ŽILINSKÁ UNIVERZITA V ŽILINE

FAKULTA RIADENIA A INFORMATIKY

DIZERTAČNÁ PRÁCA

Ing. Michal Šterbák

Systém automatizovaného zberu informačných aktív a ich hodnotenia

Vedúci práce: doc. Ing. Pavel Segeč, PhD.

Registračné číslo: 28360020233005

Žilina, 2023

ŽILINSKÁ UNIVERZITA V ŽILINE

FAKULTA RIADENIA A INFORMATIKY

DIZERTAČNÁ PRÁCA

ŠTUDIJNÝ ODBOR: Informatika

Ing. Michal Šterbák

Systém automatizovaného zberu informačných aktív a ich hodnotenia

Žilinská univerzita v Žiline

Fakulta riadenia a informatiky

Školiace pracovisko: Katedra informačných sietí

Žilina, 2023

Čestné vyhlásenie

Čestne vyhlasujem, že celú dizertačnú prácu na tému „Systém automatizovaného zberu informačných aktív a ich hodnotenie“, vrátane všetkých jej príloh a obrázkov, som vypracoval samostatne, a to s využitím dostupnej literatúry, vlastných vedomostí pod vedením vedúceho práce doc. Ing. Pavla Segeča, PhD. a školiteľa špecialistu Mgr. Jany Uramovej, PhD. Všetku literatúru použitú v práci som uviedol v priloženom zozname.

.....

V Žiline, dňa 27.2.2023 Ing. Michal Šterbák

Poďakovanie

Moje poďakovanie patrí vedúcemu práce doc. Ing. Pavlovi Segečovi, PhD. a školiteľovi špecialistovi Mgr. Jane Uramovej, PhD., ako aj ďalším kolegom, ktorí mi poskytli odbornú pomoc, pripomienky a usmernenie pri tvorbe práce.

ABSTRAKT V ŠTÁTNOM JAZYKU

ŠTERBÁK, Michal: *Systém automatizovaného zberu informačných aktív a ich hodnotenia*. [Dizertačná práca]. – Žilinská univerzita v Žiline, Fakulta riadenia a informatiky, Katedra informačných sietí. –Vedúci: doc. Ing. Pavel Segeč, PhD. – Školiteľ špecialista: Mgr. Jana Uramová, PhD. - stupeň odbornej kvalifikácie: Doktor v odbore Aplikovaná informatika. Žilina: FRI ŽU v Žiline, 2023. - 140 s.

Cieľom predloženej dizertačnej práce je navrhnúť systém automatizovaného zberu informačných aktív a ich hodnotenia. Prvá časť práce popisuje súčasné prístupy a odporúčania pre systém riadenia informačnej bezpečnosti na základe dostupných štandardov a noriem. Následne popisuje identifikované možnosti pre zlepšenie jednotlivých podprocesov s využitím automatizácie v celom procese systému riadenia informačnej bezpečnosti. Ďalšia časť práce sa venuje analýze a výberu vhodného prístupu k automatizácií procesu zberu informačných aktív. Detailne popisuje navrhované algoritmy pre automatizovaný zber informačných aktív, ako aj možnosti zlepšenia ďalších podprocesov. Časť práce je venovaná metódam, navrhovaným pre výpočet hodnoty informačných aktív ako aj možnostiam pre vytváranie simulácií, ktoré slúžia na predikciu zmeny rizika. Na základe navrhovaných riešení boli v poslednej časti práce formulované odporúčania pre implementáciu systému riadenia informačnej bezpečnosti automatizovaným spôsobom.

Kľúčové slová: automatizácia, informačná bezpečnosť, zber IT aktív, systém riadenia informačnej bezpečnosti, simulácia dopadov,

ABSTRAKT V CUDZOM JAZYKU

ŠTERBÁK, Michal: *System of automated collection of information assets and their evaluation*. [Dissertation thesis]. – University of Žilina, Faculty of Management Science and Informatics, Department of InfoComm Networks. –Tutor: doc. Ing. Pavel Segeč, PhD. – Specialist tutor: Mgr. Jana Uramová, PhD. - Qualification level: Doctor of Applied Informatics. Žilina: FRI ŽU in Žilina, 2023. - 140 s.

The aim of this dissertation thesis is to design a system for the automated collection of information assets and their evaluation. First part of the thesis describes current approach and recommendations for the information security management system based on available standards and norms. Subsequently, it describes the identified possibilities of improving individual sub-processes with the use of automation in the entire process of the information security management system. Next part deals with the analysis and selection of a suitable approach to the automation of the process of collecting information assets. It describes in detail the proposed algorithm for the automated collection of information assets from the network, as well as the possibilities of improving other sub-processes. Part of the publication is devoted to the methods proposed for calculating the value of information assets as well as the possibilities of creating simulations that serve to predict changes in risk value. Based on the proposed solutions, recommendations for the implementation of the information security management system in an automated manner were formulated in the last part of the thesis.

Key words: automation, information security, gathering IT assets, information security management system, simulation of impacts,

Obsah

Zoznam obrázkov

Zoznam tabuliek

Zoznam skratiek

Skratka	Anglický názov	Slovenský význam
API	Application Programming Interface	Rozhranie na programovanie aplikácií
BCMS	Business Continuity Management System	Systém riadenia kontinuity podnikania
CDP	Cisco Discovery Protocol	Sieťový protokol na určenie základných informácií o susedných zariadeniach
CIA	Confidentiality, Integrity, Availability	Dôvernosť, Integrita, Dostupnosť
COBIT	Control Objectives for Information and related Technology	Rámec pre správu a riadenie informatiky
COSO	Committee of Sponsoring Organizations	Organizácia, ktorá vyvíja usmernenia pre podniky na hodnotenie vnútorných kontrol a riadenie rizík
CPU	Central Processor Unit	Centrálna procesorová jednotka
CSF	Cybersecurity Framework	Rámec kybernetickej bezpečnosti
CVSS	Common Vulnerability Scoring System	Štandard hodnotenia závažnosti bezpečnostných zraniteľností počítačových systémov
DNS	Domain Name System	Systém doménových mien
DREAD	Damage, Reproducibility, Exploitability, Affected users, Discoverability	Poškodenie, Reprodukovateľnosť, Využiteľnosť, Zasiahnutí používatelia, Zistiteľnosť
GDPR	General Data Protection Regulation	Všeobecné nariadenie o ochrane údajov

GRC	Governance, Risk, Compliance	Riadenie, Riziko, Dodržiavanie predpisov
HDD	Hard Disk Drive	Pevný disk
HW	Hardware	Technické vybavenie počítača
ISO	International Organization for Standardization	Medzinárodná organizácia pre normalizáciu
ISRM	Information Security Risk Management	Riadenie rizika informačnej bezpečnosti
JSON	JavaScript Object Notation	Spôsob zápisu dát nezávislý na počítačovej platforme
KB	----------	Kybernetická Bezpečnosť
MIB	Management Information Base	Databáza na riadenie entít
MTU	Maximum Transmission Unit	Maximálna veľkosť datagramu
OS	Operating System	Operačný systém
OWASP	Open Web Application Security Project	Projekt a komunita, ktorá rieši bezpečnosť webových aplikácií
PDCA	Plan, Do, Check, Act	Plánovať, Robiť, Kontrolovať, Vykonávať
RAM	Random Access Memory	Operačná pamäť
REST API	Representational State Transfer Application Programming Interface	Všeobecne prijímaný príklad softvérovej architektúry distribuovaných systémov, najmä webových služieb
RM	Risk Management	Riadenie rizík
ROLFP	Reputation, Operational, Legal, Financial, People	Reputácia, Operatíva, Právo, Financie, Ľudia
IEC	International Electrotechnical Commission	Medzinárodná elektronická komisia
IKT	----------	Informačno-Komunikačné Technológie
IP	Internet Protocol	Internetový protokol
IS	Information system	Informačný systém

ISACA	Information System Audit and Control Association	Medzinárodná asociácia pre audit a kontrolu informačných systémov
ISO	International Standardization Organization	Medzinárodná norma pre normalizáciu
ISMS	Information Security Management System	Systém manažérstva informačnej bezpečnosti
IT	Information Technology	Informačná technológia
ITAM	Information Technology Asset Management	Informačná technológia riadenia aktív
ITU	International Telecommunication Union	Medzinárodná komunikačná agentúra
LLDP	Link Layers Discovery Protocol	Sieťový protokol na určenie základných informácií o susedných zariadeniach
MAC	Media Access Control	Riadenie prístupu k médiu
MOSP	MONARC Object Sharing Platform	MONARC Platforma pre zdieľanie inštancií objektov v databáze
NIST	National Institute of Standards and Technology	Národný inštitút pre štandardy a technológie
NIST SP	NIST Special Publication	Špeciálne publikácie NIST
SNMP	Simple Network Management Protocol	Jednoduchý protokol manažmentu siete
SSH	Secure Shell	Zabezpečený prístup k príkazovému riadku
SW	Software	Softvér
VLAN	Virtual Local Area Network	Virtuálna lokálna sieť
WMI	Windows Management Instrumentation	Zoskupenie rozšírení riadiaceho modelu pre Windows, ktorý poskytuje rozhranie operačného systému pre získavanie údajov

Úvod

Využívanie rôznej výpočtovej techniky a informačných technológií (IT), ako napríklad počítače, tlačiarne, servery, sieťové prvky, cloudové úložiská, cloudové služby a v neposlednom rade aj rôzny aplikačný softvér, sú neodmysliteľnou súčasťou každodenného života organizácií. Všetky tieto prvky podnikovej IT infraštruktúry sú potrebné a nevyhnutné pre fungovanie organizácie za účelom plnenia podnikových cieľov a dosahovania zisku. Pre všetky tieto technické ale aj netechnické prvky existuje jedno pomenovanie, a to ***informačné aktíva*** (IT aktíva). IT aktíva zohrávajú v organizácii rôzne dôležité až kľúčové úlohy. Pri kľúčových aktívach je nevyhnutné, aby boli dostupné, zabezpečené, prístupné len autorizovaným používateľom a schopné stabilne podporovať dané podnikové procesy. Na základe ich dôležitosti v organizácii spoločnosti sa naskytá otázka riadenia bezpečnosti týchto aktív a celkovo auditovania bezpečnosti organizácie za účelom dosiahnutia očakávanej úrovne zabezpečenia, súladu a šetrenia finančných prostriedkov organizácie.

Výrazným problémom súčasnej doby je masívna digitálna transformácia informácií, podnikových štruktúr a procesov do kybernetického priestoru, čo spôsobuje nárast zraniteľností, hrozieb a rizík, ktoré na podnikové aktíva vplývajú. Na druhej strane tak zároveň narastá dôležitosť bezpečnosti a zabezpečenia podnikových aktív. Z hľadiska bezpečnosti pod zraniteľnosťou rozumieme vlastnosť informačného aktíva, ktorá označuje jeho nedostatok alebo slabinu. Existencia zraniteľnosti následne umožňuje uplatnenie potencionálnej hrozby. Pod pojmom hrozba tak rozumieme označenie zdroja negatívnej udalosti, sily, osoby alebo aktivity, ktorá chce alebo môže poškodiť hodnotu aktíva. To znamená, že hrozba využíva zraniteľnosť alebo zraniteľné miesta. Hrozba tak má nežiadúci vplyv na bezpečnosť organizácie a môže pri využití objavenej zraniteľnosti spôsobiť škodu, stratu, neželanú zmenu, či iný nežiadúci jav. S pojmom hrozby tak súvisí riziko, ktoré označuje neistý výsledok s možným nežiadúcim stavom. Riziko teda vyjadruje pravdepodobnosť dosiahnutia výsledku, ktorý je rozdielny od očakávaného. Riziko znamená potenciál naplnenia hrozby, potenciálny problém, nebezpečenstvo vzniku škody, možnosť zlyhania a neúspechu, poškodenia, straty či zničenia.

Práve digitalizáciou informácií a súvisiacim nárastom rizík sa stáva v podnikovej praxi veľmi aktuálnou témou efektívne riadenie informačnej bezpečnosti [1][2][3]. Jedným z hlavných faktorov pri riadení bezpečnosti v kybernetickom priestore je čas a finančné

či personálne zdroje organizácie, aby tá vedela promptne reagovať na nepriaznivé javy, anomálie, bezpečnostné incidenty a bola schopná zmierňovať ich dopady. Cieľom informačnej bezpečnosti je dodržiavanie troch základných vlastností IT aktív, nazývaných aj CIA triádou:

- Dodržanie **dostupnosti** *(availability)*. IT aktíva budú prístupné vtedy, keď ich zainteresované strany potrebujú.
- Dodržanie **dôvernosti** *(confidentiality)*. IT aktíva budú poskytované osobám, ktoré majú autorizáciu k prístupu k nim a ich používaniu.
- Dodržanie **integrity** *(integrity)*. Informácie budú dostupné kompletné a úplné.

Pre analýzu a nastavenie informačnej bezpečnosti na základe bezpečnostných štandardov a legislatíve existujú súhrny procesov medzi ktoré radíme systém riadenia informačnej bezpečnosti (ISMS), riadenie rizík informačnej bezpečnosti (ISRM) a kontinuitu podnikania (BCMS). Pre zhodnotenie informačnej bezpečnosti alebo posúdenie súladu voči bezpečnostným štandardom a legislatíve slúži audit informačnej bezpečnosti. Problémom procesov ISMS, ako aj procesu auditovania je, že pozostávajú z mnohých podprocesov a činností, ktoré sú aj v súčasnosti vo veľkej miere manuálne, časovo náročné a podliehajú skúsenostiam audítora alebo bezpečnostného manažéra. Toto vo výsledku výrazne obmedzuje možnosti na častejšie, presnejšie a efektívnejšie vykonávanie ISMS a jeho kontrol alebo bezpečnostných auditov, ako si to súčasná dynamická doba a požiadavky digitálnej transformácie žiadajú.

Práve z tohto dôvodu považujeme za potrebné tieto podprocesy skúmať za účelom ich možného automatizovania s využitím informatických prostriedkov, čo je aj východiskom riešenia predkladanej dizertačnej práce. Vykonanou analýzou jednotlivých podprocesov ISMS s ohľadom na ich možnú automatizáciu sa nám podarilo identifikovať možné oblasti aplikácie automatizácie do procesov riadenia bezpečnosti organizácie. Predpokladáme, že s využitím automatizácie a nasadením dostupných informačných prostriedkov sa zabezpečí rýchlejší, plynulejší, presnejší a častejší priebeh auditov pre organizácie, čo povedie k znižovaniu miery rizika vyplývajúceho z uskutočnenia kybernetických hrozieb. Okrem plynulejšieho priebehu auditov takisto predpokladáme, že automatizácia má potenciál pomôcť organizáciám aj pri zavádzaní ISMS do ich podnikového prostredia.

Cieľom práce je navrhnúť systém automatizovaného zberu IT aktív a ich hodnotenia. Na dosiahnutie cieľa bolo ako prvé potrebné analyzovať existujúce riešenia, ako aj jednotlivé procesy ISMS. Výsledky analýzy sú bližšie popísané v kapitole 1.1, kde sme identifikovali viaceré možnosti uplatnenia automatizácie a vylepšení jednotlivých procesov, ktoré by mohli pomôcť pri implementácii ISMS alebo audite IT bezpečnosti.

Kapitola 2 uvádza ciele práce a metodiku jej riešenia na základe stanovaných čiastkových cieľov. Kapitola 3 ako nosná časť predkladanej práce sa venuje našim návrhom a podrobným popisom nových algoritmov automatizovaného zberu IT aktív s využitím sieťových protokolov a nástrojov skenovania siete pre aplikáciu do podnikových procesov bezpečnosti. Ako súčasť riešenia sme navrhli dátový model pre ukladanie zozbieraných údajov s ohľadom na virtualizáciu hardvérových aktív. Súčasťou návrhu je hierarchický model skladania a rozkladania IT aktív na primárne a sekundárne, ktorý sa následne využíva za účelom celkového hodnotenia IT aktív a zmierňovania rizík informačných aktív. Proces identifikácie a ohodnocovania IT aktív sme rozšírili o nový prístup, kedy využívame vytváranie topologickej mapy informačno-komunikačnej infraštruktúry podniku ako prostriedku pre lepšiu vizualizáciu vzájomných vzťahov jednotlivých aktív. Mapa sa vytvára na základe automaticky zozbieraných informácií. Lepšia vizualizácia zozbieraných informácii o aktívach organizácie napomáha v ďalších podprocesoch ISMS pri rozhodovaní o potrebách implementácie nápravných opatrení v procese riadenia rizík. Okrem vizualizácie vzájomných vzťahov využívame túto mapu pre vytváranie simulácií a znázornenie ich dopadov. Vizualizácia vzájomných vzťahov aktív napomáha aj pri riadení kontinuity podnikania a identifikácií ohrozených miest v infraštruktúre organizácie.

