebo antispywaru. GFI LanGuard zajišťuje ochranu přepínačů, směrovačů, přístupových bodů a tiskáren před útoky. Usnadňuje skenování zranitelností chytrých telefonů a tabletů. Dále také nabízí komplexní správu zranitelností s rozsáhlým reportingem, který pomáhá dodržovat normy a předpisy. (Vaughan, 2024)

6.4 Tenable Vulnerability Management

Tenable Vulnerability Management umožňuje bezpečnostním a auditorským týmům sdílet skenery Tenable Nessus, Tenable Nessus Agent a Tenable Nessus Network Monitor, plány skenování, zásady skenování a výsledky skenování mezi neomezeným počtem uživatelů, nebo skupin. (Tenable, 2024)

Tenable One Exposure Management Platform – Je platforma, která pomáhá organizacím získat komplexní přehled o moderních hrozbách. Platforma umožňuje zaměřit úsilí na prevenci pravděpodobných útoků a efektivně komunikovat o kybernetických rizicích s cílem podpořit optimální fungování podniku. Tenable One integruje nejširší pokrytí zranitelností zahrnující IT aktiva, cloudové zdroje, kontejnery, webové aplikace a systémy identit. Platforma staví na rychlosti a rozsahu detekce zranitelností od Tenable Research a přidává komplexní analytické nástroje pro stanovování priorit a komunikaci o kybernetických rizicích. Tenable One umožňuje získat ucelený přehled o rozsahu moderních útoků, předpovídat hrozby a stanovovat priority pro jejich prevenci a efektivně komunikovat o kybernetických rizicích a přijímat informovaná rozhodnutí. Tenable Vulnerability Management je dostupný

jako samostatný produkt, nebo jako součást platformy Tenable One Exposure Management. (Tenable, 2024)

Tenable Vulnerability Management – Poskytuje široké možnosti sdílení různých zdrojů mezi uživateli a skupinami. To umožňuje vytvářet individuální postupy pro programy správy zranitelností, a to bez ohledu na množství regulačních požadavků a standardů dodržování předpisů, které je nutné dodržovat. (Tenable, 2024)

Tenable Lumin – Tato funkce obohacuje data z Tenable Vulnerability Managementu. Pomocí nástroje Tenable Lumin lze rychle a přesně zhodnotit míru ohrožení a porovnat stav a efektivitu nápravy s ostatními klienty Tenable. Tenable Lumin propojuje nezpracovaná data o zranitelnostech s daty o důležitosti aktiv a kontextu hrozeb, čímž umožňuje rychlejší a cílenější analytické postupy než tradiční nástroje pro správu zranitelností. (Tenable, 2024)

Tenable Web App Scanning – Přináší významné zlepšení oproti stávající šabloně zásad Testy webových aplikací, která je součástí skeneru Tenable Nessus. Tato šablona není kompatibilní s moderními webovými aplikacemi, které se spoléhají na JavaScript a jsou postaveny na HTML5. To vede k neúplnému obrazu o stavu zabezpečení webových aplikací. Tenable Web App Scanning nabízí komplexní skenování zranitelností pro moderní webové aplikace. Přesné pokrytí zranitelností minimalizuje falešně pozitivní a falešně negativní výsledky a zajišťuje, že bezpečnostní týmy budou mít jasno o skutečných bezpečnostních rizicích webových aplikací. Produkt umožňuje bezpečné externí skenování, které nevyvolá žádné narušení, ani zpoždění produkčních webových aplikací, včetně těch, které jsou vytvořeny pomocí frameworků HTML5 a AJAX. (Tenable, 2024)

Tenable Container Security – Ukládá a skenuje kontejnerové obrazy v průběhu jejich vytváření, tedy před jejich uvedením do provozu. Poskytuje detekci zranitelností a malwaru a umožňuje průběžné sledování kontejnerových obrazů. Integrací se systémy pro kontinuální integraci a kontinuální nasazení (CI/CD), které kontejnerové obrazy vytváří, Tenable Container Security zajišťuje, že každý kontejner, který se dostane do produkčního prostředí, je bezpečný a splňuje bezpečnostní standardy. (Tenable, 2024)

Tenable Vulnerability Management API – Rozhraní API Tenable Vulnerability Management umožňuje vyvíjet vlastní aplikace, které využívají různé funkce platformy Tenable Vulnerability Management, jako je skenování, tvorba zásad a správa uživatelů. Společnost Tenable používá CVSS a dynamické hodnocení priority zranitelností (VPR – Vulnerability Priority Rating) ke kvantifikaci rizika a naléhavosti zranitelností. (Tenable, 2024)

CVSS – Společnost Tenable určuje závažnost (nízká, střední, vysoká, nebo kritická) všech zranitelností na základě statického skóre CVSSv2, nebo CVSSv3 v závislosti na konfiguraci. (Tenable, 2024)

VPR – Tenable počítá dynamický VPR pro většinu zranitelností. VPR je dynamický doplněk k informacím v hodnocení CVSS zranitelnosti, jelikož Tenable aktualizuje VPR tak, aby odpovídalo aktuálnímu stavu hrozeb. Hodnoty VPR se pohybují v rozmezí 0,1-10,0, přičemž vyšší hodnota značí větší pravděpodobnost zneužití. Tenable Vulnerability Management zobrazí hodnotu VPR při prvním skenování zranitelnosti v síti. Poté automaticky každý den poskytuje nové a aktualizované hodnoty VPR. Tenable doporučuje primárně řešit zranitelnosti s nejvyššími hodnotami VPR. (Tenable, 2024)

6.5 SAINT Security Suite

SAINT neboli Security Administrator Integrated Network Toolkit byl poprvé komerčně nabídnut v roce 2001. Od té doby společnost SAINT Corporation rozšířila nabídku na SAINT Security Suite a SAINT Cloud. Zásadní funkcí obou řešení je neinvazivní detekce bezpečnostních zranitelností na jakýchkoli vzdálených cílech, včetně serverů, pracovních stanice, síťových zařízení a dalších typů síťových hostitelů. Shromažďují také informace, jako jsou typy operačních systémů a otevřené porty. Grafické uživatelské rozhraní umožňuje přístup ke správě dat, konfiguraci skenování, plánování skenování, analýze dat a generování zpráv prostřednictvím webového prohlížeče. (SAINT, 2022)

SAINTexploit je starší produktový termín pro komponentu testování průniku v produktových řadách společnosti SAINT. Před verzí 8 byla tato součíst k dispozici jako integrovaná počást profesionální edice produktu. Od verze 8 je tato funkce plně integrovaná do obou sad Security Suite a SAINTCloud a je dostupná jednoduše prostřednictvím možnosti nabídky Exploit. Umožňuje uživateli ověřit existenci zranitelností jejich zneužitím a shromáždit důkazy o průniku. Na rozdíl od testů pro skenování zranitelností a konfigurace, které zjišťují různé typy zranitelností a slabin konfigurace, exploity spouštějí různé testy, jejichž cílem je získat přístup k cílům pro spouštění příkazů. Odhalené zranitelnosti se zobrazují v sekci Analýza na úrovni detailu záznamu a obsahují samostatný sloupec exploitů, který informuje o tom, zda je pro danou zranitelnost k dispozici exploit. Obě řešení také nabízí předpřipravené skenovací profily Pen Test, které automaticky vybírají exploity na základě operačního systému a otevřených služeb cíle. Tyto profily lze použít ve spojení s interaktivními procesy k dosažení hloubkového penetračního testu. Informace získané z počátečního skenování

a analýzy lze použít k navržení strategií pro získání přístupu ke zranitelným cílům a případně k zahájení víceúrovňového útoku (explioty, nástroje pro zneužití, sociální inženýrství), které mohou prokázat dopad zranitelností a stanovení priorit nápravných kroků. (SAINT, 2022)

Proces skenování se spouští zjištěním všech aktivních cílů v zadaném seznamu nebo rozsahu. Následně vybraná skenovací zásada určí, které základní analýzy se na každém cíli spustí. Výstupy analýz pak analytický modul využije k naplánování dalších analýz a k odvození zranitelností a dalších informací na základě sad pravidel. Konečné výsledky skenování se poté uloží do centrální databáze, která slouží k podpoře analýzy dat a reportování. To probíhá prostřednictvím webového rozhraní, rozhraní příkazového řádku, nebo s přístupem přes API. (SAINT, 2022)

Sady SAINT Security Suite a SAINTCloud podporují specifikaci SCAP (Security Content Automation Protocol) jako ověřený skener konfigurace (ACS – Automated Configuration Scanner), včetně možnosti práce s CVE (Common Vulnerabilities and Exposures). SAINT podporuje otevřené standardní jazyky, výčty a metriky, mezi které momentálně patří XCCDF, OVAL, CCE, CPE, CVE a CVSS, AI, ARF a TMSAD specifikace. SAINT přijímá datové toky vyjádřené v SCAP a posuzuje cílové konfigurace dle těchto základních hodnot. Tato funkce zahrnuje i vyhodnocování obsahu SCAP z hlediska shody, zranitelností a záplat. SAINT pracuje jak se samostatnými definičními soubory OVAL, tak i s definicemi OVAL obsaženými v datových proudech vyjádřených v SCAP. SAINT dále nabízí analýzu dat, odkazy na externí autoritativní zdroje informací, rozhraní pro úpravu zásad a vytváření zpráv. Tyto funkce usnadňují lokální zkoumání a analýzu zásad. Vykazování shody probíhá formou předem definovaných šablon zpráv a vlastní prezentace výstupů v mnoha formátech (HTML, PDF, XML a CVS). Výstupy hlášení Cyberscope jsou podporovány i povinným formátem datového kanálu XML. (SAINT, 2022)

6.6 Komparace aplikací pro analýzu rizik

Jak bylo popsáno v předešlé části, každý nástroj používá různé techniky nebo strategie pro stanovení priorit na základě rizik. Většina těchto nástrojů používá k posouzení rizika, které může zranitelnost pro podnik představovat, metriky skóre CVSS, a to buď ve vlastních strategiích nástroje, nebo přidáním nových metrik, které uživateli umožňují lépe pochopit, co se v prostředí děje. Aby bylo možné získat úplnější údaje pro řízení rizik, má navíc mnoho nástrojů integrační mechanismy s dalšími komerčními technologickými partnery, které dále zlepšují správu zranitelností, jež mohou mít na informační systém vliv.

Tabulka 4 – Komparace aplikací (Greenbone AG, 2024), (Rapid7, 2024), (Vaughan, 2024), (Tenable, 2024), (SAINT, 2022)

Nástroj	**Analýza rizika**	**Strategie**	**Mechanismy integrace**
OpenVAS	CVE, CVSS	Výsledky na základě rizikových faktorů (nízké, střední, vysoké, kritické) – stanovení priorit	Kenna Security, SecPod, Greenbone
Rapid7 InsightVM	CVE, CVSS, VRP	Upřednostňuje zranitelnosti na základě rizika a specifického kontextu – skutečné hodnocení rizik	CyberArk, Atlassian, ServiceNow, McAfee, IBM QRadar SIEM, VMware Horizon
GFI LanGuard	CVE, CVSS	Řadí bezpečnostní problémy podle výhodnosti pro útočníka a narušení provozu	Přes 2500 bezpečnostních aplikací v kategoriích: antivirus: firewall, antiphishing, VPN
Tenable Vulnerability Management	CVE, CVSS, VRP	Podporuje různé strategie určování priorit včetně CVSS, zneužitelnosti a specifických souvislostí – plánované skenování, skenování skutečných rizik a skenování PCI ASV 2.0	CyberArk, BeyondTrust Password Safe, Blackberry UEM, Centrify Vault, IBM QRadar SIEM, HashiCorp Vault, ARCON
Saint Security Suite	Vlastní	Upřednostňuje zranitelnosti na základě závažnosti a kritičnosti aktiv	Cisco, Splunk, Antian, Continuum GRC

Ačkoliv většina nástrojů pro hodnocení rizik a stanovování priorit zranitelnosti spoléhá na metriky CVSS, některé z nich zahrnují i další metriky dle specifických potřeb organizace. Tyto metriky mohou zahrnovat například dopad na konkrétní oddělení, celkovou kritičnost pro chod firmy a finanční důsledky.

Nástroje pro hodnocení rizik mohou také využívat vlastní strategie hodnocení, které zohledňují širší kontext než jen technické detaily zranitelnosti. Tyto strategie mohou kombinovat obchodní faktory s informacemi o zranitelnosti a údaji o firemním prostředí, aby poskytly komplexnější pohled na riziko.

Kromě toho, mnoho nástrojů nabízí možnost integrace s řešeními od technologických partnerů. Tito partneři poskytují specializované služby pro hodnocení rizik a podporu rozhodování. Jejich řešení dokáží zpracovat výsledky skenování zranitelností ve standardizovaném formátu, jako je XML, což umožňuje pokročilejší analýzy bezpečnosti a obchodních dopadů. Je však třeba mít na paměti, že většina řešení od těchto partnerů bývá komerční nebo má omezenou zkušební dobu.