Finálne sme na základe vykonaných analýz procesov ISMS a dostupných nástrojov navrhli a detailne popísali generickú architektúru riešenia vedúceho k tvorbe informačného systému (IS). Takýto IS má potenciál stať sa centralizovaným nástrojom celkového systému riadenia informačnej bezpečnosti organizácie s využitím prostriedkov automatizácie pre identifikované procesy.

1 Informačná a kybernetická bezpečnosť

Informačno-komunikačné technológie (IKT) sa neustále vyvíjajú a poskytujú stále viac možností ich využitia. Spracovávajú rôzne informácie a dáta, pomocou ktorých podporujú organizácie pri ich každodenných činnostiach a plnení podnikových cieľov. Ako už bolo v úvode spomenuté, digitalizáciou informácií a spôsobom ich používania sa rozšírili aj zraniteľnosti, hrozby a s tým spojené riziká, ktoré vplývajú na IT aktíva a samotné informácie. Z tohto dôvodu je potrebné riešiť bezpečnosť IT aktív, ktoré vstupujú do obchodného procesu a riešiť ich dôvernosť, integritu a dostupnosť.

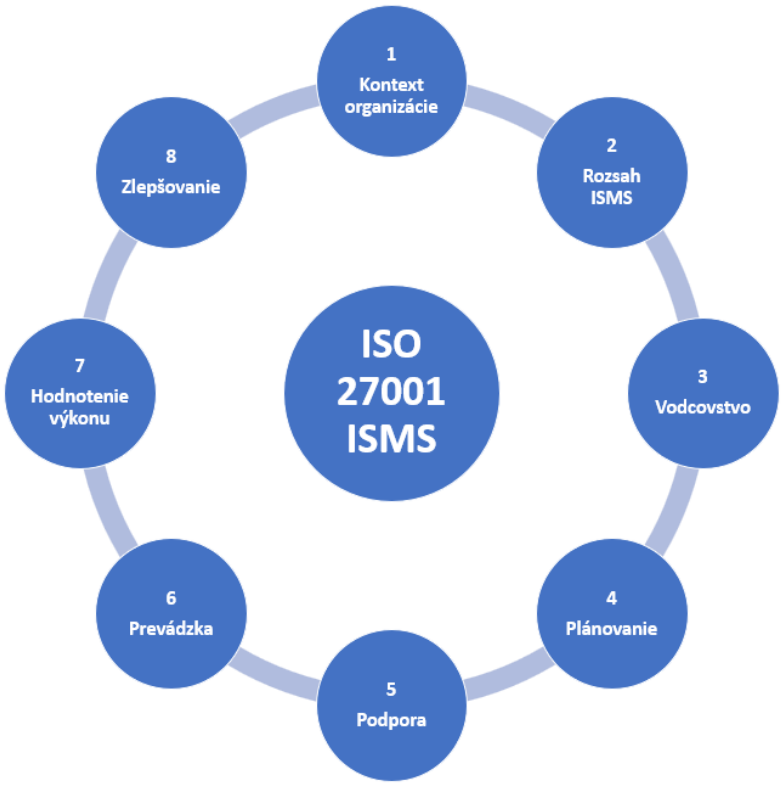
Za účelom riešenia zabezpečenia IT aktív slúži systém riadenia informačnej bezpečnosti (ISMS). ISMS je systém, ktorý je definovaný v štandarde ISO/IEC 27001 [4]. Jeho rozšírením je štandard ISO/IEC 27005, ktorý sa venuje riadeniu rizík informačnej bezpečnosti. Okrem štandardov z rodiny ISO/IEC 27000 je pre ISMS neoddeliteľnou súčasťou aj riadenie kontinuity podnikania (BCMS), ktorej systém je definovaný v štandarde ISO 22301.

Dôležitou súčasťou pre dodržiavanie informačnej a kybernetickej bezpečnosti v organizácii je bezpečnostná politika. Bezpečnostná politika je dokument, ktorý popisuje pravidlá, očakávania a celkový prístup, ktorý organizácia používa na zachovanie dôvernosti, integrity a dostupnosti svojich údajov. Normy informačnej a kybernetickej bezpečnosti sú medzinárodné uznávané odporúčania, ktoré ponúkajú techniky ako chrániť prostredie používateľa alebo organizácie. Takéto prostredie zahŕňa používateľov, komunikačnú sieť, zariadenia, softvér, procesy, informácie, aplikácie, služby a systémy. Cieľom týchto štandardov je jasne definovať postupy a rámce, na čo všetko by sa nemalo zabudnúť pri riadení informačnej bezpečnosti, posudzovaní rizík, vytváraní bezpečnostných politík a posudzovaní súladu voči týmto štandardom pri audite.

V tejto kapitole sa zameriame na popis niekoľkých štandardov a noriem, ktoré sa týkajú riadenia informačnej/kybernetickej bezpečnosti, riadenia rizík informačnej bezpečnosti, kontinuity podnikania a auditu informačnej bezpečnosti. Analyzujeme procesy potrebné pre zavedenie ISMS, s tým, že sa hlbšie zameriame na procesy v ktorých je možné aplikovať automatizáciu činností a iné možné vylepšenia.

1.1 Systém riadenia informačnej bezpečnosti (ISMS)

Systém riadenia informačnej bezpečnosti (ISMS) je efektívny dokumentovaný systém stanovujúci základné požiadavky pre informačnú bezpečnosť vo všetkých formách jej reprezentácie. ISMS je definovaný viacerými medzinárodnými štandardmi, ktoré odporúčajú požiadavky na správu systémov riadenia bezpečnosti informácií [5][6][7]. Cieľom ISMS je minimalizovať riziko a zabezpečiť kontinuitu podnikania proaktívnym obmedzením dopadu narušenia bezpečnosti. Pri implementácií ISMS v organizácii je odporúčané postupovať podľa normy ISO/IEC 27001, ktorá poskytuje odporúčania pre zavádzanie postupov a procesov v rámci riadenia informačnej bezpečnosti [8]. Norma špecifikuje požiadavky na popis kontextu organizácie, rozsah, vedenie, plánovanie, podporu, praktickú aplikáciu princípov a procesov, hodnotenie výkonu a zlepšovanie celého ISMS. Grafické znázornenie jednotlivých častí zobrazuje Obrázok 1.



Obrázok 1 Životný cyklus systému riadenia informačnej bezpečnosti (ISMS)

Týmito požiadavkami norma stanovuje postupy pri zriaďovaní, implementácii, údržbe a neustálom zlepšovaní systému riadenia informačnej bezpečnosti v kontexte organizácie. Obsahuje požiadavky na hodnotenie a ošetrenie rizík informačnej bezpečnosti prispôsobené potrebám organizácie. Požiadavky uvedené v norme predstavujú generické

odporúčania, ktoré je možné využiť pre všetky organizácie bez ohľadu na typ, veľkosť alebo povahu organizácie. Normou ISO/IEC 27001 sa sleduje proces založený na riziku, ktorý vyžaduje aby organizácie prijali opatrenia na odhaľovanie bezpečnostných hrozieb, ktoré majú vplyv na ich informačné systémy. Na riešenie identifikovaných hrozieb ISO/IEC 27001 navrhuje rôzne kontroly zamerané na zmiernenie bezpečnostných rizík, ktorých aplikáciou sa dosiahne zabezpečenie ochrany pred útokmi. Doplňujúcou normou pre ISO/IEC 27001 sú normy ISO/IEC 27002 a ISO/IEC 27005.

ISO/IEC 27002 [8] je medzinárodná norma, ktorá poskytuje návod na organizovanie informačnej bezpečnosti a skúsenosti na riadenie informačnej bezpečnosti vrátane výberu, zavedenia a riadenia opatrení, ktoré je potrebné zohľadniť v organizácii v prostredí bezpečnostných rizík. Táto medzinárodná norma je vytvorená pre organizácie, ktoré majú záujem o výber opatrení v rámci procesov zavedenia ISMS podľa normy ISO/IEC 27001. Alebo o zavedenie všeobecných platných opatrení informačnej bezpečnosti či vytvorenie vlastných návodov na riadenie informačnej bezpečnosti.

ISO/IEC 27005 [9] je medzinárodná norma, ktorá poskytuje usmernenia na vytvorenie systematického prístupu k riadeniu rizík informačnej bezpečnosti, ktorý je potrebný na identifikáciu organizačných potrieb týkajúcich sa požiadaviek informačnej bezpečnosti a na vytvorenie efektívneho systému riadenia informačnej bezpečnosti. Okrem toho táto norma podporuje koncepty ISO/IEC 27001 a je navrhnutá tak, aby pomáhala efektívnej implementácii informačnej bezpečnosti založenej na prístupe riadenia rizík.

Ako už bolo spomenuté, ISMS má za cieľ zabezpečiť kontinuitu podnikania a minimalizovať riziká, ako aj zabezpečiť IT aktíva a eliminovať ich možnú stratu, poškodenie alebo nedostupnosť tým, že:

- je definovaný kontext organizácie, za účelom pochopenia organizácie,
- sú definované a ohodnotené IT aktíva, ktoré je nutné chrániť,
- sú definované, riadené a hodnotené možné riziká informačnej bezpečnosti,
- sú definované a zavedené opatrenia s požadovanou úrovňou znižovania rizík,
- sú nastavené a vykonávané pravidelné kontroly na zlepšenie.

ISMS môže byť implementovaný pre organizačnú zložku spoločnosti, informačný systém (IS) alebo jeho časť, prípadne pre celú organizáciu v plnom rozsahu pokrytia jej zamerania a poskytovaných služieb. Zavedenie ISMS je strategické rozhodnutie vedenia

spoločnosti. Systém riadenia informačnej bezpečnosti je odporúčané využívať vo všetkých organizáciách bez ohľadu na ich veľkosť či odbor činností, pre ktoré sú informácie a informačné technológie kľúčovou súčasťou podnikateľských procesov, alebo ktoré spravujú citlivé dáta svojich klientov a majú potrebu efektívne a komplexne zaistiť ich bezpečnosť.

Zavádzanie a udržiavanie ISMS v organizácií je nepretržitý a opakujúci sa proces. Prináša so sebou viacero krokov, ktoré je potrebné dodržiavať a neustále zlepšovať pre zabezpečenie primeranej úrovne bezpečnosti a súladu so štandardom ISO/IEC 27001.

Norma zahŕňa návrhy na dokumentáciu, interné audity, neustále zlepšovanie, nápravné a preventívne opatrenia. Na úspešné implementovanie štandardu ISO/IEC 27001 organizácia vyžaduje ISMS, ktorý identifikuje aktíva organizácie a poskytuje nasledujúce hodnotenie:

- hodnotenie rizík, ktorým čelia IT aktíva,
- kroky podniknuté na ochranu informačných aktív,
- akčný plán v prípade narušenia bezpečnosti,
- identifikáciu osôb zodpovedných za každý krok procesu informačnej bezpečnosti.

1.1.1 Vytváranie kontextu organizácie, určovanie rozsahu ISMS a jeho podpora

Obsahom tejto podkapitoly sú časti 1-5 štandardu ISO/IEC 27001 ISMS, ktoré sú znázornené na Obrázok 1. Ako prvý krok procesu riadenia informačnej bezpečnosti alebo auditovania je uvedomenie si kontextu organizácie za účelom získať o danej organizácii dostatok informácií pre nasledujúce podprocesy ISMS. To znamená určiť účel a rozsah pôsobnosti organizácie, zistiť obchodný zámer, popísať obchodné procesy, oboznámiť sa s politikami spoločnosti, dokumentovať organizačnú štruktúru a identifikovať zodpovednosti za účelom presnej charakteristiky danej organizácie. Identifikácia týchto informácií môže prebiehať viacerými spôsobmi, avšak ako je uvádzané vo viacerých zdrojoch [10][11], táto identifikácia podlieha nutnosti osobného stretnutia. Rovnako je uvádzané, že tento proces je vykonávaný manuálne s využitím rôznych textových a tabuľkových procesorov, čo podlieha časovej náročnosti a neefektívnosti.

Digitalizáciu a čiastočnú automatizáciou tohto podprocesu sme definovali vo vytvorení preddefinovaného vetviaceho sa dotazníka, ktorý by pozostával z generických otázok na identifikáciu organizácie a zozbieranie vyššie spomínaných informácií na základe štandardu ISO/IEC 27001. Na popis organizačnej štruktúry a vzťahu jednotlivých oddelení by slúžil preddefinovaný model organizačnej štruktúry, ktorý by organizácia upravila podľa vlastných požiadaviek, k jej reálnemu obrazu. Digitalizácia tohto procesu by mohla byť poskytovaná v rámci komplexnejšieho informačného systému (IS), ktorý by pokrýval celý proces ISMS. V organizačnej štruktúre by bolo možné prideliť IP adresné rozsahy pre jednotlivé oddelenia, čo by malo za následok prepojenie ďalšieho kroku, a to identifikáciu IT aktív a ich prepojenie k organizačnej štruktúre, oddeleniu a konkrétnemu vlastníkovi. Riešenie automatizácie tohto podprocesu bližšie popisujeme v kapitole 3.1

1.1.2 Identifikácia a ohodnocovanie informačných aktív

Táto podkapitola popisuje podproces identifikácie rizík v rámci riadenia rizík, čo je obsahom štandardu ISO/IEC 27005, ktorý je popísaný v kapitole 1.2, avšak v tomto podprocese existuje prekryv aj s ISMS v časti prevádzkovanie. Po vytvorení kontextu organizácie je teda ďalším krokom identifikácia, kategorizácia a vytvorenie zoznamu IT aktív, ktoré je potrebné chrániť a zabezpečiť ich informačnú bezpečnosť. Tento podproces je možné vykonávať viacerými spôsobmi. Ako je uvádzané v rôznych odporúčaniach a štandardoch [12][13][9], alebo prípadne zákonoch [14], identifikácia IT aktív je vo väčšine prípadov vykonávaná manuálne, pomocou brainstormingu o IT aktívach, ktoré sa využívajú v každodenných podnikových procesoch. Keďže v súčasnosti neexistujú nástroje priamo určené pre zber IT aktív za účelom informačnej bezpečnosti, pre čiastočnú automatizáciu je možné využiť niektoré existujúce softvérové nástroje, ktoré však nie sú primárne určené pre proces získavania IT aktív zo siete za účelom informačnej bezpečnosti. Možností identifikácie IT aktív je v dnešnej dobe viacero [15][16][17]. Z hľadiska využitia IT prostriedkov existujú v súčasnosti viaceré softvérové nástroje, ktoré dokážu na rôznej úrovni preskúmať komunikačnú sieť a identifikovať IT aktíva ako napríklad inštalovaný softvér, dostupný hardvér a s nimi súvisiace detailné informácie. Analýzou dostupných riešení [18][19][20] sme zistili, že ich primárne zameranie je správa majetku, čomu sa venuje štandard ISO/IEC 19770-1 [21]. Dostupné nástroje vytvárajú inventár majetku, ale nie za účelom identifikácie IT aktív, ktorý by bol priamo využiteľný z pohľadu aplikácie procesov ISMS. Všetky analyzované nástroje sú prevažne založené na agentovom prístupe, čo obmedzuje možnosti ich použitia a zvyšuje náročnosť

implementácie. Nevýhodou týchto riešení je, že o IT aktívach uchovávajú príliš detailné informácie, ktoré nepredstavujú vstupy do ďalších podprocesov ISMS. Pri analýze dostupných riešení pre automatizovaný zber IT aktív sme nenatrafili na žiadne relevantné riešenia, ba ani štúdie, ktoré by popisovali vhodný systematický prístup k riešeniu automatizácie tohto procesu [17]. Väčšina štúdií týkajúca sa automatizácie informačnej bezpečnosti sa zameriava na identifikáciu hrozieb a proces hodnotenia rizík. V súčasnosti však vnímame potrebu venovať sa problematike riadenia informačnej bezpečnosti v širšom zmysle, a to od jej základov. Celý proces riadenia informačnej bezpečnosti, ako aj riadenia rizík sa odvíja od správne a presne identifikovaných IT aktív [15]. Potrebu systematického prístupu k automatickej identifikácií IT aktív, ktoré majú byť chránené preto vnímame ako prvý krok k úspešnosti riešenia ISMS, prípadne auditovaniu IT systému. Zoznam IT aktív by mal obsahovať informácie, ktoré predstavujú relevantné vstupy do ďalších podprocesov riadenia informačnej bezpečnosti, a teda všetok hardvér, softvér, služby, časti infraštruktúry, aplikácie podporujúce biznis procesy ale aj netechnické údaje ako napríklad spracovávané informácie, personál, procesy a podobne. Nami identifikované informácie vstupujúce do ďalších podprocesov ISMS sú preto popísané v kapitole 3.3.1.