6.6.1 Mechanismy integrace OpenVAS

Mezi mechanismy integrace patří **Kenna Security**. Kenna Security, nyní součást společnosti Cisco, je platforma pro řízení zranitelností a predikci kybernetických hrozeb, která pomáhá organizacím identifikovat a řešit bezpečnostní rizika. Platforma využívá umělou inteligenci k analýze dat o zranitelnostech, hrozbách a narušeních a k hodnocení rizik jednotlivých aktiv. Díky tomu mohou bezpečnostní týmy efektivněji určit své zdroje a zaměřit se na nejkritičtější problémy. Výhodou Kenna Security je automatizace, která umožňuje automatizovat skenování zranitelností, nápravu zranitelností a dokumentaci. Zmíněná umělá inteligence slouží k predikci hrozeb a jejich prioritní nápravu. (Cisco, 2024)

SecPod je společnost zabývající se kybernetickou bezpečností, která nabízí platformu nazvanou SanerNow. Tato platforma pomáhá organizacím všech velikostí chránit a spravovat jejich koncové body. SanerNow dokáže automaticky objevovat a spravovat všechny aktiva v síti, včetně serverů, koncových bodů, síťových zařízení a cloudových instancí. Dále dokáže skenovat aktiva a identifikovat zranitelnosti. Tyto zranitelnosti mohou být zneužity útočníky k narušení systémů. Umožňuje automatizovat nasazení oprav pro zranitelnosti. To pomáhá organizacím rychle a efektivně snižovat riziko. SanerNow může zjednodušit správu koncových bodů, včetně nasazení softwaru, konfigurace a správy oprav. (SecPod Technologies, 2024)

Greenbone Enterprise Appliances jsou řada hardwarových zařízení určených pro skenování zranitelností a správu kybernetické bezpečnosti v síťových prostředích. Jsou dostupné v různých modelech s různou kapacitou a funkčností, které splňují potřeby organizací všech velikostí. Modely Greenbone Enterprise Appliances:

- **EXA** – Nejvýkonnější model, určený pro velké organizace a datová centra. Podporuje skenování milionů IP adres a disponuje rozsáhlým úložištěm pro ukládání dat o zranitelnostech.

- **PETA** – Vhodný pro středně velké organizace a pobočky. Nabízí vysoký výkon a kapacitu za dostupnou cenu.
- **TERA** – Ideální pro malé a střední firmy. Poskytuje spolehlivý výkon a funkce pro správu zranitelností v kompaktním a cenově dostupném zařízení.
- **DECA** – Určený pro menší sítě a pobočky. Nabízí základní funkce skenování zranitelností a správy kybernetické bezpečnosti.
- **CENO** – Nejkompaktnější model, vhodný pro malé sítě a individuální uživatele. Poskytuje základní funkce skenování zranitelností v přenosném zařízení.
- **25V** – Speciální model určený jako senzor pro distribuované skenovací systémy. Může být spravován master zařízením Greenbone Enterprise Appliance. (Greenbone, 2024)

Všechny modely Greenbone Enterprise Appliances zahrnují:

- **OpenVAS** – Open-source skener zranitelností, který dokáže skenovat širokou škálu systémů a aplikací a identifikovat tisíce známých zranitelností.
- **Greenbone Management System (GMS)** – Webové rozhraní pro správu skenerů OpenVAS, zranitelností a reportů. GMS umožňuje uživatelům snadno sledovat stav jejich síťové bezpečnosti a podnikat kroky k nápravě zranitelností.
- **Greenbone Security Feed (GSF)** – Databáze s více než 60 000 testy zranitelností. GSF je pravidelně aktualizován o nové zranitelnosti a testy, aby uživatelé měli vždy k dispozici nejnovější informace o hrozbách. (Greenbone, 2024)
- **CyberArk Identity Security** je komplexní řešení, které umožňuje organizacím chránit své nejcitlivější aktiva, jako jsou privilegované účty (PAM), hesla a klíče. Hlavní funkce této platformy jsou správa privilegovaných přístupů, správa hesel, správa klíčů, detekce hrozby a reakce na incidenty. (CyberArk Software, 2024)

6.6.2 Mechanismy integrace Rapid7 InsightVM

CyberArk PAM centralizuje kontrolu nad privilegovanými účty, které jsou oblíbeným cílem útočníků. Platforma umožňuje definovat granulace oprávnění, sledovat aktivity a auditovat přístup. To pomáhá organizacím chránit se před neoprávněným přístupem a eskalací privilegií. CyberArk Password Vault bezpečně ukládá a spravuje hesla, klíče API a další citlivá data. Platforma umožňuje uživatelům přistupovat k heslům bez nutnosti je si pamatovat,

čímž se snižuje riziko phishingových útoků a prolomení hesel. CyberArk Key Vault bezpečně ukládá a spravuje kryptografické klíče. Platforma umožňuje centralizovat správu klíčů, kontrolovat přístup a provádět rotaci klíčů, čímž se snižuje riziko úniku dat a narušení provozu. CyberArk Threat Detection analyzuje aktivity uživatelů a identifikuje podezřelé chování, které může indikovat kybernetický útok. Platforma umožňuje včasnou detekci a reakci na hrozby, čímž se snižuje dopad kybernetických útoků. CyberArk Incident Response umožňuje organizacím rychle a efektivně reagovat na kybernetické incidenty. Platforma umožňuje izolaci napadených systémů, obnovu dat a forenzní analýzu. (CyberArk Software, 2024)

Atlassian nabízí širokou škálu produktů, které pokrývají různé potřeby vývoje softwaru a správy projektů. Mezi nejpopulárnější produkty patří:

- Jira – Platforma pro správu projektů a sledování chyb, která umožňuje uživatelům plánovat, sledovat a dokončovat práci.
- Confluence – Platforma pro spolupráci a sdílení informací, která umožňuje uživatelům vytvářet a sdílet dokumenty, wiki stránky a další obsah.
- Bitbucket – Platforma pro hostování úložišť Git, která umožňuje uživatelům spravovat a sdílet kód.
- Bamboo – Platforma pro kontinuální integraci a kontinuální dodávání (CI/CD), která umožňuje uživatelům automatizovat testování a nasazení softwaru.
- Jira Service Management – Platforma pro správu služeb IT, která umožňuje uživatelům spravovat požadavky na podporu, incidenty a změny. (Atlassian, 2024)

Platforma **ServiceNow** umožňuje organizacím automatizovat a zefektivnit procesy v různých oblastech, jako je IT, HR, zákaznický servis a bezpečnost. Klíčové vlastnosti platformy ServiceNow zahrnují:

- IT Service Management (ITSM) – Automatizace a zefektivnění procesů ITSM, jako je správa incidentů, změn a konfigurace.
- IT Operations Management (ITOM) – Získání komplexního přehledu o IT infrastruktuře a monitorování výkonu.
- Customer Service Management (CSM) – Automatizace a zefektivnění procesů zákaznického servisu, jako je správa požadavků a řešení problémů.