Na základe vykonanej analýzy môžeme povedať, že vytváranie zoznamu IT aktív, či už manuálne alebo s využitím agentovo-orientovaných inventarizačných nástrojov je časovo náročné a jeho efektivita podlieha potrebe zmeny infraštruktúry pri jeho implementácii ako aj potrebe disponovať vhodným technickým personálom. Výrazne jednoduchší sa nám javí prístup založený na bez agentovom systéme. Bez agentový prístup nepožaduje aplikáciu agentov do každého IT prvku infraštruktúry, čo zjednodušuje jeho nasadenie. Z hľadiska experimentov vykonaných v súvislosti s overovaním navrhovaných algoritmov by riešenie mohlo využívať dostupné nástroje s otvoreným kódom zamerané na skenovanie siete. Ich využitie popisujeme v kapitole 3.4 zameranej na popis navrhovaných algoritmov. Funkcie skenovacích nástrojov sú v algoritmoch doplnené o dodatočné získavanie ďalších informácii s využitím sieťových protokolov, ako napríklad Simple Network Management Protocol (SNMP), Secure Shell (SSH), Telnet alebo prípadne Windows Management Instrumentation (WMI). V návrhoch algoritmov zberu aktív tak predpokladáme aj situácie, kedy organizácie môžu mať implementované základné sieťové protokoly, ktoré sú využívané na vzdialený manažment, prípadne monitorovanie sieťových alebo koncových zariadení.

Po zbere, identifikácii, kategorizácii a vytvorení hierarchického zoznamu IT aktív organizácie je nevyhnutné ich ohodnotenie. Ohodnotenie aktív je kľúčovým krokom pre zabezpečenie objektívneho, opakovateľného a logicky správneho zabezpečenia procesu analýzy rizík. Tento proces je kritický v zmysle riadenia bezpečnosti a plánovania nákladov, aby organizácia bola schopná zabezpečiť požadovanú úroveň bezpečnosti a využila na to vhodné prostriedky. Ohodnocovanie aktív je proces závislý na subjektívnom pohľade danej organizácie na hodnotu svojich IT aktív. Z tohto dôvodu nie je možné proces dostatočne zovšeobecniť a následne plne automatizovať tak, aby vyhovoval rôznym organizáciám súčasne. Vylepšenie manuálnych činností procesu však vidíme vo vykonanom návrhu hierarchického modelu skladu a rozkladu IT aktív, ktorý by mohol byť využitý v procese ohodnocovania a môže byť predmetom návrhu a realizácie IS. Keďže z viacerých štúdií vyplýva [22][23][24], že závislosť IT aktív medzi sebou má vplyv na výslednú hodnotu aktíva, považujeme za prínosné na určovanie hodnoty IT aktív využiť práve nami navrhovaný hierarchický model skladu a rozkladu. Navrhovaný model skladu a rozkladu IT aktív je možné využiť pri navrhovanej metóde ohodnocovania IT aktív, a teda pri dedení hodnoty aktíva z primárneho na sekundárne. Tým by sa odbremenila časová náročnosť a manuálna potreba ohodnocovať všetky identifikované IT aktíva *(primárne aj sekundárne)* iba na kategóriu primárnych aktív. Bližší popis navrhovaného ohodnocovania IT aktív popisujeme v kapitole 3.7. Ako je uvádzané v [25], nie je veľa štúdií zaoberajúcich sa metódami ohodnocovania IT aktív pre proces informačnej bezpečnosti. Článok [22] uvádza niektoré štúdie, ktoré popisujú model ohodnocovania IT aktív založený na aspektoch bezpečnosti informačného systému a úrovne závažnosti rizík na stupnici jedna až tri, pričom hodnoty následne znamenajú kritickosť aktíva ako 1 – mierne, 2 – významné, 3 – závažné. Iné štúdie [26] udávajú hodnotu IT aktívam z pohľadu dopadu na dôvernosť, integritu a dostupnosť ako aj s ohľadom na peňažnú hodnotu potrebnú na obnovenie týchto troch aspektov. Ohodnocovanie IT aktív nie je jednoduchá úloha a proces je obzvlášť zložitejší ak sa aktívum ohodnocuje s ohľadom na nehmotné aspekty, ako napríklad povesť organizácie, právne či prevádzkové dopady a podobne. Pre potreby informačnej bezpečnosti sú práve informácie najdôležitejšími aktívami. Bez informácií nie je možné spoľahlivo vykonať ohodnotenie IT aktív. Aby sme sa vyhli neúplnému ohodnocovaniu aktív zameranému len na technické aspekty informačnej bezpečnosti, je potrebné vziať do úvahy aj sociálne, právne a netechnické aspekty. Ako popisuje štúdia [25], je vhodné pristupovať

k ohodnocovaniu IT aktív na základe kategórií a primárnosti aktív, a teda od informácií, cez softvér až po hardvérové aktíva. S využitím hierarchického modelu, ktorý rozdeľuje aktíva na hardvér, softvér, informácie a prípadne procesy, je možné zamedziť prípadným problémom pri nesprávnom určovaní hodnôt jednotlivým IT aktívam a skĺznuť tak iba do ich posudzovania len z technického pohľadu. Na základe analýzy dostupných metód [27][26][28][29][22] sme navrhli vlastný spôsob ohodnocovania IT aktív. Nami vypracovaná metóda navrhuje pristupovať k určovaniu hodnoty IT aktívam s využitím hierarchického modelu (viď. Obrázok 28) a so zohľadnením dopadov na tri základné aspekty informačnej bezpečnosti, a to dôvernosť, integritu a dostupnosť. Jednotlivé hodnoty pre aspekty CIA sa určujú s ohľadom na reputačné, prevádzkové, právne, finančné a ľudské dopady. Pridaním viacerých aspektov do výsledného výpočtu hodnoty rizika, na základe, ktorých sa určujú hodnoty pre dôvernosť, integritu a dostupnosť sa odstráni subjektívny pohľad pri výbere jednotlivých hodnôt a zváži sa dopady s ohľadom na širšie spektrum, a to reputačné prevádzkové, finančné, právne a ľudské. Presný popis metódy pre výpočet hodnoty aktíva uvádzame v kapitole 3.7. Výsledkom prepracovaného druhého podprocesu celého ISMS je zoznam identifikovaných a ohodnotených IT aktív s využitím novej hodnotiacej metódy.

1.1.3 Analýza rizík informačnej bezpečnosti

Ďalším, v poradí tretím podprocesom ISMS je identifikácia zraniteľností, hrozieb a hodnotenie rizík IT aktív. V tomto podprocese je potrebné identifikovať zraniteľnosti definovaných IT aktív a hrozby, ktoré pôsobia na tieto zraniteľnosti a môžu ich využiť. Proces identifikácie zraniteľností a hrozieb prebieha na základe brainstormingu s podporou noriem a štandardov, ktoré popisujú niektoré generické zraniteľnosti a hrozby, ktoré sú prípadne doplnené o vedomosti a skúsenosti bezpečnostného manažéra alebo audítora. Pri hodnotení rizík sa riziká identifikujú, analyzujú a vyhodnocujú. Riadeniu rizík informačnej bezpečnosti sa podrobnejšie venuje norma ISO/IEC 27005, ktorá je bližšie popísaná v kapitole 1.2. Výstupom tohto podprocesu sú zdokumentované a vyhodnotené riziká v zozname rizík vrátane hrozieb, zraniteľností a vlastníkov rizík namapovaných na konkrétne IT aktíva. Pri hodnotení rizík sa zohľadňujú dôsledky a dopady na poskytované služby a kontinuitu podnikania organizácie. Taktiež sa prihliada na pravdepodobnosť využitia zraniteľnosti a teda naplnenia hrozby. Výsledné hodnoty rizika sa porovnávajú s rizikovými kritériami, ktoré si organizácia definovala a následne sa pristupuje k spracovaniu rizík, čo je popísané v nasledujúcej kapitole.

1.1.4 Spracovanie rizík informačnej bezpečnosti

Predposledným podprocesom ISMS je spracovanie rizík informačnej bezpečnosti. Cieľom je definovať a zaviesť vhodné opatrenia pre prioritné riziká, pomocou ktorých je možné znížiť hodnotu celkového rizika pre vybrané IT aktívum. Kroky analýza rizík, ako aj riadenie rizík sú taktiež súčasťou normy ISO/IEC 27005, avšak tieto kroky sú súčasťou celého procesu riadenia informačnej bezpečnosti a ISMS ich popisuje v častiach 6 a 7 z Obrázok 1. V tomto kroku sa vypočítava zvyškové riziko na základe aplikácie navrhnutých opatrení, prípadne sa riziká akceptujú alebo presunú na iného vlastníka. Výstupom tohto podprocesu je zoznam vhodne vybraných opatrení a kontrol, ktoré sú namapované na konkrétne hrozby a zraniteľnosti za účelom znížiť alebo odstrániť riziko. V zozname je vhodné uviesť aj prostriedky potrebné pre implementáciu navrhovaného opatrenia alebo kontroly za účelom vhodného výberu navrhovaných opatrení. Pri výbere opatrení zameraných na zmiernenie rizika je potrebné zvážiť hodnotu IT aktíva a prostriedky alebo zdroje potrebné pre implementáciu opatrení na jeho zabezpečenie.

1.1.5 Monitorovanie, kontrola a zlepšovanie informačnej bezpečnosti

Posledný krok v procese riadenia informačnej bezpečnosti je udržiavanie a zlepšovanie aktuálneho stavu celého systému informačnej bezpečnosti. To znamená, že je potrebné definovať a implementovať kontroly zamerané na monitorovanie dodržiavania ISMS v celom jeho definovanom rozsahu, čomu sa venuje časť 8. Okrem toho je potrebné dokumentovať odporúčania a zmeny pre zlepšenie systému riadenia informačnej bezpečnosti v budúcnosti. Výstupom tohto podprocesu je zoznam potrebných kontrol a ich cieľov, plán spracovania rizík vrátane akceptovania zvyškových rizík, plán implementácie kontroly a požiadavky na zmeny v procese riadenia zmien informačnej bezpečnosti, ktoré sa používajú ako vstupy pre opätovný priebeh a zlepšovanie procesov ISMS. Ako už bolo spomenuté, ISMS je nepretržitý proces, ktorý je nevyhnutné neustále zlepšovať. Z tohto dôvodu je pri implementácii opatrení a navrhovaných zmenách alebo odporúčaniach potrebné vykonať všetky kroky ISMS odznova.

Implementáciou ISMS v organizácií je možné [30]:

Zabezpečiť informácie mnohými spôsobmi, vrátane použitia bezpečnostných kontrol, ktoré môžu pomôcť chrániť informácie pred neoprávneným prístupom, použitím, zverejnením alebo zničením. Bezpečnostné kontroly pomáhajú zabezpečiť, aby boli informácie presné a spoľahlivé a aby boli dostupné v prípade potreby.

Zlepšiť firemnú kultúru tým, že propaguje prostredie s ohľadom na bezpečnosť a poskytuje zamestnancom znalosti a nástroje potrebné na ochranu informačných aktív organizácie.

Vytvoriť centrálne riadený rámec organizácie zameraný na vytvorenie, implementáciu, prevádzku, monitorovanie, kontrolu a neustále zlepšovanie jej informačnej bezpečnosti.

Chrániť celú svoju organizáciu tým, že poskytuje rámec pre riadenie rizík bezpečnosti informácií. Zahŕňa zásady a postupy na identifikáciu, hodnotenie a riadenie rizík pre bezpečnosť informácií a na reakciu na incidenty a ich obnovu.

Reagovať na vyvíjajúce sa bezpečnostné hrozby implementáciou komplexného a proaktívneho prístupu k bezpečnosti, ktorý zahŕňa pravidelné hodnotenie rizík, vývoj bezpečnostných politík a postupov, implementáciu bezpečnostných kontrol a priebežné monitorovanie a podávanie správ. Implementáciou týchto krokov pomáha ISMS organizáciám držať krok s najvyššími bezpečnostnými hrozbami a zraniteľnými miestami a prijímať proaktívne opatrenia na ich predchádzanie alebo zmierňovanie.

Znížiť náklady spojené s bezpečnosťou informácií zavedením súboru štandardizovaných postupov a kontrol, ktoré možno použiť na riadenie a ochranu IT aktív. Vďaka centralizovanému a koordinovanému prístupu k informačnej bezpečnosti sa môžu organizácie vyhnúť duplicitnému úsiliu a plytvaniu zdrojmi. Okrem toho môže ISMS pomôcť organizáciám včas identifikovať potenciálne riziká a zraniteľné miesta, čo môže pomôcť predchádzať alebo zmierniť dopad bezpečnostných incidentov.

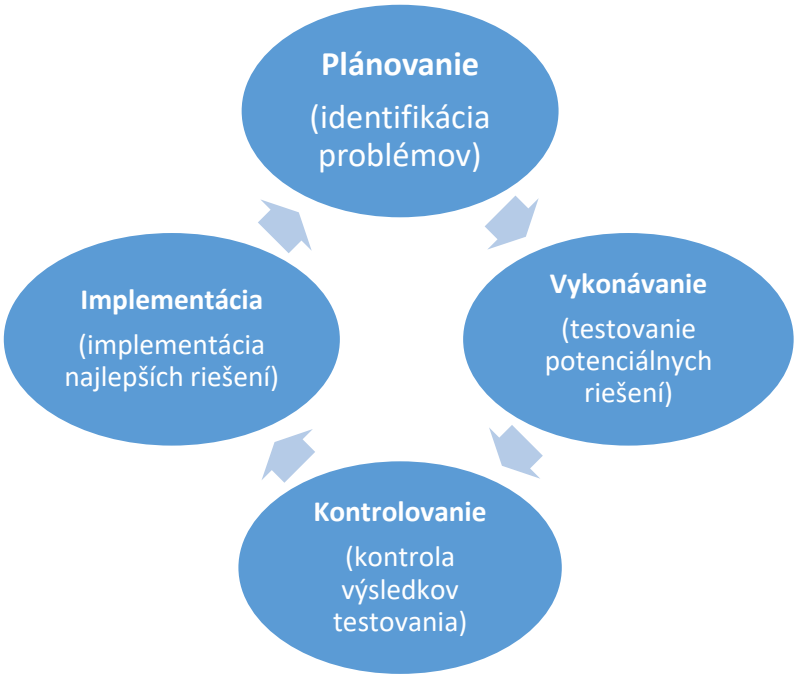
Chrániť dôvernosť, dostupnosť a integritu údajov implementáciou kontrol a procesov, ktorých cieľom je predchádzať incidentom informačnej bezpečnosti, zisťovať ich a reagovať na ne. Zavedené kontroly a procesy sa budú líšiť v závislosti od špecifických potrieb organizácie, ale môžu zahŕňať opatrenia na kontrolu prístupu, šifrovanie údajov a pravidelné monitorovanie a audit systémov a údajov.

Zvýšiť odolnosť voči kybernetickým útokom pomocou zvýšenia povedomia o potenciálnych hrozbách, implementáciou kontrol na zníženie pravdepodobnosti útokov a zavedením plánu rýchlej a efektívnej reakcie na útok, ak k nemu dôjde.

1.2 Riadenie rizík informačnej bezpečnosti (ISRM)

Riešením problémov ochrany IT aktív organizácie pred rizikami vyplývajúcimi z prevádzky IT je zavedenie ISMS, ktorý je prispôsobený individuálnym potrebám podniku a zahŕňa v sebe aj návrh procesov účinného riadenia informačných rizík. Existujú rôzne definície informačnej bezpečnosti, avšak je možné povedať, že bezpečnosť je udržiavanie akceptovateľnej miery identifikovaného rizika [31]. Bezpečnosť je teda komplex procesov a činností zameraných na odvrátenie alebo zmenšenie identifikovaných rizík, resp. prejavov hrozieb ktoré pôsobia na IT aktíva.

Ako bolo popásané v kapitole 1.1, riadenie rizík informačnej bezpečnosti (ISRM) je tretím, prípadne štvrtým podprocesom ISMS. Rovnako ako ISMS, aj riadenie rizík je nepretržitý, cyklický a kontinuálny proces, ktorý je možné znázorniť na Demingovom cykle (model PDCA) známom z normy ISO/IEC 27001.



Obrázok 2 Demingov cyklus model PDCA

Pre korektné uplatnenie metodiky riadenia informačného rizika sa IT riziko definuje ako: „*Riziko finančných a reputačných strát spôsobených narušením dôvernosti, integrity, dostupnosti alebo sledovateľnosti IT aktív, vytvorených, uložených, spracúvaných alebo prenášaných informačnými technológiami.*“

Prístup k manažmentu rizík na základe normy ISO/IEC 27001 podporuje osvojenie si procesného prístupu k návrhu, implementácii, prevádzke, monitorovaniu, udržiavaniu a zlepšovaniu efektivity ISMS. Najvhodnejšia metóda ošetrenia rizika by mala byť vybratá na základe výsledku hodnotenia rizika. Použitá by mala byť vždy tá metóda, ktorou je možné získať výraznejšiu redukciu rizika s dosiahnutím relatívne nižších nákladov. V zmysle normy ISO/IEC 27005 je možné na zmierňovanie rizík použiť protiopatrenia, ktoré je možné zradiť do jednej z možných kategórií, a to:

- zníženie rizika,
- presun rizika,
- vyhnutie sa riziku,
- zachovanie rizika.

Zníženie rizika je metóda ošetrenia rizika, pri ktorej je uplatnený výber vhodných opatrení, aby riziko bolo znížené až na úroveň zostatkového rizika, ktoré môže byť následne prehodnotené ako akceptovateľné. Výber opatrení by mal brať do úvahy kritéria akceptácie rizika ako napr. právne, regulačné, zmluvné požiadavky, ako aj primeranosť nákladov a časový rámec na implementáciu opatrení. Okrem toho, je dôležitá aj otázka návratnosti investície súvisiacej so znížením rizika a potenciál na využívanie nových obchodných príležitostí získaný implementáciou opatrení.

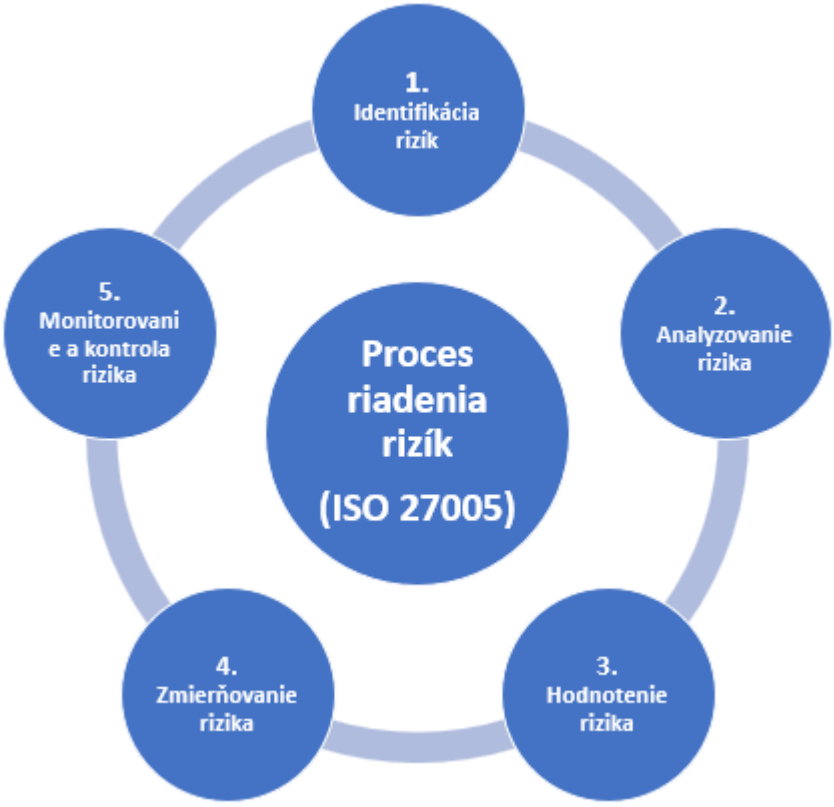
Presun rizika je metóda ošetrenia rizika, pri ktorej bude určitá časť rizika zdieľaná s externými subjektmi. Presun rizika môže byť uskutočnený napr. poistením alebo výberom zmluvného partnera, ktorý bude monitorovať vybraný proces, alebo informačný systém a prijímať okamžité opatrenia na zastavenie hrozby skôr, ako vznikne škoda.

Vyhnutie sa riziku je metóda ošetrenia rizika, pri ktorej bude riziko obídené nevykonaním príslušných rizikových aktivít, alebo uplatnením špecifických podmienok na vykonanie aktivity. V prípade, že je identifikované riziko vyhodnotené ako príliš vysoké, alebo náklady na implementáciu ošetrenia rizika presahujú prínosy, rozhodnutím môže byť aj úplne vyhnutie sa riziku, a to odobratím plánovanej alebo existujúcej aktivity (súboru aktivít), prípadne zmenou podmienok prevádzkovania danej činnosti.

Zachovanie rizika je metóda ošetrenia rizika, pri ktorej nie sú uplatnené žiadne opatrenia a riziko zostane zachované v pôvodne ohodnotenej úrovni. V prípade, že táto

úroveň spĺňa kritéria pre prijatie rizika, nie je potrebné implementovať opatrenia a riziko môže zostať zachované.

ISRM je nepretržitý proces analýzy toho, ako bude organizácia ovplyvnená rušivým incidentom a aké môžu byť dôsledky. To zahŕňa akýkoľvek scenár, v ktorom je ohrozená dôvernosť, integrita a dostupnosť údajov. Posúdenie rizík pomáha pri rozhodovaní o najlepšom spôsobe zníženia rizika na prijateľnú úroveň. Správne nastavenie tohto procesu je nevyhnutné, pretože celý ISMS je formovaný podľa reakcie na riziká. ISRM sa skladá z viacerých procesov, ktoré sú rozšírením jednotlivých podprocesov ISMS. Pre aplikovanie vhodných metód a protiopatrení pre ošetrenie rizika je potrebné riziko identifikovať. Pri identifikácii a zmierňovaní/ošetrovaní rizika je potrebné dodržať kroky, odporúčané štandardom ISO/IEC 27005.



Obrázok 3 Riadenie rizík podľa ISO/IEC 27005 – životný cyklus

Odporúčaný prístup ošetrovania/zmierňovania rizík sa skladá z:

Vytváranie kontextu: V tomto kroku sa detailne stanovuje a popisuje kontext organizácie. To znamená zdokumentovať pôsobenie organizácie, jej ciele a podnikový zámer. Ako ďalšie je tiež potrebné definovať rozsah a cieľ pre analýzu rizík, definovať

kritéria analýzy rizík a štruktúru prístupu k riadeniu rizík. Tento proces je totožný s prvým procesom ISMS, ako je uvádzané v kapitole 1.1.1.

Identifikácia a analýza rizík: Druhý krok predstavuje vývojovú fázu modelu rizika. Identifikovať IT aktíva a určiť či sa jedná o primárne alebo sekundárne (podporné) aktívum. ISO/IEC 27005 uvádza, že primárnymi aktívami sú informácie alebo obchodné procesy a podpornými aktívami sú súvisiace IT systémy, infraštruktúra a ľudské zdroje. Ako popisujeme v kapitole 1.1.2, tento proces je totožný s procesom identifikácie IT aktív a ich ohodnocovaním, čo popisuje norma ISO/IEC 27001. Našimi navrhovanými zlepšeniami a automatizáciu tohto procesu popisujeme v kapitole 3.2. Po identifikácii informačných aktív, ich prioritnom rozdelení na primárne a sekundárne, je potrebné identifikovať ich riziká. Identifikácia rizík zahŕňa identifikáciu hrozieb a slabých miest organizácie, ako aj existujúcich kontrol. Pri identifikácii hrozieb a slabých stránok je potrebné vychádzať práve z kontextu organizácie a jej pôsobenia. Na rozdiel od iných metodológii hodnotenia rizík, hodnotenie podľa ISO/IEC 27005 vyžaduje, aby organizácia identifikovala všetky svoje existujúce kontroly a zohľadnila ochranu poskytovanú týmito kontrolami pred aplikáciou akýchkoľvek nových.

V súčasnosti existujú normy alebo verejné katalógy hrozieb, ako napríklad ISO/IEC 27005, ENISA Threat Taxanomy, Bundesamt fur Sicherheit in der Informationstechnik (BSI) IT alebo NIST SP 800-30, ktoré uvádzajú zoznam hrozieb a zraniteľností, ktoré môžu slúžiť ako pomoc pri implementácií techník identifikácie rizík. Tento generický zoznam však nie je konečný a každá organizácia si musí doplniť do zoznamu svoje vlastné špecifické hrozby a zraniteľné miesta, ktoré ohrozujú dôvernosť, integritu a dostupnosť jej IT aktív. Na identifikáciu rizík existuje viacero metód [32], ako napríklad:

- analýza pomocou kontrolného zoznamu,
- brainstorming,
- Delphi metóda,
- What-if analýza,
- SWOT analýza,
- a ďalšie...

Analýzou metód pre identifikáciu rizík informačných aktív sme navrhli spôsob ako by bolo možné zjednodušiť proces identifikácie rizík, ktorý je popísaný v kapitole 3.8.1

ISO/IEC 27005, prípadne katalógy hrozieb stanovujú svoje odporúčania na zmierňovanie rizík organizáciám, aby zamerali svoje úsilie v reakcii na najväčšie hrozby, takže informácie, ktoré boli zhromaždené o IT aktívach, slabých miestach a hrozbách, by sa mali použiť na uprednostnenie najväčších rizík.

Hodnotenie a zmierňovanie rizík: Hodnotenie rizika zahŕňa stanovenie úrovne hrozieb a zraniteľných miest skúmaného typu kontextu danej organizácie. Existuje viacero metód pre výpočet rizika, avšak najbežnejší spôsob výpočtu popisuje nasledujúca rovnica:

$$\boldsymbol{R = p.i}$$

kde: $\boldsymbol{R}$ – riziko; $\boldsymbol{p}$ – pravdepodobnosť, že hrozba využije zraniteľnosť; $\boldsymbol{i}$ – celkový dopad zneužitej zraniteľnosti z pohľadu CIA.

Výsledkom takéhoto hodnotenia je matica hodnotenia rizika. Matica hodnotenia rizika poskytuje jednoduchý spôsob, ako rizikám určiť prioritu a kvantifikovať riziko pomocou jednoduchého bodovacieho systému.

Tabuľka 1 Matica hodnotenia rizika

Veľmi vysoké (4)	**4**	**8**	**12**	**16**
Vysoké (3)	**3**	**6**	**9**	**12**
Stredné (2)	**2**	**4**	**6**	**8**
Nízke (1)	**1**	**2**	**3**	**4**
	Nízke (1)	**Stredné (2)**	**Vysoké (3)**	**Veľmi vysoké (4)**

Matica je farebne odlíšená na základe série prahových hodnôt: 1-3, 4-6 atď. Organizácie môžu použiť tieto prahové hodnoty, aby im pomohli určiť úroveň rizika, ktoré sú ochotné prijať alebo naopak, prioritne riešiť ich zmierňovanie. V súčasnosti neexistuje žiadny univerzálny systém na určenie bodu, v ktorom sa pravdepodobnosť alebo poškodenie rizika pohybuje z jednej hodnoty na druhú. Organizácie sa o prahových hodnotách musia rozhodnúť na základe vlastného uváženia a svoje odôvodnenie zdokumentovať vo svojej metodike hodnotenia rizík.

Po výpočte úrovne rizika, ktorú predstavuje každá hrozba, je potrebné rozhodnúť, ako s danými rizikami bude organizácia zaobchádzať. Existujú štyri možnosti ako pristúpiť k zmierňovaniu rizík, ktoré sú popísané vyššie: zníženie rizika, presun rizika, vyhnutie sa riziku a zachovanie rizika.

Nami navrhovaná metóda výpočtu rizika berie do úvahy hodnotu IT aktíva, a teda celkový dopad na CIA z pohľadu ROLFP, pravdepodobnosť hrozby a významnosť zraniteľnosti. S využitím topologickej mapy pre vizualizáciu súvzťažností pre jednotlivé IT aktíva by bolo možné predikovať zmenu celkového rizika primárneho aktíva po implementácii vybraného opatrenia na zmiernenie hrozby, prípadne zraniteľnosti. Návrh výpočtu rizika pre jednotlivé aktíva, ako aj celkové riziko pre primárne aktívum a predikciu jeho zmeny bližšie popisujeme v kapitole 3.8.2.

Implementácia a monitorovanie: Posledným krokom je výber vhodných opatrení, ich implementácia pre zníženie identifikovaných rizík, kontrola a monitorovanie. Monitorovanie zahŕňa pravidelnú kontrolu hlavných zmien v kontexte analýzy rizík, ako aj akýchkoľvek väčších zmien mimo tohto kontextu, ktoré by znamenali prepracovanie iterácie analýzy.

Riadenie rizík a teda všeobecne súlad s normou ISO/IEC 27001 je nepretržitý proces z čoho vyplýva, že je potrebné pravidelne monitorovať a kontrolovať svoj plán riadenia. Pravidelné kontroly a monitorovanie systému umožňujú kontrolovať či zvolené možnosti zmierňovania fungujú podľa navrhnutého plánu. Je potrebné kontrolovať, či boli dosiahnuté požadované výsledky po implementácii vybraných opatrení, alebo či naopak dané opatrenie nerieši riziko podľa očakávaní a nie je vhodné. Monitorovanie a kontroly taktiež pomáhajú pri posudzovaní meniaceho sa prostredia hrozieb. V priebehu času sa môžu vyskytnúť nové riziká a existujúce sa naopak môžu zmeniť. Týmto je organizácia nútená prehodnocovať priority a prístup k celkovému riadeniu rizík.

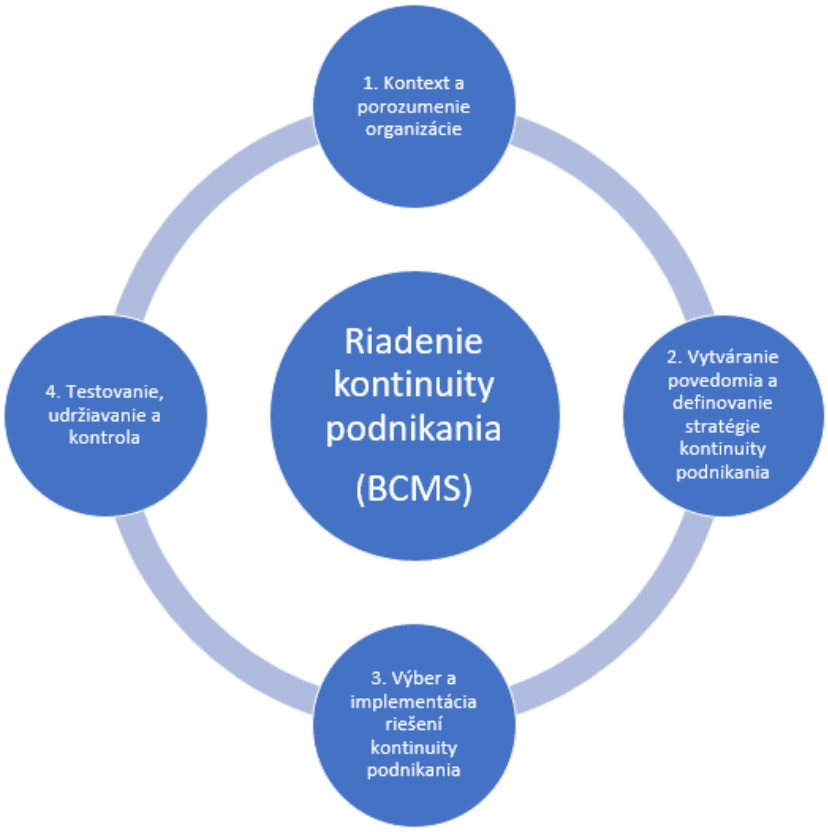
Pri procese monitorovania nasadených opatrení a ich kontrole, by bolo možné využiť už spomínanú topologickú mapu, ktorá by znázorňovala vzťahy medzi primárnymi a sekundárnymi aktívami a tým by bolo možné vizuálne odzrkadliť nasadené opatrenia a ich dopady na IT aktíva priamo v topologickej mape. Taktiež by ju bolo možné využiť v procese predikcie rizika, v prípade implementácie vybraných opatrení. Bližší popis navrhovaného riešenia a využitia topologickej mapy v procese monitorovania a kontroly je v kapitole 3.8.3.

1.3 Systém riadenia kontinuity podnikania (BCMS)

Súčasťou systému informačnej bezpečnosti je neodmysliteľne aj zabezpečenie kontinuity podnikania. V modernom prostredí je nevyhnutná kontinuita podnikania,

pričom kybernetické útoky pribúdajú a čoraz viac digitálnej pracovnej sily vytvára ďalší tlak na závislosti od technológií. Systém riadenia kontinuity podnikania (BCMS) je norma, ktorá je popísaná v ISO 22301 [33] a definuje postupy, ktoré pomáhajú organizáciám pripraviť sa na rušivé incidenty a zabezpečiť, aby rýchlo reagovali v prípade neočakávanej udalosti. Organizácie môžu riziká výpadku riešiť vytvorením BCMS, ktorý obsahuje usmernenia o tom, čo robiť v prípade rôznych prerušení a incidentov. Norma napomáha definovať postupy pomocou ktorých je možné vyrovnať sa s incidentmi, ktoré ovplyvňujú kritické obchodné procesy a aktivity, od zlyhania jedného servera až po úplnú stratu informácií, informačného systému alebo veľkého počtu zariadení.

BCMS predstavuje medzinárodnú normu, ktorá najlepšie popisuje postupy pre kontinuitu podnikania a uvádza, že existujú štyri hlavné komponenty úspešného BCMS.