- Security Operations Management (SOM) – Automatizace a zefektivnění procesů kybernetické bezpečnosti, jako je detekce a reakce na hrozby.
- Human Resource Management (HRM) – Automatizace a zefektivnění procesů HR, jako je nábor, onboarding a správa výkonu. (ServiceNow, 2024)

McAfee je americká společnost zabývající se kybernetickou bezpečností, která se zaměřuje na ochranu jednotlivců, domácností a organizací před kybernetickými hrozbami. McAfee nabízí širokou škálu produktů a služeb pro kybernetickou bezpečnost, které pokrývají různé potřeby. Mezi nejpopulárnější produkty patří:

- McAfee Total Protection – Komplexní antivirové řešení pro ochranu počítačů, smartphonů a tabletů před viry, malwarem, ransomwarem a dalšími kybernetickými hrozbami.
- McAfee LiveSafe – Antivirus, který zahrnuje všechny funkce McAfee Total Protection a navíc funkce pro rodičovskou kontrolu, ochranu identity a VPN.
- McAfee Mobile Security – Antivirové řešení pro smartphony a tablety, které chrání tato zařízení před viry, malwarem a kybernetickými útoky. (McAfee, 2024)

IBM Security QRadar SIEM (Security Information and Event Management) je platforma pro centralizovanou správu a analýzu bezpečnostních událostí, která pomáhá organizacím chránit se před kybernetickými útoky. QRadar shromažďuje a analyzuje data z různých zdrojů, jako jsou firewally, servery, síťová zařízení a koncové body, a umožňuje uživatelům sledovat a reagovat na bezpečnostní hrozby v reálném čase. Klíčové vlastnosti QRadar SIEM zahrnují:

- Sběr a agregace dat – QRadar shromažďuje data z široké škály zdrojů a umožňuje uživatelům centralizovat a normalizovat tato data pro snadnější analýzu.
- Analýza dat – QRadar používá různé techniky analýzy dat, jako je korelace událostí, strojové učení a analýza chování uživatelů, k identifikaci potenciálních bezpečnostních hrozeb.
- Detekce hrozeb – QRadar používá pravidla a detekční modely k identifikaci známých a neznámých hrozeb.
- Vyšetřování incidentů – QRadar umožňuje uživatelům vyšetřovat bezpečnostní incidenty a sledovat jejich kořenovou příčinu.

- Reakce na incidenty – QRadar umožňuje uživatelům automaticky reagovat na bezpečnostní incidenty, jako je izolace napadených systémů nebo blokování škodlivého provozu.
- Reporting a compliance – QRadar umožňuje uživatelům generovat reporty o bezpečnostní situaci a splňovat regulační požadavky. (IBM, 2024)

6.6.3 Mechanismy integrace Tenable Vulnerability Management

VMware Horizon umožňuje uživatelům přistupovat k virtuálním desktopům (plochám) a aplikacím z jakéhokoli zařízení a odkudkoli. Horizon umožňuje organizacím centralizovat správu desktopů a aplikací, což snižuje náklady a zjednodušuje správu. Základní vlastnosti této platformy jsou:

- Přístup odkudkoli – Uživatelé mohou přistupovat k desktopům a aplikacím z jakéhokoli zařízení, včetně notebooků, tabletů, smartphonů a tenkých klientů.
- Centralizovaná správa – Horizon umožňuje centralizovat správu desktopů a aplikací, což snižuje náklady a zjednodušuje správu.
- Zvýšená bezpečnost – Horizon umožňuje izolovat desktopy a aplikace od koncových bodů, čímž se snižuje riziko kybernetických útoků.
- Zlepšená škálovatelnost – Horizon umožňuje snadno škálovat desktopy a aplikace pro různé potřeby. (Broadcom, 2024)

BeyondTrust Password Safe je řešení pro správu hesel, které umožňuje organizacím bezpečně ukládat a spravovat hesla pro uživatele, aplikace a systémy. Password Safe pomáhá organizacím dodržovat regulační požadavky a chránit se před kybernetickými útoky. BeyondTrust Password Safe zahrnuje:

- Centralizované úložiště hesel – Password Safe umožňuje ukládat všechna hesla v centralizovaném úložišti, čímž se eliminuje potřeba ručního zadávání hesel uživateli.
- Správu hesel – Password Safe umožňuje automaticky generovat silná hesla, resetovat hesla a sledovat životní cyklus hesel.
- Jediné přihlášení – Password Safe umožňuje uživatelům přihlásit se k více aplikacím pomocí jediného hesla.

- Vícefaktorové ověřování (MFA) – Password Safe podporuje MFA pro další vrstvu zabezpečení.
- Auditování a reporty – Password Safe umožňuje generovat auditní reporty o aktivitách uživatelů a přístupu k heslům. (BeyondTrust, 2024)

BlackBerry UEM (Unified Endpoint Management) je platforma pro správu koncových bodů, která umožňuje organizacím spravovat a zabezpečovat širokou škálu zařízení, včetně smartphonů, tabletů, notebooků, stolních počítačů a IoT zařízení. BlackBerry UEM umožňuje:

- Nasadit a konfigurovat zařízení – BlackBerry UEM umožňuje organizacím nasadit a konfigurovat zařízení automaticky, čímž se snižuje čas a náklady na správu.
- Chránit zařízení – BlackBerry UEM umožňuje organizacím chránit zařízení před malwarem, phishingovými útoky a dalšími kybernetickými hrozbami.
- Spravovat aplikace – BlackBerry UEM umožňuje organizacím instalovat, aktualizovat a odinstalovat aplikace na zařízeních.
- Sledovat a kontrolovat zařízení – BlackBerry UEM umožňuje organizacím sledovat polohu zařízení, kontrolovat jejich obsah a blokovat ztracená nebo ukradená zařízení. (BlackBerry, 2024)

Centrify Vault je platforma pro správu privilegovaných přístupů (PAM), která umožňuje organizacím kontrolovat a spravovat přístup k privilegovaným účtům, zařízením a systémům. Centrify Vault pomáhá organizacím:

- Chránit privilegované účty – Centrify Vault umožňuje organizacím chránit privilegované účty před neoprávněným přístupem, zneužitím a krádeží.
- Sledovat a kontrolovat privilegované aktivity – Centrify Vault umožňuje organizacím sledovat a kontrolovat aktivity privilegovaných uživatelů, čímž se snižuje riziko kybernetických útoků.
- Spravovat tajné klíče – Centrify Vault umožňuje centrálně ukládat a spravovat tajné klíče, jako jsou hesla, SSH klíče a API klíče. (Delinea, 2024)

HashiCorp Vault je platforma pro centralizovanou správu tajných klíčů a konfigurací, mezi které patří hesla, kryptografické klíče a další citlivá data. Základní vlastnosti HasiCorp Vault jsou:

- Centralizované úložiště – Umožňuje centralizovaně ukládat všechna tajná data v jednom úložišti, čímž se usnadňuje správa a přístup k datům.
- Silná šifrování – Šifruje všechna tajná data v klientském i serverovém režimu, čímž se zajišťuje jejich ochrana před neoprávněným přístupem.
- Přístup na bázi rolí – Umožňuje kontrolovat přístup k tajným datům na bázi rolí a oprávnění, čímž se snižuje riziko neoprávněného přístupu.
- Auditování a reporty – Umožňuje generovat auditní reporty o aktivitách uživatelů a přístupu k tajným datům. (Hashi, 2024)

Arcon je společnost, která se zabývá vývojem softwaru pro správu dokumentů a podnikového procesního řízení. Jejich produkty pomáhají organizacím zefektivnit workflow, zlepšit spolupráci a snížit náklady. Arcon nabízí širokou škálu produktů, které splňují potřeby organizací všech velikostí, od malých firem až po velké korporace. Mezi základní vlastnosti produktů společnosti Arcon patří:

- Správa dokumentů – Ukládání, správa a sdílení dokumentů v bezpečném a centralizovaném úložišti.
- Workflow – Automatizace opakujících se úkolů a procesů pro zefektivnění práce.
- Spolupráce – Usnadnění spolupráce na dokumentech a projektech v reálném čase.
- Vyhovění regulačním požadavkům – Dodržování regulačních požadavků a zajištění bezpečnosti dat.
- Analýza a reporty – Získávání poznatků z dat a generování reportů pro zlepšení rozhodování. (ARCON, 2024)

6.6.4 Mechanismy integrace Saint Security Suite

Cisco se zabývá vývojem, výrobou a prodejem síťových zařízení, telekomunikačních produktů a dalších technologií. Mezi produkty, které nabízí patří:

- Směrovače – Zařízení, která směřují síťový provoz mezi různými sítěmi.
- Switche – Zařízení, která propojují zařízení v rámci jedné sítě.
- Síťová úložiště – Zařízení pro ukládání a sdílení dat v síti.
- Servery – Počítače pro hostování aplikací a dat.