Obrázok 4 Systém riadenia kontinuity podnikania (BCMS) životný cyklus

Prvou zložkou BCMS je hľadanie podpory manažmentu. Organizácia si musí byť vedomá potreby zabezpečiť kontinuitu podnikania a z toho dôvodu je nutné aby BCMS bol podporovaný vedúcimi zamestnancami pre dosiahnutie jeho efektívnosti. Podporou BCMS sa zabezpečí, že organizácia dostane potrebné zdroje pre implementáciu jednotlivých

postupov a BCMS bude podporované v rámci celej organizácie. Taktiež je potrebné poznať ciele organizácie a jej celkový kontext a pôsobenie na trhu.

Druhý krok pri riadení kontinuity podnikania je vykonanie analýzy vplyvu na podnikanie. Analýzou je potrebné identifikovať kritické aktivity a závislosti organizácie, ktoré určujú jej priority pre obnovu po prerušení alebo obmedzení jej prevádzky počas a po incidente. Veľká časť analýzy zisťuje a definuje, ako rýchlo po incidente je potrebné obnoviť jednotlivé činnosti a kompromitovanú prevádzku organizácie.

Treťou zložkou je vykonanie hodnotenie a identifikácia rizík. V tomto kroku je pre organizáciu potrebné identifikovať a definovať všetky riziká, ktoré môžu negatívne ovplyvniť kontinuitu kritických aktivít a závislostí organizácie. Hodnotenie rizika teda napomáha organizáciám určiť:

- špecifické scenáre, ktoré môžu ovplyvniť každú obchodnú činnosť,
- určiť pravdepodobnosť, že identifikované scenáre nastanú,
- definovať závažnosť poškodení pri každom zo scenárov.

Výsledkom hodnotenia rizík pre zabezpečenie kontinuity podnikania je zoznam všetkých identifikovaných negatívnych scenárov, rizík a ich ohodnotenie. Na ohodnotenie rizík je možné použiť číselnú stupnicu. Priradením čísla každej úrovni pravdepodobnosti a závažnosti môžu organizácie vytvoriť tzv. skóre rizika pre každú hrozbu. Na základe stanovenia si prahových hodnôt akceptácie rizika, sa organizácia ďalej rozhoduje o plánovaní implementácii nápravných opatrení. Pre všetky riziká, ktoré presahujú prahovú hodnotu akceptácie rizika bude potrebné naplánovať ich zmiernenie. Riziká, ktorých skóre je pod prahovou hodnotou rizika je možné ignorovať s odôvodnením, že daný scenár pravdepodobne nenastane a/alebo nespôsobí významné škody.

Štvrtým komponentom je vytvorenie plánu kontinuity podnikania (BCP), testovanie a udržiavanie implementovaných opatrení a udržiavanie aktuálneho BCMS. BCP je dokument, ktorý spája všetky tri predchádzajúce zložky. Plán kontinuity podnikania podrobne popisuje scenáre obnovy, na ktoré sa musí organizácia pripraviť a ako na nich bude reagovať v prípade vzniknutia incidentu. Cieľom BCP je definovať presné kroky postupy na stabilizovanie vzniknutej neočakávanej situácie a umožniť organizácii pokračovať v prevádzke čo najefektívnejšie, kým sa situácia úplne nevyrieši.

Implementácia BCMS zahŕňa vývoj plánov kontinuity podnikania, berúc do úvahy organizačné nepredvídané udalosti a schopnosti, ako aj individuálne obchodné potreby organizácie. Zameranie dizertačnej práce je z pohľadu zabezpečenia kontinuity podnikania iná oblasť riešeného problému. Aj na základe toho si myslíme, že nami navrhovaný centralizovaný systém by bolo možné využiť aj pri vytváraní plánov kontinuity podnikania a obnovovacích scenárov doplnením otázok do vetviaceho sa dotazníka ohľadom analýzy vplyvu na podnikanie. Práve s využitím navrhovanej topologickej mapy a vytváraním komunikačnej cesty by bolo možné identifikovať možné nežiadúce scenáre, ktoré môžu nastať v infraštruktúre organizácie, čím by systém predstavoval podklady pre návrh vhodných plánov obnovy, prípadne určenie a zabezpečenie procesov pre udržanie kontinuity. Podobne by bolo možné využiť organizačnú štruktúru pre popis zodpovedností a vytvorenie komunikačnej matice.

Výstupom BCMS sú presne zdokumentované kroky a postupy pre každý aspekt kontinuity podnikania. Je potrebné zabezpečiť testovanie plánov kontinuity a testovanie ich aplikovateľnosti v neustále sa meniacom a vyvíjajúcom sa prostredí hrozieb. Je tiež potrebné osvojiť si štruktúrovaný prístup k BCMS a k jeho implementácii. To znamená komunikáciu so zamestnancami organizácie, aby sa zabezpečila konzistentnosť v rámci celej organizácie čím sa zabezpečí, že postupy sú relevantné, dodržiavané a zamestnanci poznajú svoje povinnosti s ohľadom na bezpečnosť a kontinuitu podnikania.

1.4 Audit – kontrola bezpečnosti a integrity systému

Nastavením štruktúrovaného a dokumentovaného systému riadenia informačnej bezpečnosti, ako aj systému riadenia rizík, prípadne zabezpečením kontinuity podnikania sa kybernetická a informačná bezpečnosť nekončí. Kybernetická, rovnako ako aj informačná bezpečnosť sú cyklické nepretržité procesy, ktoré je potrebné neustále udržiavať a vylepšovať. Certifikáciou voči vyššie spomínaným normám sa organizácia preukazuje a zaväzuje dodržiavať požadované implementované postupy informačnej bezpečnosti. Na posúdenie súladu a zhody voči týmto normám sú organizácie nútene podliehať auditu. Rovnako ako pri problematike BCMS, ani audit nie je primárnym zameraním tejto dizertačnej práce, avšak navrhovaný IS je možné využiť ako podklad pre audítora pri vykonávaní auditu. Audit informačnej bezpečnosti by mal zahŕňať preskúmanie všetkých oblastí informačnej bezpečnosti, alebo aspoň minimálne rozsah, ktorý je definovaný pri tvorbe auditného plánu. Audit môže prebiehať formou diskusie

s oprávnenými osobami, preskúmaním konzultovaných opatrení a postupov, preskúmaním dokumentácie a záznamov a podobne.

Audit, rovnako ako aj riadenie rizík informačnej bezpečnosti, sú procesy v ktorých je potrebné prezradiť a odhaliť všetky stratégie a ciele organizácie, silné aj slabé stránky, zraniteľné miesta a využívané informačné systémy v celej organizácii. Všetky získané informácie vstupujú do celého procesu auditu. Slúžia na posúdenie a preskúmanie procesov organizácie, informácií, dát a taktiež bezpečnosti, udržaní si náskoku pred internými hrozbami, narušeniami bezpečnosti a ďalšími kybernetickými útokmi, ktoré môžu pre organizáciu znamenať nepriaznivý vplyv na reputáciu, právne povinnosti, operatívu, ľudské zdroje alebo financie. Existujú dva prístupy ako môže prebiehať bezpečnostný audit so zámerom na informačnú bezpečnosť:

Interný audit: Vykonáva ho interný pracovník spoločnosti. Vo väčších organizáciách to môže byť vyčlenený pracovník, ktorý je certifikovaný ako audítor informačných systémov a disponuje dostatočnými vedomosťami. Interný audit môže vykonávať aj senior IT manažér, ktorého úlohou je vytvárať rozsiahle audítorské správy, tzv. reporty, ktoré slúžia riadiacim pracovníkom a externým pracovníkom zodpovedným za bezpečnosť.

Externý audit: Externý audit je vykonávaný externým pracovníkom, ktorý môže byť zamestnancom audítorskej spoločnosti alebo pochádza zo štátnych orgánov. Externí audítori sa najímajú, ak to vyžadujú určité rámce súladu, alebo ak organizácia nemá dostatok ľudských zdrojov a špecialistov na vykonanie interného auditu.

Okrem členenia auditu z pohľadu jeho vykonávania na interný a externý, ešte existuje aj delenie podľa druhu auditu, ako napríklad [34]:

Finančný audit: preveruje správnosť finančných výkazov organizácie.

Audit kvality: spravidla sa vykonáva podľa niektorej z noriem ISO a preveruje sa systém riadenia kvality v organizácii na základe vopred stanovených kritérií.

Bezpečnostný audit: nezávislí od štandardov (napr. ISO) alebo legislatívy (napr. zákon o KB). Preveruje sa systém riadenia bezpečnosti v organizácii.

Certifikačný audit: vykonáva sa podľa požiadaviek zákazníka alebo v rozsahu definovanom štandardom informačnej bezpečnosti ISO/IEC 27001 ISMS.

Procesný audit: preveruje jednotlivé procesy v organizácii.

IT audit: audit informačného systému preveruje a posudzuje hardvér, softvér, informácie, prevádzkovú dokumentáciu systému a bezpečnosť daného systému.

Audit IT bezpečnosti sa skladá z viacerých podprocesov, ktoré sú podobné jednotlivým podprocesom systému riadenia informačnej bezpečnosti. Spravidla bez ohľadu na druh auditu je odporúčané [35][36][37], aby sa vykonával najmenej raz alebo dvakrát ročne. Môže sa však vykonávať aj mesačne alebo štvrťročne za účelom dosiahnutia včasnej identifikácie a odhalenia slabých stránok, zraniteľných miest podniku a ich eliminovanie. Aktuálnosť výsledkov z auditu je potrebné udržiavať z toho dôvodu, ako už bolo spomenuté, že audit sa využíva na preverenie skutočného stavu a slúži ako podklad pre rozhodovanie, prijímanie a vykonávanie zmien a implementáciu protiopatrení.

Obrázok 5 Audit – životný cyklus

V prvom kroku auditu, procese získavania informácií je potrebné zhromaždiť a identifikovať všetky informačné aktíva skúmaného systému. To znamená identifikovať všetok hardvér, softvér, procesy, informácie, ľudské zdroje a bezpečnostnú dokumentáciu danej organizácie alebo skúmaného systému. Ako uvádza [14] audit je možné vykonávať metódami:

1. Vo vzájomnej súčinnosti audítora a organizácie na mieste alebo na diaľku (cez interaktívne komunikačné prostriedky):
   - Vykonaním rozhovorov manažmentom spoločnosti,
   - Doplnením kontrolných záznamov a dotazníkov za spoluúčasti manažmentu organizácie,
   - Vykonaním preskúmania objektu a jeho posúdenie za spoluúčasti manažmentu spoločnosti,
   - Vzorkovaním.
2. Bez osobnej vzájomnej súčinnosti audítora a organizácie na mieste alebo na diaľku:
   - Vykonaním preskúmania objektu a jeho posúdenia (napr. záznamy a analýza údajov),
   - Pozorovanie výkonu práce,
   - Vykonanie návštevy na mieste a doplnenie kontrolného zoznamu,
   - Vzorkovaním a analýzou údajov,
   - Posúdením predpisov a regulačných požiadaviek.

Druhý krok pozostáva z posúdenia zhody s vybranými normami voči ktorým sa vykonáva audit. V prípade auditu informačnej bezpečnosti je to posudzovanie súladu napr. voči norme ISO/IEC 27001. V tomto kroku audítor skúma existenciu dokumentácie, ktorá presne popisuje a dokumentuje dodržiavané postupy, technické vybavenie, zodpovednosti a nápravné opatrenia.

Ďalším krokom je identifikácia rizík a odhalenie slabých miest informačnej bezpečnosti. K identifikovaným IT aktívam je potrebné namapovať zraniteľnosti a hrozby, ktoré dané zraniteľnosti môžu využiť.

Štvrtý krok auditu je vytváranie auditnej správy, ktorá poskytuje výstup z auditu. Auditná správa obsahuje:

- počet súladov, čiastkových súladov a nesúladov s kritériami auditu vrátane efektívnosti implementovaných opatrení v plnení zamýšľaných bezpečnostných cieľov,
- identifikáciu rizík a primeranosť implementovaných opatrení na zvládanie rizík pre jednotlivé kritéria auditu,

- dosiahnutie cieľov auditu, pokrytie predmetu auditu a splnenie kritérií auditu,
- podobné zistenia z rôznych oblastí, ktoré sa auditovali, alebo zo spoločného auditu alebo z predchádzajúceho auditu za účelom identifikácie trendov,
- odporúčania a prípadne návrhy na zlepšenie za jednotlivé oblasti, ktoré boli relevantné pre audit.

Posledný krok je výber vhodných nápravných opatrení a ich implementácia. Organizácia na základe auditnej správy posúdi výber vhodných opatrení pre zvýšenie informačnej bezpečnosti. Pri výbere je potrebné vziať do úvahy dostupné zdroje (ľudské, technické, finančné), mieru rizika, čas na implementáciu a dopad na informačnú bezpečnosť.

Proces riadenia informačnej bezpečnosti ako aj bezpečnostný audit sa skladá z podobných procesov. Navrhované riešenia, pre vylepšenie a automatizáciu jednotlivých procesov pre implementáciu systému riadenia informačnej bezpečnosti je možné využiť práve aj v procese auditovania. S využitím centralizovaného systému pre ISMS, ktorý je popísaní v kapitole 4, by bolo možné zabezpečiť jednoduchší a plynulejší priebeh auditu. Audítor by bol z veľkej časti odbremenený od nadmernej manuálnej činnosti, a to hlavne v procese identifikácie IT aktív. Navrhovaným prístupom by sa z časti eliminovala potreba osobných skúseností audítora, a to poskytnutím zoznamu základných zraniteľností a hrozieb, ako aj opatrení pre ich zabezpečenie. Rovnako by bolo vhodné využiť topologickú mapu pre potreby dokazovania implementácie navrhovaných opatrení pre zníženie rizík. S navrhovaným prístupom výpočtu rizika by sa zabezpečil detailnejší pohľad na hodnotu rizika a dopad na CIA z pohľadu ROLFP čo by malo za následok objektívnejší prístup k výpočtom. S využitím topologickej mapy a výpočtu celkového rizika pre primárne aktívum by bolo možné predpovedať zmenu hodnoty rizika po implementácií vybraných opatrení pre konkrétne IT aktíva, ktoré tvoria celok primárneho aktíva.

2 Ciele práce

Čoraz viac organizácií v súčasnosti čelí potrebe systematicky a flexibilne riadiť informačnú bezpečnosť. Informačná bezpečnosť je úzko spojená s riadením informačných rizík, zabezpečením kontinuity podnikania a kontrolou súladu, čiže auditom. Všetky spomínané oblasti informačnej bezpečnosti majú z veľkej časti spoločné procesy. Svoju prácu sme predovšetkým zamerali na problematiku zlepšenia procesov potrebných pre systém riadenia informačnej bezpečnosti a auditu. Ako sme v úvode už spomínali, hlavným problémom procesu riadenia informačnej bezpečnosti organizácie je nárast rizík spôsobený digitalizáciou a transformáciou informácií a procesov do kybernetického priestoru. To prináša požiadavky na efektívnejšiu správu bezpečnosti, na častejšie a efektívnejšie vykonávanie kontrol informačnej bezpečnosti a auditov. Hlavným problémom na ich častejšie a efektívnejšie vykonávanie je veľký podiel manuálnych činností, ktoré sú časovo náročné a podliehajú skúsenostiam bezpečnostného manažéra alebo audítora.

Hlavným cieľom práce je tak návrh riešení automatizácie vybraných procesov ISMS, pôvodne vykonávaných manuálne s využitím navrhovaných algoritmov pre identifikáciu IT aktív a metód výpočtu hodnoty IT aktív, ako aj návrh možných simulácií pre proces predikcie zmeny rizika po implementácii nápravných opatrení. Navrhované algoritmy automatizovaného zberu IT aktív a metódy výpočtu hodnoty aktív môžu predstavovať vstupné požiadavky pre vytvorenie centralizovaného informačného systému riadenia informačnej bezpečnosti. Prínosom automatizácie v podobe navrhovaných algoritmov je zefektívnenie vykonávania procesu identifikácie IT aktív a kontroly ISMS, ako aj odbremenenie bezpečnostných manažérov a audítorov od repetitívnych manuálnych činností a technických zručností. Ďalší prínos vidíme v návrhu metódy pre výpočet hodnoty informačného aktíva na základe navrhovaného modelu skladania a rozkladania IT aktív, pomocou ktorého sa uľahčí proces ohodnocovania IT aktív. Návrh simulácií pre zmenu hodnoty rizika predstavuje prínos v neskorších fázach procesu ISMS, a teda riadení rizík, čím vieme optimalizovať výber vhodných opatrení na základe výsledkov simulácií.

Ako bolo zdôraznené v kapitole 1.1, možností na automatizáciu a zefektívnenie jednotlivých podprocesov ISMS je viacero. Z tohto dôvodu sme v rámci metodiky riešenia vykonali hlbšiu analýzu jednotlivých podprocesov ISMS s bližším zameraním sa na manuálne vykonávané činnosti a možnosti využitia automatizácie pri týchto činnostiach.

Zameriame sa na počiatočné činnosti riadenia informačnej bezpečnosti a teda, analýzu možností pre vytváranie kontextu organizácie a mapovanie IT aktív na ich vlastníkov. Taktiež sa zameriame na analýzu dostupných riešení pre proces automatickej identifikácie IT aktív, ktoré sú potrebné ako vstupy pre ďalšie podprocesy ISMS. Analyzujeme dostupné metódy identifikácie rizík a hrozieb pre IT aktíva a zameriame sa na možnosti ich automatizácie. Rovnako sa zameriame na automatizáciu výpočtov rizika pre IT aktíva, ako aj pre automatizáciu vhodných opatrení pre ich znižovanie.

Aby bolo možné porovnať spôsoby implementácie ISMS a vykonávanie auditu v súčasnosti a nami navrhovanými zlepšeniami a automatizovaným spôsobom, vykonali sme analýzu dostupnej literatúry a taktiež sme sa zúčastnili prednášok a konferencií, ktoré boli orientované na túto problematiku. Na základe získaných poznatkov sme pristúpili k riešeniu automatizácie ISMS od základov, a to návrhom vytvárania kontextu organizácie a automatickou identifikáciou IT aktív a ich hodnotenia.

Pri návrhu automatizácie zberu aktív je potrebné do riešenia zakomponovať dostupné sieťové protokoly, navrhnúť algoritmy a vykonať ich pilotnú implementáciu a overenie. Za týmto účelom v práci využívame riešenia s otvoreným zdrojovým kódom (napríklad tie, určené pre skenovanie siete), ktoré sú nevyhnutné pre správne fungovanie navrhovaného systému. Vytvorené návrhy pre automatizáciu jednotlivých podprocesov je potrebné porovnať s existujúcou metodikou za účelom návrhu ich zlepšenia. Ako finálny výstup je potrebné formulovať odporúčania na základe výsledkov porovnania pre správnu implementáciu navrhovaných postupov pre informačný systém, ktorý predstavuje centralizovaný systém riadenia informačnej bezpečnosti.

Jednotlivé čiastkové ciele sú teda nasledovné:

- na základe analýzy dostupnej literatúry a metodík pre jednotlivé podprocesy ISMS vykonať identifikáciu a popis možných zlepšení a ich automatizácie pre podprocesy ISMS,
- navrhnúť hierarchický model skladania a rozkladania IT aktív na základe ich primárnosti a sekundárnosti,
- navrhnúť zlepšenie procesu vytvárania kontextu organizácie digitalizovaným spôsobom,
- navrhnúť algoritmy pre automatizáciu podprocesu identifikácie IT aktív,
- navrhnúť metódu pre automatické ohodnocovanie IT aktív,

- navrhnúť dátový model, na základe hierarchického modelu, pomocou ktorého by bolo možné vytvárať komunikačnú trasu a vizualizovať vzťahy medzi primárnymi a sekundárnymi aktívami,
- navrhnúť metódy pre vytváranie simulácií za účelom predikcie zmeny rizika,
- porovnanie odporúčaní s existujúcimi riešeniami.

3 Automatizácia procesov ISMS a ISRM

Keďže jedným z cieľov práce bolo navrhnúť metodiku pre postup implementácie systému riadenia informačnej bezpečnosti a auditu ISMS so zameraním sa na automatizáciu jeho podprocesov, v kapitole 1.1 sme popísali niektoré z možností ich automatizácie.

Aby bolo možné vytvoriť metodiku a navrhnúť nový prístup k automatizovanej implementácii a udržiavaniu ISMS, bola vykonaná analýza jednotlivých krokov spojených s implementáciou ISMS. Na základe zistení vykonávania jednotlivých krokov, popísaných v kapitole 1, identifikujeme možné oblasti pre ich automatizáciu. Z výsledkov analýzy jednotlivých procesov ISMS, nám vyplynuli možné riešenia pre zlepšenie a zjednodušenie niektorých identifikovaných podprocesov, ktoré boli publikované v [38]. Navrhnutím vhodných algoritmov pre potreby získavania relevantných informácií zo siete automatizovaným spôsobom, prípadne digitalizáciou niektorých krokov ISMS by bolo možné z veľkej časti automatizovať viaceré podprocesy riadenia informačnej bezpečnosti. Po analýze jednotlivých procesov ISMS a dostupných riešení, popísaných v kapitole 3.2, sme dospeli k záveru, že v súčasnosti chýba automatizovaný systém, ktorý by automatizovane riešil jednotlivé podprocesy ISMS, prípadne centralizovaný informačný systém, ktorý by riešil celý životný cyklus implementácie ISMS automatizovaným spôsobom, ktorý by odbremenil bezpečnostných manažérov a audítorov od prílišnej manuálnej činnosti, časovej náročnosti a subjektívneho rozhodovania.

Keďže z analýzy vyplynulo, že neexistujú vhodné riešenia pre počiatočné procesy ISMS, zamerali sme sa na návrh zlepšení pre procesy zamerané na vytváranie kontextu organizácie a identifikáciu IT aktív automatizovaným spôsobom, ako aj ich mapovanie k jednotlivým vlastníkom na základe vytvárania organizačnej štruktúry. Bližšie sa tejto téme venujeme v kapitole 3.1. Hlavným prínosom predkladanej práce je návrh algoritmov pre automatizáciu procesu identifikácie IT aktív s ich následným hodnotením. Zameriavame sa na návrh vhodných prístupov skenovania siete za účelom získať potrebné informácie do ďalších podprocesov ISMS, ako aj návrhu dátového modelu pre ukladanie týchto údajov čomu je venovaná kapitola 3.2. Následne sa v práci zameriavame aj na možné zlepšenia pre ďalšie podprocesy ISMS, ako identifikácia rizík, výpočet rizika a predikcia zmeny rizika automatizovaným spôsobom. Navrhované prístupy sú bližšie spracované v kapitole 3.8.

3.1 Vytváranie kontextu organizácie

Ako už bolo v kapitole 1.1.1 spomenuté, vytváranie kontextu organizácie je prvý krok pri implementácií ISMS, ako aj ISRM alebo auditu. Pre splnenie tohto kroku je potrebné zvolať úvodné stretnutie so všetkými zainteresovanými stranami. Zainteresované strany sú audítori, biznis vlastníci, manažment organizácie a všetok administratívny personál, ktorý je zapojený do procesov ISMS alebo auditu. Výstupom úvodného stretnutia by mala byť správa popisujúca organizáciu za účelom jej identifikácie, či už z pohľadu ISMS alebo auditu. Správa by mala obsahovať:

- **všeobecné úvahy:** účel a rozsah ISMS, ISRM a auditu, príprava plánov kontinuity a plány reakcie na incidenty, dodržiavanie právnych predpisov, a podobne,
- **prístup k riadeniu rizika**: poskytovanie zdrojov, politiky a postupy pre riadenie rizika, popis rolí a zodpovednosti a podobne,
- **základné kritéria**: kritéria hodnotenia rizika, strategická hodnota procesu alebo informácie, právne záväzky, regulačné požiadavky alebo zmluvy, stratégia spoločnosti a podobne,
- **rozsah a hranice**: obchodné činnosti a procesy organizácie, ciele organizácie, limity organizácie (logické, geografické, právne...), politiky organizácie a iné požiadavky.

V súčasnosti sa úvodne stretnutie vykonáva za asistencie všetkých spomínaných zainteresovaných strán, pričom je nutné zo stretnutia vytvoriť správu, ktorá obsahuje všetky spomínané náležitosti. Na vytváranie zápisov zo stretnutí a výslednej správy sa využívajú textové alebo tabuľkové procesory čo je z veľkej časti nie veľmi efektívne v ďalšom spracovaní, časovo náročné a v prípade implementácie ISMS do organizácie je potrebné vytvoriť si vlastné šablóny čo podlieha skúsenostiam bezpečnostného manažéra.

Pri vytváraní návrhu pre zlepšenie tohto podprocesu sme začali dizajnom jednotlivých častí. Z analýzy a podstaty úvodného stretnutia je jasné, že je nemožné tento krok plne automatizovať, avšak je ho možné vylepšiť. Navrhované zlepšenie je v podobe digitalizácie procesu vytvárania kontextu organizácie. Nami navrhnutá digitalizácia spočíva vo vytvorení preddefinovaného dotazníka, ktorý by sa skladal zo všeobecných otázok, ktoré je nutné zodpovedať, rovnako ako na fyzickom úvodnom stretnutí. Dotazník

by bol rozdelený do viacerých kategórií, na základe rolí a právomocí zainteresovaných strán. Digitalizácia tohto kroku by mohla byť súčasťou a implementáciou informačného systému, ktorý by poskytoval centralizované riešenie pre celý životný cyklus ISMS. Jednotlivé kategórie dotazníka by boli vyplnené príslušnou rolou a zainteresovanou stranou, kde vo výsledku by bolo možné vygenerovať výslednú správu vo vopred definovanom formáte.

Výsledná správa by poskytovala ucelený prehľad o kontexte organizácie a predstavuje digitalizovaný a spracovateľný vstup do ďalších procesov, či už ISMS, ISRM alebo auditu. S využitím digitalizovaného prístupu k riešeniu tohto kroku by sa zabezpečil plynulejší priebeh identifikácie základných informácií o organizácii, znížili by sa nároky na osobné skúsenosti bezpečnostného manažéra, prípadne audítora a zefektívnil by sa časový priebeh tohto kroku, tým, že jednotlivé zainteresované strany by mali dostupné iba svoje kategórie dotazníka, ktoré obsahujú cielené otázky na základe ich role a odpadá nutnosť osobného stretnutia.

3.1.1 Rozdelenie kategórií

Z podstaty úvodného stretnutia je zrejmé, že nie všetky otázky, ktoré sa týkajú kontextu organizácie sú cielené pre všetky zainteresované strany v plnom rozsahu. Z tohto dôvodu je pre zefektívnenie tohto podprocesu potrebné rozdeliť otázky dotazníka na základe ich obsahu a výslednej informácie do viacerých kategórií. Navrhované kategórie na základe odporúčaní sú:

- top manažment spoločnosti
- biznis vlastník
- bezpečnostný manažér
- zodpovedná osoba
- systémový vlastník
- administratívny a technický pracovníci
- *prípadne audítor*

3.1.2 Návrh dotazníka

Tabuľka 2 predstavuje ukážku možných otázok pre jednotlivé kategórie, za účelom vytvorenia kontextu organizácie. V dotazníku sú obsiahnuté aj otázky pre ďalšie podprocesy a získanie informácií pre podprocesy identifikácie zraniteľností a hrozieb. Na

základe výsledkov dotazníka sa generuje výsledná správa, prípadne čiastkový report podprocesu vytvárania kontextu organizácie. Zahrnutie otázok, ktoré sa týkajú viacerých podprocesov ISMS napomáha pri urýchlení procesu a plynulejšiemu priebehu automatizácie, kde na začiatku procesu je možné definovať všetky potrebné, informácie vstupujúce do ďalších procesov, ako napríklad: hodnotiace stupnice, kritéria hodnotenia rizík, stupnicu dopadov, identifikáciu primárnych aktív a podobne.

Tabuľka 2 Vzorový návrh dotazníka pre vytváranie kontextu organizácie

Kategória	Rola / Meno	Otázka	Odpoveď
Top manažment spoločnosti / Biznis vlastník	*„Text...“*	Aký je účel vašej organizácie?	*„Text...“*
	„Text...“	Aký je vývoj vášho podnikania za posledné roky?	*„Text...“*
	„Text...“	Aký je vývoj vonkajšieho prostredia, prípadne čo ovplyvňuje spoločnosť? (konkurencia, právne požiadavky, zákony, atď...)	*„Text...“*
	„Text...“	Aké by mohli byť dôvody pre vznik incidentu?	- *financie* - *pomsta* - *politická výhoda* - *ekonomická špionáž* - *ekonomická alebo obchodný výhoda* - *atď...*
	„Text...“	Aké sú vaše najdôležitejšie obchodné procesy?	*„Text...“*
	„Text...“	Čo je najcennejšie aktívum vo vašej organizácii?	*„Text...“*
	„Text...“	Aké je najdôležitejšie kritérium pre vaše podnikanie a čo sú najdôležitejšie údaje z hľadiska dôvernosti, dostupnosti a integrity?	*„Text...“*
	„Text...“	Aké právne a zákonné požiadavky musí spĺňať vaša organizácia prípadne	*„Text...“*

		v súlade s akými normami musí byť vaša činnosť? (lekárske právo na ochranu informácií, GDPR, atď...)	
	„Text...“	Čo vnímate ako najväčšiu hrozbu pre vaše podnikanie?	*„Text...“*
	„Text...“	Aké sú vaše najväčšie obavy, ktoré by výrazne narušili vaše podnikanie?	*„Text...“*
	„Text...“	Zažili ste niekedy kybernetický útok/incident? Vediete si zápis o týchto udalostiach?	*„Text...“*
	„Text...“	Je vaše geografické prostredie náchylné na záplavy, požiar, búrku, sneh, a podobne?	*„Text...“*
Bezpečnostný manažér, audítor	*„Text...“*	Existujú bezpečnostné politiky, ktoré sú schválené manažmentom a dodržujú sa popísané predpisy?	*„Text...“*
	„Text...“	Sú definované zodpovednosti a úlohy?	*„Text...“*
	„Text...“	Existuje segregácia definovaných povinností?	*„Text...“*
	„Text...“	Existuje dôkaz o informačnej bezpečnosti v projektovom manažmente?	*„Text...“*
	„Text...“	Existujú politiky pre mobilné zariadenia a prácu na diaľku?	*„Text...“*
	„Text...“	Existujú politiky pre zabezpečenie ľudských zdrojov?	*„Text...“*
	„Text...“	Sú definované politiky pre správu aktív/majetku? *(vlastníctvo, prijateľné používanie, vrátenie, atď...)*	*„Text...“*
Administratívny a technický pracovníci	*„Text...“*	Aké sú zásady riadenia prístupu a zodpovednosti pri riadení prístupu?	*„Text...“*

	„Text...“	Ako je zabezpečená fyzická a environmentálna bezpečnosť?	*„Text...“*
	„Text...“	Ako je zabezpečená prevádzková bezpečnosť?	*„Text...“*
	„Text...“	Aké sú komunikačné postupy a zabezpečenie vývoja a údržby systémov?	*„Text...“*
	„Text...“	Aké sú postupy pre dodržiavanie právnych a zmluvných požiadaviek?	*„Text...“*

3.1.3 Vytváranie organizačnej štruktúry

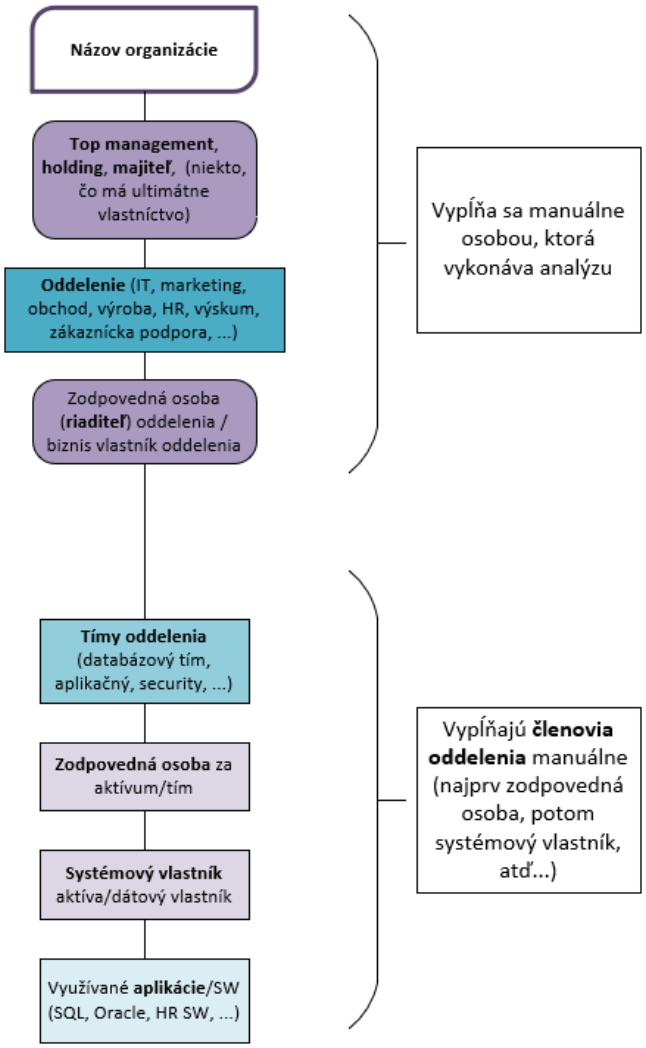
Ako sme na začiatku kapitoly 3 poukázali na potrebu mapovania IT aktív k ich vlastníkom, v tejto podkapitole uvádzame spôsob ako by bolo vhodné takéto prepojenie vytvárať v širšom kontexte. Do navrhovaného digitalizovaného procesu vytvárania kontextu organizácie navrhujeme zakomponovať vytváranie digitalizovanej formy organizačnej štruktúry podniku.