- Síťová virtualizace – Technologie pro vytváření virtuálních sítí na fyzické infrastruktuře.
- Brány firewall – Zařízení pro ochranu sítě před kybernetickými hrozbami.
- Systémy pro detekci a prevenci vniknutí – Systémy pro detekci a prevenci neoprávněného přístupu do sítě. (Cisco Systems, 2024)

Splunk je platforma pro analýzu dat a správu logů, která umožňuje organizacím shromažďovat, analyzovat a vizualizovat data z široké škály zdrojů, včetně serverů, aplikací, síťových zařízení a zařízení IoT. Splunk umožňuje:

- Získat poznatky z dat – Splunk umožňuje organizacím extrahovat poznatky z dat, které jim pomáhají lépe porozumět jejich podnikání a rozhodovat se na základě dat.
- Řešit problémy – Splunk umožňuje organizacím rychle a efektivně identifikovat a řešit problémy v jejich IT infrastruktuře a aplikacích.
- Dodržovat předpisy – Splunk shromažďuje a analyzuje auditní protokoly, čímž pomáhá splňovat regulační požadavky. Auditní protokol slouží k trvalému dohledu nad dodržováním pravidel, brání neoprávněnému proniknutí do systému a umožňuje identifikaci a analýzu podezřelé aktivity.
- Zlepšit kybernetickou bezpečnost – Splunk umožňuje analyzovat data z různých zdrojů, jako jsou firewally, antivirové programy a síťové protokoly. (Splunk, 2024)

Anitian je platforma pro kybernetickou bezpečnost, která umožňuje organizacím chránit se před kybernetickými hrozbami. Platforma Anitian využívá umělou inteligenci a strojové učení k proaktivní identifikaci a blokování kybernetických útoků v reálném čase. Klíčové vlastnosti platformy Anitian zahrnují:

- Detekce hrozeb založená na AI – Anitian využívá AI k detekci známých i neznámých kybernetických hrozeb.
- Analýza chování – Anitian analyzuje chování uživatelů a entit v síti, aby identifikoval podezřelé aktivity.
- Automatizovaná reakce – Anitian automaticky reaguje na kybernetické útoky, aby minimalizoval jejich dopad.
- Řízení a reporting – Anitian poskytuje uživatelům řídicí panely a reporty pro monitorování kybernetické bezpečnosti jejich organizace. (Anitian, 2024)

Continuum GRC je platforma pro správu rizik a dodržování předpisů, která umožňuje organizacím identifikovat, analyzovat a řídit rizika a dodržovat regulační požadavky. Platforma Continuum GRC pomáhá:

- Získat komplexní přehled o rizicích – Continuum GRC umožňuje identifikovat a analyzovat rizika z různých zdrojů, včetně interních a externích hrozeb.
- Prioritizovat rizika – Continuum GRC umožňuje prioritizovat rizika na základě jejich pravděpodobnosti a dopadu.
- Vyvíjet a implementovat kontrolní mechanismy – Continuum GRC umožňuje vyvíjet a implementovat kontrolní mechanismy pro zmírnění rizik.
- Monitorovat a reportovat o rizicích – Continuum GRC umožňuje organizacím monitorovat rizika a reportovat o nich managementu a regulačním orgánům. (Continuum GRC, 2024)

7 NÁVRH KONCEPTUÁLNÍHO DATOVÉHO MODELU APLIKACE

Aplikace pro analýzu rizik v kybernetické bezpečnosti umožňuje identifikovat a hodnotit rizika. To zahrnuje identifikaci aktiv, hrozeb a zranitelností, analýzu pravděpodobnosti a dopadu rizik a hodnocení závažnosti rizik. Aplikace uživatelům umožňuje spravovat rizika kybernetické bezpečnosti implementací kontrol a zmírňovacích opatření. Mezi zmírňovací opatření patří sledování stavu kontrol, generování reportů o rizicích a doporučování opatření ke zmírnění rizik.

Dalším důležitým prvkem aplikace je sledování událostí. Aplikace umožňuje sledovat všechny události kybernetické bezpečnosti, ke kterým dochází v síti. Mezi tyto události se řadí sledování protokolů, identifikace podezřelých aktivit a také reakce na incidenty kybernetické bezpečnosti. Aplikace poskytuje možnost generování reportů o rizicích, událostech a kontrolách. Tyto reporty mohou být použity k podpoře rozhodování v oblasti řízení rizik.

Aplikace nabízí uživatelsky přívětivé prostředí, které je intuitivní a snadné pro používání. To zahrnuje grafické uživatelské rozhraní, dashboardy a nástroje pro vizualizaci dat.