Proces vytvárania digitalizovanej organizačnej štruktúry podniku prebieha za účelom jej popisu, vizualizácie vzťahov a rozdelení úrovne právomocí medzi pracovnými pozíciami. Informácie obsiahnuté pri vytváraní organizačnej štruktúry, ako dôležitosť rolí, štruktúra riadenia, vlastníctvo IT aktív a top manažment ďalej vstupujú a budú využívané v procese riadenia rizík. Aplikačná časť spomínaného informačného systému by poskytovala priestor pre manuálne vytváranie organizačnej štruktúry delegovaným spôsobom systémom zhora nadol. Navrhovaný postup vytvárania organizačnej štruktúry je:

- **Top manažment** *(môže byť aj skupina biznis vlastníkov)* – definuje a vytvorí oddelenia organizácie, ku ktorým priradí biznis vlastníkov a prioritu pre dané oddelenie. Využitie hodnoty priority oddelenia bližšie popisujeme v kapitole 3.7.
- **Biznis vlastník** – definuje a vytvorí tímy pre jednotlivé oddelenia, ku ktorým priradí zodpovedné osoby.
    - Biznis vlastník taktiež zadefinuje a popíše svoj biznis proces alebo procesy, ako aj všetky kritické a dôležité softvérové aktíva, ktoré daný biznis proces podporujú. Okrem softvérových aktív definuje aj kritické a dôležité informácie a personál s ohľadom na tieto softvérové aktíva.

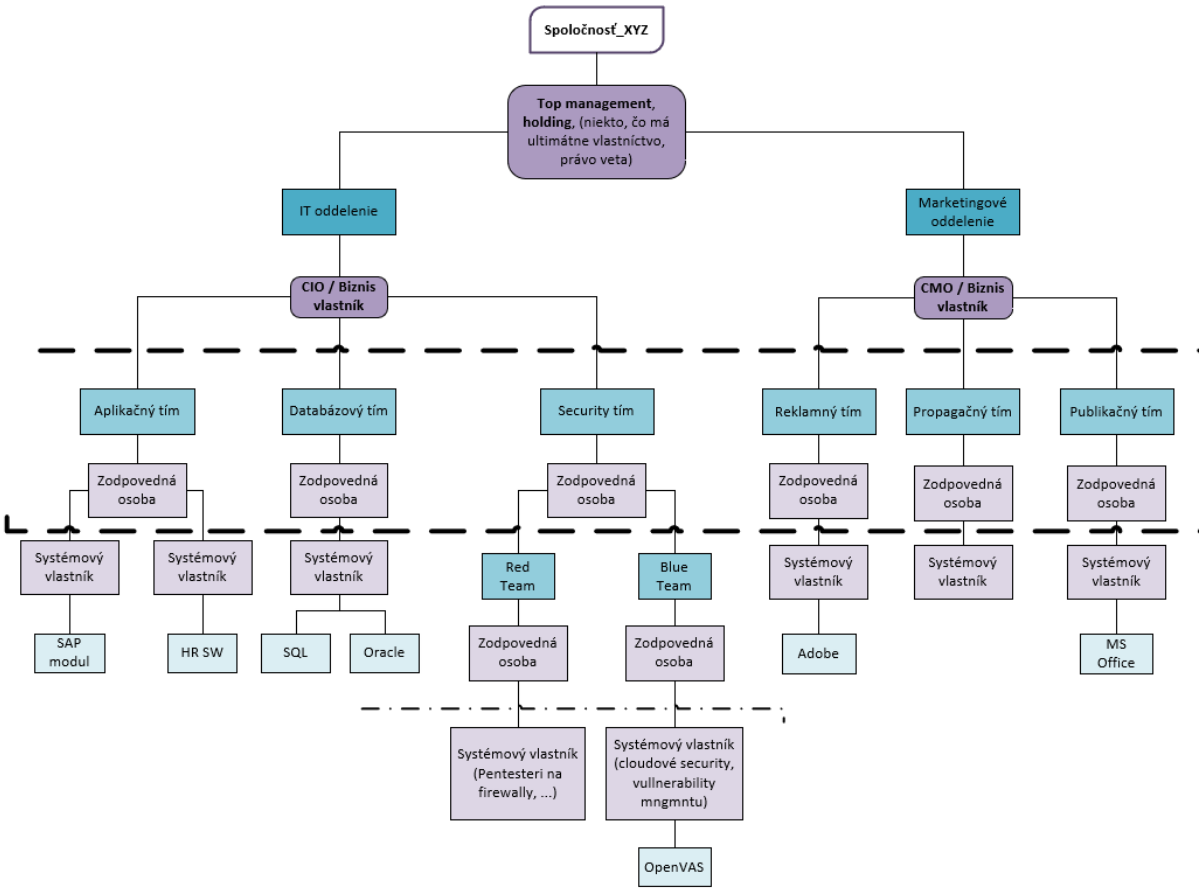
- **Zodpovedná osoba** *(môže byť aj systémový vlastník)* – definuje systémových vlastníkov IT aktív, ktoré spadajú pod konkrétny tím.
- **Systémový vlastník** – priradí si IT aktíva, ktoré vlastní *(softvérové aj hardvérové IT aktíva)* na základe zoznamu IT aktív. Zoznam IT aktív sa vytvorí nami navrhnutým automatizovaným spôsobom, ktorý je popísaný v kapitole 3.4.

Navrhovaný model vytvárania organizačnej štruktúry znázorňuje Obrázok 6.



Obrázok 6 Model vytvárania organizačnej štruktúry

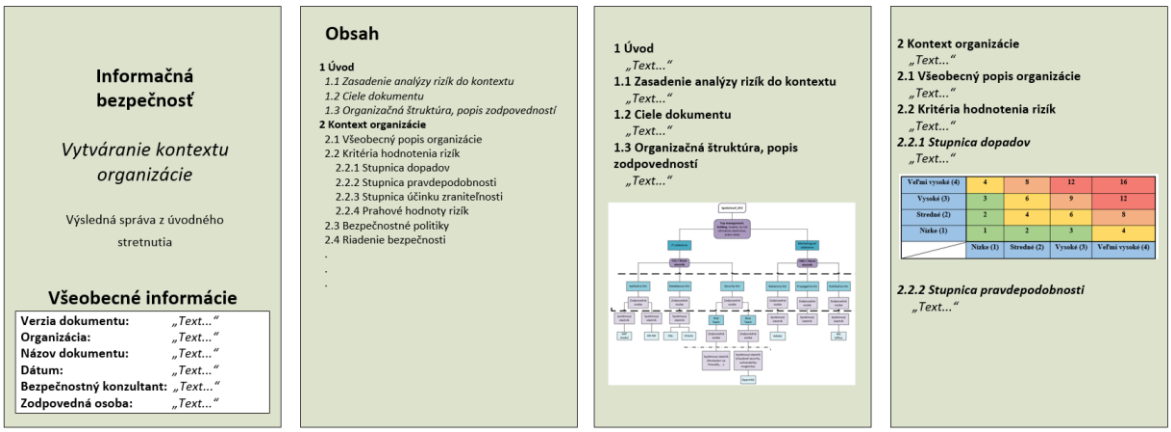
Výsledkom vytvorenej organizačnej štruktúry je presný popis a pohľad na právomoci jednotlivých rolí, definovaná váha oddelení, ktorá bude využívaná pre výpočet hodnoty IT aktív a prepojenie vlastníkov na jednotlivé IT aktíva. Príklad organizačnej štruktúry je znázornený na Obrázok 7.



Obrázok 7 Príklad vytvorenej organizačnej štruktúry

3.1.4 Generovanie výslednej správy

Po vyplnení dotazníka a vytvorení organizačnej štruktúry sa vygeneruje výsledná správa vo zvolenom elektronickom formáte (napríklad .docx, .pdf, .json). Ukážku vzorovej správy znázorňuje Obrázok 8.



Obrázok 8 Ukážka vzorovej vygenerovanej správy

3.2 Analýza dostupných riešení pre identifikáciu informačných aktív

Počas analýzy jednotlivých podprocesov ISMS sme sa zamerali aj na prieskum stavu riešení určených na vytváranie inventára majetku, ktoré patria do kategórie tzv. inventarizačných nástrojov. Okrem inventarizačných nástrojov sme analyzovali aj stav riešení určených pre analýzu rizík, čo môžeme kategorizovať ako nástroje riadenia rizík. Pre potreby poukázania dôležitosti riešenia problematiky automatizácie procesu identifikácie IT aktív sa preto v tejto kapitole venujeme analýze dvoch typov nástrojov.

Analýzu sme vykonávali na základe nami definovaných kritérií, ktoré sme navrhli nasledovne:

- licencia nástroja,
- hodnotenie nástroja *(fóra, spätná väzba používateľov, slabé a silné stránky)*,
- možnosti nasadenia nástroja,
- generovanie priebežných alebo výsledných správ,
- informačné aktíva *(import, export, automatická identifikácia, kategorizácia, vytváranie hierarchie, možnosti definovania aktív, uchovávané informácie o aktívach, ohodnotenie aktív...)*,
- hrozby, zraniteľnosti a riziká *(mapovanie hrozieb a zraniteľností, existencia zoznamu hrozieb a zraniteľnosti, metódy výpočtu rizika, existencia odporúčaní pre zmierňovanie rizík...)*.

3.2.1 Analýza inventarizačných nástrojov

Prvým z analyzovaných riešení boli inventarizačné nástroje. Pozornosť sme venovali nástrojom ako Lansweeper [18], Spiceworks [19] a iTop [39]. Tento typ aplikácií poskytuje funkcionalitu, ktorá sa najviac približuje potrebám identifikácie IT aktív organizácie. Ich zameranie a využitie je však prevažne pri správe majetku. Správe majetku, aktív a systémom ich riadenia sa venuje norma ISO 55001 [40], ktorá popisuje postupy pre správu aktív, avšak nie z pohľadu informačnej bezpečnosti. Úlohou týchto nástrojov je vytvoriť inventár majetku, ktorý poskytuje detailný obraz o informačných aktívach. To znamená, že pomocou nástroja sú uchovávané detailné informácie o každom aktíve, ako napríklad nainštalovaný softvér a jeho verzie, komplexné hardvérové informácie, model

zariadenia, typ zariadenia, výrobca, detailné informácie ohľadom operačného systému a podobne.

Existujú viaceré typy nástrojov pre správu majetku. Prvý typ takýchto riešení vôbec neposkytuje funkcionalitu automatickej identifikácie IT aktív. Riešenia ale slúžia iba ako prehľadná knižnica, ktorú je potrebné manuálne naplniť. Druhý typ inventarizačných nástrojov poskytuje automatickú detekciu IT aktív, avšak sú založené na agentovom prístupe. To znamená, že je potrebná inštalácia agenta na každé zariadenie pre správne fungovanie nástroja. Táto nutná podmienka je pomerne obmedzujúca v prípade nasadenia agentov na uzavreté medziľahlé sieťové (smerovače, prepínače, firewally a podobne) a IT prvky (úložiska, diskové polia, niektoré hypervízory a podobne), kde to nie je možné. Finálne na základe prevedeného skúmania tak môžeme konštatovať, že tieto nástroje sú nevýhodné pre ich využitie v automatizácii procesu identifikácie IT aktív pre ISMS. Dôvody sú ich prílišná detailnosť získavaných údajov, ktoré nepredstavujú vhodné vstupy do ďalších podprocesov ISMS. Ďalšou nevýhodou je potreba manuálnych vstupov či nutnosť inštalácie agentov na zariadenia IKT infraštruktúry, kde je nedostatočná podpora agentov pre operačné systémy (OS) medziľahlých sieťových prvkov. Oboje tak zároveň vyžaduje nadmernú časovú ale aj manuálnu náročnosť požadovaných úkonov spojených s ich nasadením a prevádzkou.

Výsledné porovnanie spomínaných inventarizačných nástrojov je reprezentované v Tabuľka 3. Nástroje boli porovnané v kategóriách ako licencia nástroja, nasadenie a implementácia nástroja, hodnotenie nástroja z pohľadu používateľov, získavanie informácií o aktívach, kategorizácia aktív, monitorovanie IKT infraštruktúry a aktív. Legenda symbolov uvedených v tabuľke a ich významy sú: **N** – nie, **Y** – áno, **N/A** – nehodnotené.

Tabuľka 3 Porovnanie inventarizačných nástrojov

Kategória	**Požadovaná funkcionalita**	**Nástroje pre manažment aktív (inventár aktív)**		
		Lansweeper	**iTop**	**Spiceworks**
Licencia	Komerčný bez skúšobnej verzie	N	N	N
	Komerčný so skúšobnou verziou	Y	Y	N
	Existuje prístup k zdrojovému	N	Y	N/A

	kódu?			
	Druh licencie	Úplná licencia po zakúpení	Úplná licencia	Úplná licencia po registrácii
	Cena licencie	Záleží od počtu aktív, do 5000 je cena 1 €/aktívum na rok	N/A	0,00 $
Nasadenie nástroja/ implementácia	lokálne (on-premise)	Y	Y	Y
	lokálne (v privátnom cloude)	Y	Y	Y
	hosťuje to tretia strana (napr. AWS privátny cloud, atď...) (napr. prístup cez webový prehliadač?)	Y	Y	Y
Hodnotenie nástroja, fóra, spätná väzba od používateľov	Silné stránky	Je možné použiť na komplikovanejšie/obsiahlejšie systémy, ktoré vyžadujú viacero funkcionalít; agentless; vopred definovaná široká škála typov aktív; aktívne fórum; dokáže odhaliť zraniteľnosti	Pomerne rozšírený a kustomizovateľný nástroj ku ktorému existuje dokumentácia a poskytuje viaceré funkcionality	Možnosť automatickej detekcie IT aktív, bezagentové získavanie informácií je pomerne nedostatočné, definovaná pomerne široká škála typov aktív, nástroj poskytuje definovanú kategorizáciu aktív

	Slabé stránky	Obsahuje nepodstatné funkcionality, bez autentifikačnýc h údajov je možné zistiť iba základné informácie, typy aktív sú nevyužiteľné pre náš systém; poskytovanie reportov iba pomocou SQL skriptov	Nástroj poskytuje manuálny manažment, nie je možné automaticky identifikovať aktíva	agentový prístup pre dosahovanie potrebných výsledkov
Aktíva	Aké kategórie aktív vie nástroj zastrešiť? Existuje v inventári nejaká hierarchia? Kategórie, podkategórie? (Inventár HW/SW a poskytovaných služieb, atď...)	Zariadenia, Softvér, Cloudové služby, Ľudia	Biznis procesy, služby, databázy, aplikácie, softvér, kontakt, lokácie, licencie, servery, sieťové zariadenia, dokumenty	Zariadenia Softvér Ľudia Cloudové služby
	Manuálne pridávanie aktív?	Y	Y	Y
	Ponúka nástroj automatickú identifikáciu aktív?)	Y (pomocou IP rozsahu aj konkrétnej IP, odchytávaním komunikácie na rozhraniach zariadenia kde Lansweeper beží - Asset Radar	N	Y

	Je daný nástroj agentless/agent? Je potrebná dodatočná inštalácia agentov? (za účelom podrobnejšieho skenu aktív)	Agentless, ale pre potreby získania detailnejších informácií je potrebný agent, pre využitie agentless sú potrebné autentifikačné údaje	Nie je možné automaticky oskenovať aktíva	Áno, pre úplný prehľad HW a SW na danom aktíve je potrebná inštalácia agenta na koncových zariadeniach.
	Aké informácie je možné zistiť automatickým skenom o aktíve? (IP adresy, MAC adresy, HW komponenty, nainštalovaný SW, atď...)	V prípade, že sú autentifikačné údaje a agent tak je možné zistiť IP, MAC, OS, nainštalovaný SW, HW detaily, výrobca, MTU, rýchlosť linky, maska, vlan. Ak NIE tak iba IP, typ zariadenia prípadne výrobcu (prípadne model zariadenia)	Nie je možné automaticky oskenovať aktíva	Záleží či je na danom aktíve nainštalovaný skenovací agent. Ak ÁNO, tak vie zistiť všetko (IP adresu, MAC adresu, OS, nainštalovaný SW, detaily o HW atď...). Ak NIE tak zistí len (IP adresu, MAC adresu, prípadne výrobcu)
	Je možný import aktív? (pomocou akého formátu? XML, CSV, PDF...)	Áno, je možný import pomocou CVS, existuje preddefinovaný vzor pre import	Áno je možný import, avšak iba objektov, nie konkrétne informácií o aktíve.	Áno, je to možné pomocou CSV súboru, kde je preddefinovaný formát
	Je možný export aktív? (pomocou akého formátu? XML, CSV, PDF...)	Áno, je možný export do XLS, CSV, XML	Áno je možný export avšak iba objektov nie celkovo informácie o aktívach	Áno, buď celý inventár, alebo konkrétnu tabuľku (napr. tabuľka zariadení)

	Aký HW je možné zistiť na danom aktíve? je možné zistiť aj podrobné informácie?	Je možné zistiť všetok HW daného aktíva, t.j.: posledný prihlásený používateľ, OS, výrobca, RAM, CPU, základná doska, grafické, sieťové a zvukové karty, využitie HDD, periférie, antivírus...	N/A	Je možné zistiť všetok HW daného aktíva, t.j.: OS, CPU, RAM, informácie o HDD, BIOS...
	Aký nainštalovaný SW je možné zistiť o aktíve? Je možné zistiť aj verziu softvéru, dátum inštalácie atď...?	Je možné zistiť všetok nainštalovaný SW na aktíve (názov, verziu, dátum inštalácie, zdroj)	N/A	Vie zistiť všetok nainštalovaný SW na aktíve, t.j.: názov, verziu, dátum nainštalovania, typ inštalácie
	Rozlišujú sa aktíva a ich HW komponenty? Existuje priradzovanie HW k aktívu?	Áno existuje mapovanie HW k aktívu.	Ku každému aktívu je aj HW popis	Je to rozdelené, kde ku každému aktívu je priradený jeho HW
	Rozlišujú sa aktíva a ich SW komponenty? Existuje priradzovanie SW k aktívu?	Áno existuje mapovanie SW k aktívu	Ku každému aktívu je aj SW popis	Je to rozdelené, kde ku každému aktívu je priradený jeho SW
	Existuje v inventári nejaká hierarchia? Kategórie, podkategórie?(Inventár HW, inventár SW, inventár poskytovaných služieb atď...)	Zariadenia, Softvér, Cloudové služby, Ľudia	biznis procesy, služby, databázy, aplikácie, softvér, kontakt, lokácie, licencie, servery, sieťové zariadenia	Áno, sú rozčlenené jednotlivé IT aktíva ako: zariadenia, softvér, ľudia, cloudové služby
	Rozlišujú sa IT aktíva ako napr.	ľudské zdroje	ľudské zdroje, kontakty	ľudské zdroje

	ľudské zdroje, biznis procesy, informácie?			
	Je možné k aktívam priradiť ich vlastníkov? (biznis/softvérový vlastník, administrátor atď..)	Y	Y	Y
	Je možné manuálne pridať aktíva typu: ľudské zdroje, biznis procesy, atď...?	Je možné pridávať **Team** (HR, IT Mngmt...) **Rolu** (Administrátor, manažér aktíva...) **Používateľa**, taktiež je možné importovať používateľov cez CSV	Y	Áno, je možné pridať ľudí a pridať im **rolu**, napr.: Admin, koncový používateľ. Je možné priradiť **pracovnú pozíciu** ľudí: Marketing, Predaj, Operatíva...
Hierarchia	Ako je riešené rozdelenie/hierarchie v inventári aktív?	N/A	N/A	**Všeobecné info**: popis, typ, výrobca, model, OS, sériové číslo, IP adresa, MAC adresa **HW:** celková kapacita, rozhranie, **Sieť:** IPv4 a IPv6/MAC adresy, maska, DNS...**SW:** nainštalovaný SW
Monitoring	Poskytuje nástroj monitorovanie siete?	N	N	N
	Poskytuje nástroj monitorovanie HW častí?	Y	N	Y
	Poskytuje nástroj	Y	N	Y

	automatickú aktualizáciu zoznamu IT aktív pri zmenách?			

Na základe výsledkov analýzy sme dospeli k záverom, že v súčasnosti chýba pokrytie automatizovaného procesu pre identifikáciu IT aktív. Analýza ukázala nedostatok vhodných riešení a potvrdila potrebu riešenia uceleného systematického prístupu k automatizácii procesu identifikácie IT aktív. Nami navrhované riešenie by malo využívať bez agentový prístup, čo by časovo zefektívnilo nasadenie takéhoto systému a odbremenilo by správcov systémov od nadmernej manuálnej či procesnej činnosti.

3.2.2 Analýza nástrojov riadenia rizík

Ďalším z analyzovaných riešení boli nástroje riadenia rizík. Pozornosť sme venovali nástrojom ako Eramba [41], Archer [42], SimpleRisk [43], PTA Professional [44]. Tento typ aplikácií poskytuje funkcionalitu, ktorá pokrýva oblasť riadenia rizík, pričom ako vstup vyžaduje identifikované informačné aktíva. Z tohto dôvodu sme skúmali možnosti využitia týchto riešení v procese automatizácie riadenia rizík a skúmali sme či nástroje poskytujú funkcionalitu, ktorá by pokrývala automatizovanú identifikáciu IT aktív.

Úlohou týchto nástrojov je zabezpečiť digitalizáciu procesu analýzy rizík, na základe manuálne zvolených vstupov. To znamená, že pomocou nástroja je možné na základe manuálnych vstupov definovať IT aktíva a následne pristúpiť k analýze rizík. Tento typ nástrojov poskytuje rôzne prístupy a metódy pre definovanie hodnoty pre IT aktíva, ako aj prístupy pre identifikáciu a spracovanie rizika. Niektoré poskytujú preddefinovaný zoznam hrozieb a zraniteľností, ktoré si vie používateľ manuálne priradiť k vybraným aktívam, iné poskytujú priestor pre vlastnú definíciu zraniteľností a hrozieb. Čo sa týka možností využitia nástrojov pre proces automatickej identifikácie IT aktív, niektoré zo spomínaných poskytujú tzv. automatickú detekciu aktív. Automatickou detekciou však nástroje dokážu zistiť iba IP adresy, pre ktoré nie sú zistené žiadne bližšie informácie.

Výsledné porovnanie spomínaných inventarizačných nástrojov je reprezentované v Tabuľka 4. Nástroje boli porovnané v kategóriách ako licencia nástroja, hodnotenie nástroja z pohľadu používateľov, získavanie informácií o aktívach, kategorizácia

zraniteľností hrozieb a opatrení. Legenda symbolov uvedených v tabuľke a ich významy sú: **N** – nie, **Y** – áno, **N/A** – nehodnotené.

Tabuľka 4 Porovnanie nástrojov manažmentu rizík

Kategórie	Požadovaná funkcionalita	Nástroje pre manažment rizík			
		Eramba	**Archer**	**SimpleRisk**	**PTA Professional**
Licencia	Komerčný bez skúšobnej verzie	N	N	Y	N
	Komerčný so skúšobnou verziou	Y	Y	Y	Y
	OpenSource	Y	N	Y	N
	Druh licencie	Podniková alebo Komunitná	N/A	Core, On-premise, Hosted	Trial verzia, voľný PTA program
Hodnotenie nástroja, fóra, spätná väzba od používateľov	Slabé stránky	Community verzia sa aktualizuje len raz za rok, odpadkový kôš sa nedá premazať	Pomalý script, updaty robia problémy s UI, dokumentácia je nepresná a chýbajú informácie	Aktíva sa musia zadávať ručne, dokáže skenovať iba IP adresy, chýba podpora UX	Slabá dokumentácia, neaktivita vývojárov, zastaralý softvér, manuálne pridávanie všetkých položiek
	Silné stránky	Celkom prehľadné prostredie, je možné mapovať iné štandardy (NIST, ISO, ...)	Detailná kontrola pracovných tokov, reporty, hostované na cloude, integruje viacero štandardov real-time informácie	Databáza rizík, prehľadné prostredie, dostupné tutoriály, fórum, časté updaty, vytváranie skupín aktív, viaceré metódy ohodnotenia rizika	Komplexné riešenie pre analýzu hrozieb

Reporty	Je možné generovať report?	Y	Y	Y (len pre extra funkcie)	Y
	Aký formát generovania reportov je podporovaný? (PDF, CSV...)	PDF, CSV	XLS, CSV, PDF, RTF, HTML, XML	CSV	výpis v programe
Aktíva	Existuje preddefinovaný zoznam aktív?	Y	N/A	N	Y
	Je zoznam aktív hierarchický?	N	N/A	Y	N
	Rozlišujú sa primárne a sekundárne (podporné) aktíva?	N	N/A	N	N
	Je zoznam aktív totožný s normou ISO 27005?	Y	N/A	N	Existuje knižnica podľa normy ISO 27001
	Čo chýba, alebo je navyše oproti ISO zoznamu aktív?	Navyše aktíva, ktoré je možné na ISO 27005 namapovať	N/A	N/A	Je to len vzorová knižnica (.thl)
	Existuje možnosť pridávať nové aktíva manuálne?	Y	N/A	Y	Y
	Je k dispozícií automatický zber aktív?	N	N/A	Y	N
	Čo je automaticky možné zistiť o aktívach?	N/A	N/A	IP adresy	N/A

	Pridáva automatický zber aktíva do zoznamu aktív?	N/A	N/A	Y	N/A
Hodnotenie aktív	Hodnotia sa aktíva iba jedným číslom?	Y	N/A	Y	Y
	Aká je použitá metóda hodnotenia? Aký? (0 - 5, 1 - 10, cena aktíva)	Cena aktíva	N/A	Cena aktíva	Cena aktíva
	Používa sa nejaká zložitejšia metrika?	N	N	N	N
	Môžu aktíva ohodnocovať viacerí zadávatelia a ich výsledky sa nejako prepočítajú do hodnoty aktíva?	N	N	N/A - skôr nie	N
	Ak môžu ohodnocovať aktíva viacerí, je možné zadávateľom priradiť váhu/prioritu?	N	N	N	N
Riziká, hrozby, zraniteľnosti	Mapuje sa riziko priamo k aktívu?	Y	N	Y	Y
	Je možné namapovať rovnaké riziko k viacerým aktívam?	Y	N/A	Y	Y
	Rozlišuje sa hrozba/zraniteľnosť/riziko?	Y	N/A	Y	Y

	HROZBY				
	Je k dispozícii preddefinovaný zoznam hrozieb?	Y	N	N	Y
	Je zoznam hrozieb hierarchický?	N	N	N	N
	Je zoznam úplný podľa ISO 27005?	N	N	N	N
	Čo chýba, alebo je navyše oproti ISO zoznamu hrozieb?	Naviac napr. štrajky, ale aj veci, ktoré sa tam nie sú	N/A	N/A	Je to len vzorová knižnica (.thl)
	Existuje možnosť pridávať nové hrozby manuálne?	Y	N	N	Y
	Hodnota/miera hrozby sa uvádza len ako jedno číslo?	N	N/A	N/A	Y
	Je použitý nejaký rozsah hodnotenia hrozby? Aký? (0 - 5, 1 - 10, cena straty)	N	N	N	N
	Vstupuje do výpočtu hrozby aj pravdepodobnosť hrozby?	N	N	N	N
	Vstupuje do výpočtu hrozby aj miera dopadu hrozby?	N	N	N	N
	RIZIKÁ				

	Je k dispozícii preddefinovaný zoznam rizík?	N	N	Y	Y
	Je zoznam rizík hierarchický?	N/A	N	Y	N
	Je zoznam úplný s ISO 27005?	N/A	N	N	N
	Čo chýba, alebo je navyše oproti ISO zoznamu rizík?	N/A	N	N/A	Je to len vzorová knižnica (.thl)
	Existuje možnosť pridávať nové riziká manuálne?	Y (jediná možnosť)	N/A	Y	Y
	Existuje možnosť automaticky zisťovať riziká v systéme?	N	N/A	Y	N
	Hodnota/miera rizika sa uvádza len ako jedno číslo?	Y	N/A	Y	Y
	Aká je použitá metrika hodnotenia? Aký? (0 - 5, 1 - 10, cena/strata v prípade výskytu rizika)	1-250	N/A	0.4 - 10	N/A
	Vstupuje do výpočtu rizika pravdepodobnosť tohto rizika?	Y	N/A	Y	N/A
	Vstupuje do výpočtu rizika aj miera dopadu rizika?	Y	N/A	Y	N/A

	Aká metóda pre hodnotenie rizika je k dispozícii?	Eramba Multiply, alebo napr. Magerit...	N/A	Klasický, DREAD, CVSS, OWASP, Custom Value(0-10)	N/A
	ZRANITEĽNOSTI				
	Je k dispozícii preddefinovaný zoznam zraniteľností?	Y	N	N	Y
	Je zoznam zraniteľností hierarchický?	N	N	N	N
	Je zoznam úplný v porovnaní s ISO 27005? (príloha D)	Y	N	N	N
	Čo chýba, alebo je navyše oproti zoznamu zraniteľností podľa ISO? (príloha D)	Informácie ktoré nie sú priamo v ISO, kt. je možné namapovať na ISO	N/A	N/A	Je to len vzorová knižnica (.thl)
	Existuje možnosť pridávať nové zraniteľnosti manuálne?	Y	N	N	Y
	Existuje možnosť automaticky zisťovať zraniteľnosti v systéme?	N	N	N	N
	Hodnota/miera zraniteľnosti sa uvádza len ako jedno číslo?	N/A	N/A	N/A	N/A

	Je použitý nejaký rozsah hodnotenia zraniteľnosti? Aký? (0 - 5, 1 - 10)	N	N	N	N
Zmierňovanie rizík	Je možné do systému zadávať odporúčania pre zmierňovanie rizík?	Y	N	Y	Y
	Existuje preddefinovaný zoznam bezpečnostných opatrení (BO)?	Y	N/A	N	N
	Je možné pridať BO k viacerým rizikám?	Y	N/A	Y	Y
	Je možné sa priradiť viacero rizík k jednému opatreniu?	Y	N/A	Y	Y
	Poskytuje automatický prepočet miery rizika?	N (resp. je tu prepočet na zvyškové skóre)	N/A	N	Y (prepočet na zvyškové riziko daného aktíva)

Analýzou riešení, ktoré pokrývajú problematiku manažmentu rizík sa ukázalo, že taktiež nevyužívajú automatizovanú identifikáciu IT aktív. Nástroje sa venujú analýze rizík, ktorá závisí od správne definovaných IT aktív, avšak tie je do nástrojov potrebné zadávať manuálne. Analýza tak potvrdila nedostatok vhodných riešení a potrebu venovania sa problematike automatizovaného zberu IT aktív tak vnímame ako základný problém pri automatizácií procesov ISMS.

3.3 Automatická identifikácia informačných aktív

Hlavným cieľom práce je navrhnúť riešenia automatizácie vybraných procesov ISMS, do čoho spadá aj proces identifikácie IT aktív. Aby bolo možné dokázať potrebu riešenia tejto problematiky, pristúpili sme k analýze stavu, kde sme sa zamerali na analýzu dostupných riešení zameraných na túto oblasť. Na základe získaných poznatkov, ktoré vyplynuli z analýzy popísanej v kapitole 3.2, sme identifikovali potrebu riešenia automatickej identifikácie IT aktív. Niektoré štúdie [45] popisujú možnosti využitia rôznych nástrojov pre potreby získavania informácií zo siete, avšak ani jeden z týchto nástrojov neposkytuje ucelené riešenie, ktoré by plne automatizovalo tento proces a poskytovalo požadované výstupy. Aj napriek existencii nástrojov zameriavajúcich sa na skenovanie IKT infraštruktúry, nie je možné jednoznačne vybrať taký, ktorý by poskytoval relevantné dáta, ktoré by predstavovali vstupy do ďalších podprocesov ISMS. Na základe prieskumu stavu môžeme povedať, že v súčasnosti chýba systematický a ucelený prístup k riešeniu automatickej identifikácie IT aktív zo siete (IKT infraštruktúry).

V ďalšom riešení sme teda pristúpili k ďalším krokom, potrebným pre podprocesy ISMS a ISRM. Zamerali sme sa na analýzu dostupných nástrojov a sieťových protokolov, ktoré by bolo možné využiť pri návrhu uceleného systému automatizovaného zberu IT aktív. Bližší popis analýzy jednotlivých nástrojov a sieťových protokolov je popísaný v kapitolách 3.3.3 a 3.3.4. V kapitolách 3.3.1 a 3.3.2 sme definovali porovnávacie kritériá ako aj atribúty IT aktív, ktoré požadujeme zo siete automatizovane získavať na základe čoho sme vykonali analýzu výberu vhodných nástrojov a sieťových protokolov. Nástroje sme porovnali a na základe výsledkov vybrali najvhodnejšie pre naše potreby. Ako ďalším, a teda hlavným krokom bol návrh dvoch algoritmov pre automatický zber IT aktív, ktoré sme na základe definovaných porovnávacích kritérií porovnali a vybrali vhodný pre implementáciu. Návrhom jednotlivých algoritmov sa venuje kapitola 3.4. Ako posledný krok pre dosiahnutie hlavného cieľa, bolo potrebné vytvoriť dátový model, pre ukladanie získavaných informácií, a teda IT aktív pre potreby ich použitia v ďalších podprocesoch ISMS a ISRM. Kapitola 3.6 je venovaná práve návrhu dátového modelu v ktorom sme pokryli aj oblasť virtualizovaných zariadení a oblasť cloud computingu, čo taktiež patrí do IKT infraštruktúry spoločnosti a môže predstavovať informačné aktíva.