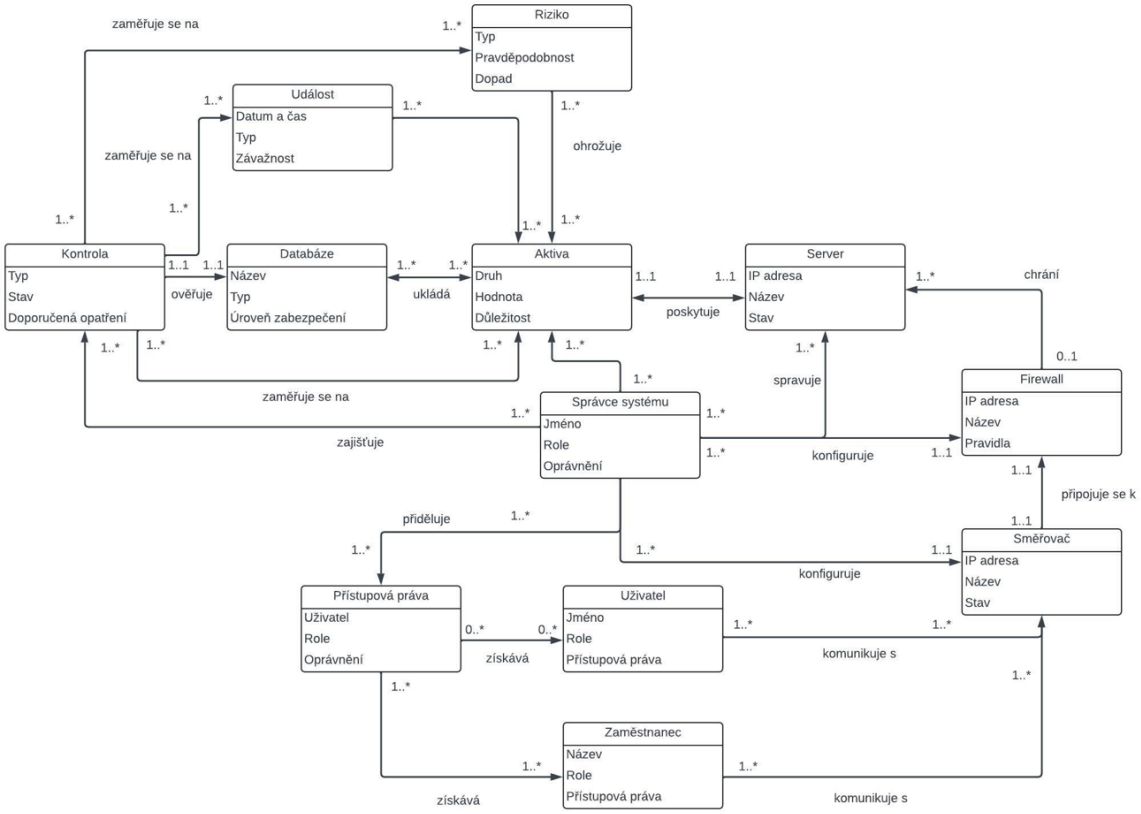
Podstatnou funkcí aplikace je integrace s jinými nástroji. Jedná se například o nástroje pro správu zranitelností, které slouží k automatické identifikaci a následné opravě zranitelností v softwaru a systémech. Dále také nástroje pro správu konfigurací, které umožňují sledovat a kontrolovat konfigurace systémů a zařízení, čímž se snižuje riziko zranitelnosti systému. Nástroje pro správu identity a přístupu umožňují aplikaci centralizovaně spravovat identitu a oprávnění uživatelů. Nástroje pro ochranu dat umožňují aplikaci šifrovat a zálohovat citlivá data. Nástroje pro detekci a reakci na hrozby slouží k automatické detekci a následné reakci na kybernetické hrozby. Nástroje pro správu hrozeb umožňují aplikaci shromažďovat a analyzovat informace o hrozbách z různých zdrojů. Nástroje pro filtrování webového obsahu umožňují aplikaci blokovat přístup k webovým stránkám a online službám, které představují hrozbu pro kybernetickou bezpečnost. Integrace s jinými nástroji poskytuje jednotné a centralizované zobrazení stavu kybernetické bezpečnosti.

Při tvorbě konceptuálního datového modelu je klíčové vymezení všech entit, které jsou důležité pro analýzu rizik v kybernetické bezpečnosti.

Obrázek 16 – Vymezení entit (Vlastní)

Entita událost reprezentuje jakoukoli událost, která se v systému stane. Může se jednat o přihlášení uživatele, změnu konfigurace nebo chybovou zprávu. Atributy této entity jsou datum a čas, typ, závažnost. Riziko představuje potenciální hrozbu pro systém. Může se jednat o malware, phishingový útok nebo neoprávněný přístup k datům. Atributy rizika jsou typ rizika, pravděpodobnost že riziko nastane a dopad rizika. Entita server představuje fyzický, nebo virtuální server, na kterém je systém provozován. Atributy jsou IP adresa, název a stav serveru. Přístupová práva definují, kdo má přístup k jakým datům a funkcím systému. Atributy přístupových práv jsou uživatel, role a oprávnění. Aktiva jsou jakýkoli cenný zdroj, který je chráněn systémem. Může se jednat o data, software, nebo hardware. Atributy aktiv jsou druh, hodnota a důležitost. Databáze představuje úložiště dat, které je používáno systémem. Entity databáze jsou název, typ a úroveň zabezpečení. Kontrola představuje mechanismus, který se používá k zmírnění rizika. Atributy zahrnují typ, stav a doporučená opatření. Zaměstnanec je osoba, která pracuje v organizaci. Atributy zaměstnance jsou jméno, role a přístupová práva. Firewall je síťové zařízení, které chrání systém před neoprávněným přístupem. Entity firewallu jsou IP adresa, název a pravidla. Správce systému je osoba zodpovědná za správu systému. Její atributy jsou jméno, role a oprávnění. Směřovač je zařízení, které směruje síťový provoz. Mezi atributy patří IP adresa, název a stav. Entita uživatel reprezentuje osobu, která používá systém, ale není zaměstnancem organizace. Atributy jsou jméno, role a přístupová práva.

Dalším krokem je definice vztahů entit. Při určování multiplicity je důležité zvážit kardinalitu vztahu.



Obrázek 17 – Konceptuální datový model (Vlastní)

Kardinalita vztahu mezi „správce systému“ a „přístupová práva“ je 1..* u obou entit, protože každý správce může mít jedno, nebo více přístupových práv.

Kardinalita přístupových práv a uživatele je 0..*, protože uživatel nemusí mít žádná přístupová práva a přístupové právo nemusí být přiděleno žádným uživatelům.

U přístupových práv a zaměstnance je kardinalita 1..*, protože každý zaměstnanec má alespoň jedno přístupové právo a každé přístupové právo je přiděleno alespoň jednomu zaměstnanci.

Kardinalita uživatele a směřovače je 1..*, což znamená že uživatel se může připojit k mnoha směřovačům a ke směřovači se může připojit mnoho uživatelů.

Kardinalita mezi zaměstnancem a směřovačem je 1..*, protože zaměstnanec se může připojit k mnoha směřovačům a k směřovači se může připojit mnoho zaměstnanců.

Kardinalita mezi směřovačem a firewallem je 1..1, protože každá směřovač je spojen s jedním firewallem a každý firewall je spojen s jedním směřovačem.

Kardinalita u firewallu (0..1) a serveru (1..*) znamená, že firewall může být připojen k žádnému, nebo k jednomu serveru. Server může být připojen alespoň k jednomu firewallu.

Kardinalita mezi entitami aktiva a server je 1..1, protože každé aktivum je umístěno na jednom serveru, a každý server hostuje jedno aktivum.

Kardinalita mezi správcem systému (1..*) a směřovačem (1..1) znamená, že jeden správce může spravovat více směřovačů, ale jeden směřovač může být spravován pouze jedním správcem.

Kardinalita mezi správcem systému (1..*) a firewallem (1..1), znamená, že jeden správce může spravovat více firewallů, ale jeden firewall může být spravován pouze jedním správcem.

Kardinalita mezi správcem systému a aktivy je 1..*, protože správce může spravovat libovolný počet aktiv. Aktivum může být spravováno libovolným počtem správců.

Kardinalita mezi kontrolou a správcem systému je 1..*, protože správce může provádět libovolný počet kontrol. Kontrola může být prováděna libovolným počtem správců.

Kardinalita mezi správcem systému a serverem je 1..*, což znamená, že správce systému může být odpovědný za několik serverů a server může spravovat několik správců systému.

Kardinalita mezi kontrolou a databází je 1..1, což znamená, že každá kontrola má přesně jednu databázi a ke každé databázi je přirazena jedna kontrola. To znamená, že informace o dané kontrole jsou uloženy v jediné databázi a tato databáze neukládá informace o žádné jiné kontrole. Příkladem může být firewall, který má svou vlastní konfigurační databázi, která ukládá nastavení a protokoly specifické pro tento firewall.

Kardinalita mezi databází a aktivem je 1..*, což znamená, že záznam v databázi může popisovat mnoho aktiv. To je užitečné, pokud sdílejí společnou vlastnost, jako je typ, umístění, nebo funkce. Například jedna databáze by mohla obsahovat informace o všech serverech, zatímco jiná by mohla obsahovat informace o všech síťových zařízeních. Aktivum může být popsané ve více databázích. Informace o jednom aktivu se mohou nacházet v různých databázích, v závislosti na kontextu a potřebách.

Kardinalita mezi kontrolou a událostí je 1..* a znamená to, že kontrola se může zabývat mnoho událostmi. Událost může být spojena s libovolným počtem kontrol.

Kardinalita mezi kontrolou a rizikem je 1..*, což znamená že záznam kontroly může popisovat více rizik. Riziko může být spojeno s mnoho kontrolami.

Kardinalita mezi rizikem a aktivem je 1..*. To znamená že aktivum může ohrožovat více rizik a riziko může ohrožovat více aktiv.

Kardinalita mezi aktivem a událostí je 1..*. Znamená to, že k aktivu se může vztahovat více událostí a k události může patřit mnoho aktiv.

Kardinalita mezi kontrolou a aktivem 1..* znamená, že kontrola může zahrnout mnoho aktiv. Aktivum pak může být podrobeno mnoho kontrolám.

Konceptuální datový model aplikace pro analýzu rizik v kybernetické a informační bezpečnosti popisuje vztahy mezi entitami pomocí sloves. Například správce systému zajišťuje kontrolu, která se zaměřuje na rizika, která ohrožují aktiva.

ZÁVĚR

Kybernetická bezpečnost procházela v posledních letech dynamickou transformací, aby dokázala reagovat na neustále se vyvíjející hrozby. Útočníci se stávají sofistikovanějšími a využívají pokročilé techniky, jako je malware, phishing a ransomware, k napadení systémů a krádeži dat. Rostoucí popularita cloudu s sebou přináší i nárůst rizika kybernetických útoků, a proto je nezbytné, aby poskytovatelé cloudových služeb implementovali dostatečná bezpečnostní opatření pro ochranu dat svých klientů.

V teoretické části práce byla využita metoda rešerše, která sloužila ke stanovení základních pojmů v oblasti kybernetické bezpečnosti. Řízení rizik v oblasti informační bezpečnosti představuje komplexní proces, který umožňuje organizacím systematicky identifikovat, analyzovat a zvládat rizika ohrožující jejich informační aktiva. V oblasti kybernetické bezpečnosti se termín informační aktiva používá pro označení všech informačních zdrojů organizace, které je nutné chránit před kybernetickými útoky. Mezi informační aktiva patří datové zdroje, software, hardware a sítě.

V praktické části byly představeny jednotlivé aplikace pro analýzu v kybernetické a informační bezpečnosti a jejich funkce, které nabízí. Následně byla provedena komparace těchto aplikací. Každá aplikace nabízí také takzvané mechanismy integrace, které umožňují propojení různých aplikací pro analýzu rizik v kybernetické bezpečnosti a sdílet mezi nimi data a informace. V návaznosti na kapitolu datového modelování je v závěru práce vypracován konceptuální datový model aplikace pro analýzu rizik v kybernetické bezpečnosti. Na základě obsahu zpracované práce byly cíle naplněny. Přínosem bakalářské práce je získání základních znalostí a návazností v oblasti kybernetické bezpečnosti.

V závěru lze konstatovat, že ochrana informačních systémů je komplexní a neustálý proces, který vyžaduje trvalou pozornost a investice. Vzhledem k rostoucí závislosti na informačních technologiích je to však nezbytná investice, která se v konečném důsledku mnohonásobně vrátí v podobě zajištění bezpečnosti dat a integrity informační infrastruktury.

SEZNAM POUŽITÉ LITERATURY

AGAR, Robert, 2021. *Stages and Types of Data Models* [online]. [cit. 2024-04-21]. Dostupné z: https://tdan.com/stages-and-types-of-data-models/28201

ANITIAN, 2024. *Anitian* [online]. [cit. 2024-04-21]. Dostupné z: https://www.anitian.com/

ARCON, 2024. *Arcon* [online]. [cit. 2024-04-21]. Dostupné z: https://arconnet.com/

ATLASSIAN, 2024. *Atlassian* [online]. [cit. 2024-04-20]. Dostupné z: https://www.atlassian.com/

AWATI, Rahul a Linda ROSENCRANCE, 2021. *Computer hardware*. In: TechTarget [online]. [cit. 2024-01-10]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/hardware

AWATI, Rahul a Marry K. PRATT, 2023. *ICT (information and communications technology or technologies).* In: TechTarget [online]. [cit. 2024-01-01]. Dostupné z: https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies

BEYONDTRUST, 2024. *BeyondTrust Password Safe* [online]. [cit. 2024-04-21]. Dostupné z: https://www.beyondtrust.com/products/password-safe

BLACKBERRY, 2024. *BlackBerry UEM* [online]. [cit. 2024-04-21]. Dostupné z: https://www.blackberry.com/us/en/products/blackberry-uem

BROADCOM, 2024. *VMware Horizon* [online]. [cit. 2024-04-21]. Dostupné z: https://www.vmware.com/products/horizon.html

CANHASI, Ercan, 2023. *OOP: Inheritance vs. Aggregation* [online]. [cit. 2024-04-21]. Dostupné z: https://www.baeldung.com/cs/inheritance-aggregation

CISCO SYSTEMS, 2024. *Cisco: Software, Network and Cybersecurity Solutions* [online]. [cit. 2024-04-21]. Dostupné z: https://www.cisco.com/

CISCO, 2024. *Kenna Security Is Part of Cisco*. Introducing Cisco Hypershield [online]. [cit. 2024-04-20]. Dostupné z: https://www.cisco.com/c/en/us/products/security/kenna-is-part-of-cisco.html

CLARK, Robert M., HAKIM, Simon, ed., 2017. *Cyber-Physical Security*. 3rd edition. Springer. ISBN 978-3-319-32824-9.

CONTINUUM GRC, 2024. *Enterprise Risk Management Solution Provider: Continuum GRC* [online]. [cit. 2024-04-21]. Dostupné z: https://continuumgrc.com/

CYBERARK SOFTWARE, 2024. *Introducing CyberArk Secure Browser: Your gateway to securing all identities with a single click.* [online]. [cit. 2024-04-20]. Dostupné z: https://www.cyberark.com/

ČESKÁ REPUBLIKA, 2020. *Národní strategie kybernetické bezpečnosti České republiky*. In: s. 23. [cit. 30. 10. 2023]. Dostupné také z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

DELINEA, 2024. *Delinea Vault Suite* [online]. [cit. 2024-04-21]. Dostupné z: https://delinea.com/products/delinea-vault-suite

GREENBONE AG, 2024. *Background*. Greenbone Community Edition – Documentation [online]. [cit. 2024-04-20]. Dostupné z: https://greenbone.github.io/docs/latest/background.html#history-of-the-openvas-project

HASHI, 2024. *HashiCorp Vault* [online]. [cit. 2024-04-21]. Dostupné z: https://www.vaultproject.io/

IBM, 2024. *IBM Security QRadar SIEM* [online]. [cit. 2024-04-21]. Dostupné z: https://www.ibm.com/products/qradar-siem

INDEED, 2022. *Systems Analyst Interview Questions With Example Answers* [online]. [cit. 2024-04-21]. Dostupné z: https://www.indeed.com/career-advice/interviewing/systems-analyst-interview-questions

KALUŽA, Jindřich a Ludmila KALUŽOVÁ, 2012. *Modelování dat v informačních systémech*. 1. Praha: Ekoexpress. ISBN 978-80-86929-91-1.

KERNER, Sean Michael, 2021. *Internet Protocol (IP)*. In: TechTarget [online]. [cit. 2024-02-11]. Dostupné z: https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol

KOLOUCH, Jan et al., 2019. *CyberSecurity*. 1. Praha: CZ.NIC. ISBN 978-80-88168-34-8.

KOLOUCH, Jan, 2017. *CyberCrime*. 1. CZ.NIC. ISBN 978-80-88168-15-7.

MCAFEE, 2024. *McAfee* [online]. [cit. 2024-04-21]. Dostupné z: https://www.mcafee.com/

MICROSOFT, 2024. Co je modelování dat? [online]. [cit. 2024-04-30]. Dostupné z: https://powerbi.microsoft.com/cs-cz/what-is-data-modeling/

NOVÁČEK, Šimon, 2023. *Lekce 1 - Sítě – Typy používaných sítí*. In: Itnetwork.cz [online]. [cit. 2024-02-09]. Dostupné z: https://www.itnetwork.cz/site/zaklady/site-typy-pouzivanych-siti

ORACLE, 2024. *Práce s nástrojem Data Modeler ve službě Oracle Analytics Cloud* [online]. [cit. 2024-04-21]. Dostupné z: https://docs.oracle.com/cloud/help/cs/analytics-cloud/ACSMD/GUID-D53FEF32-BEE5-4612-9041-430D09294E65.htm#BILUG31

RAPID7, 2024. *Glossary*. Rapid7 – Documentation [online]. [cit. 2024-04-20]. Dostupné z: https://docs.rapid7.com/insightvm/glossary

RAPID7, 2024. *Welcome to InsightVM*. Rapid7 – Documentation [online]. [cit. 2024-04-20]. Dostupné z: https://docs.rapid7.com/insightvm/

REFSDAL, Atle, Bjørnar SOLHAUG a Ketil STØLEN, 2015. *Cyber-Risk Management*. 1. Springer. ISBN 978-3-319-23570-7.

ROSENCRANCE, Linda, 2021. *Software*. In: TechTarget [online]. [cit. 2024-01-10]. Dostupné z: https://www.techtarget.com/searchapparchitecture/definition/software

SAINT, 2022. *SAINT v9 Security Suity User Documentation*. SAINT Security Suite [online]. [cit. 2024-04-20]. Dostupné z: https://my.saintcorporation.com/resources/documentation/SAINT9UserDocumentation.pdf

SCARPATI, Jessica, 2023. *WAN (wide area network).* In: TechTarget [online]. [cit. 2024-02-11]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/WAN-wide-area-network

SECPOD TECHNOLOGIES, 2024. *Prevent Cyberattacks. Faster. Better.* [online]. [cit. 2024-04-20]. Dostupné z: https://www.secpod.com/

SERVICENOW, 2024. *ServiceNow* [online]. [cit. 2024-04-21]. Dostupné z: https://www.servicenow.com/

SILVA, Nishadha, 2024. *What is an Entity Relationship Diagram* [online]. [cit. 2024-04-21]. Dostupné z: https://creately.com/guides/er-diagrams-tutorial/

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk. ISBN 9788073807658.

SPLUNK, 2024. *Splunk* [online]. [cit. 2024-04-21]. Dostupné z: https://www.splunk.com/

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 148 s. ISBN 9788073807375.

TENABLE, 2024. *Tenable Vulnerability Management User Guide*. Tenable [online]. [cit. 2024-04-20]. Dostupné z: https://docs.tenable.com/vulnerability-management/Content/PDF/Tenable_Vulnerability_Management-User_Guide.pdf

UNIVERSITY OF BRISTOL, 2024. *What are multilevel models and why should I use them?* [online]. [cit. 2024-04-21]. Dostupné z: https://www.bristol.ac.uk/cmm/learning/multilevel-models/what-why.html

ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ, 2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik a informační bezpečnosti*. 4.

VAUGHAN, Eric, 2024. *GFI Languard*. GFI Software [online]. [cit. 2024-04-20]. Dostupné z: https://www.gfi.com/products-and-solutions/network-security-solutions/languard

WATT, ADRIENNE, 2014. *Chapter 8 The Entity Relationship Data Model* [online]. [cit. 2024-04-21]. Dostupné z: https://opentextbc.ca/dbdesign01/chapter/chapter-8-entity-relationship-model/

WRIGHT, Gavin, 2021. *Metropolitan area network (MAN).* In: TechTarget [online]. [cit. 2024-02-10]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/metropolitan-area-network-MAN

YASAR, Kinza, 2022. *MAC address (media access control address).* In: TechTarget [online]. [cit. 2024-02-16]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/MAC-address

YASAR, Kinza, 2022. *Personal area network (PAN)*. In: TechTarget [online]. [cit. 2024-02-10]. Dostupné z: https://www.techtarget.com/searchmobilecomputing/definition/personal-area-network

YASAR, Kinza, 2022. *Primary key (primary keyword)*. TechTarget [online]. [cit. 2024-04-21]. Dostupné z: https://www.techtarget.com/searchdatamanagement/definition/primary-key

YASAR, Kinza, 2023. *IP address (Internet Protocol address).* In: TechTarget [online]. [cit. 2024-02-14]. Dostupné z: https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address

YASAR, Kinza, GILLIS, Alexander S., ed., 2023. *Computer network*. In: TechTarget [online]. [cit. 2024-02-10]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/network

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API Application Programming Interface

CERT Computer Emergency Response Team

E-R Entity Relationship

ERM Enterprise Risk Management

ICT Informační a komunikační technologie

IP Internet Protocol

NIC Network Interface Controller

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

OID Object Identifier

SQL Structured query language

TCP Transmission Control Protocol

UML Unified Modelling Language

VM Vulnerability Management

XML Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK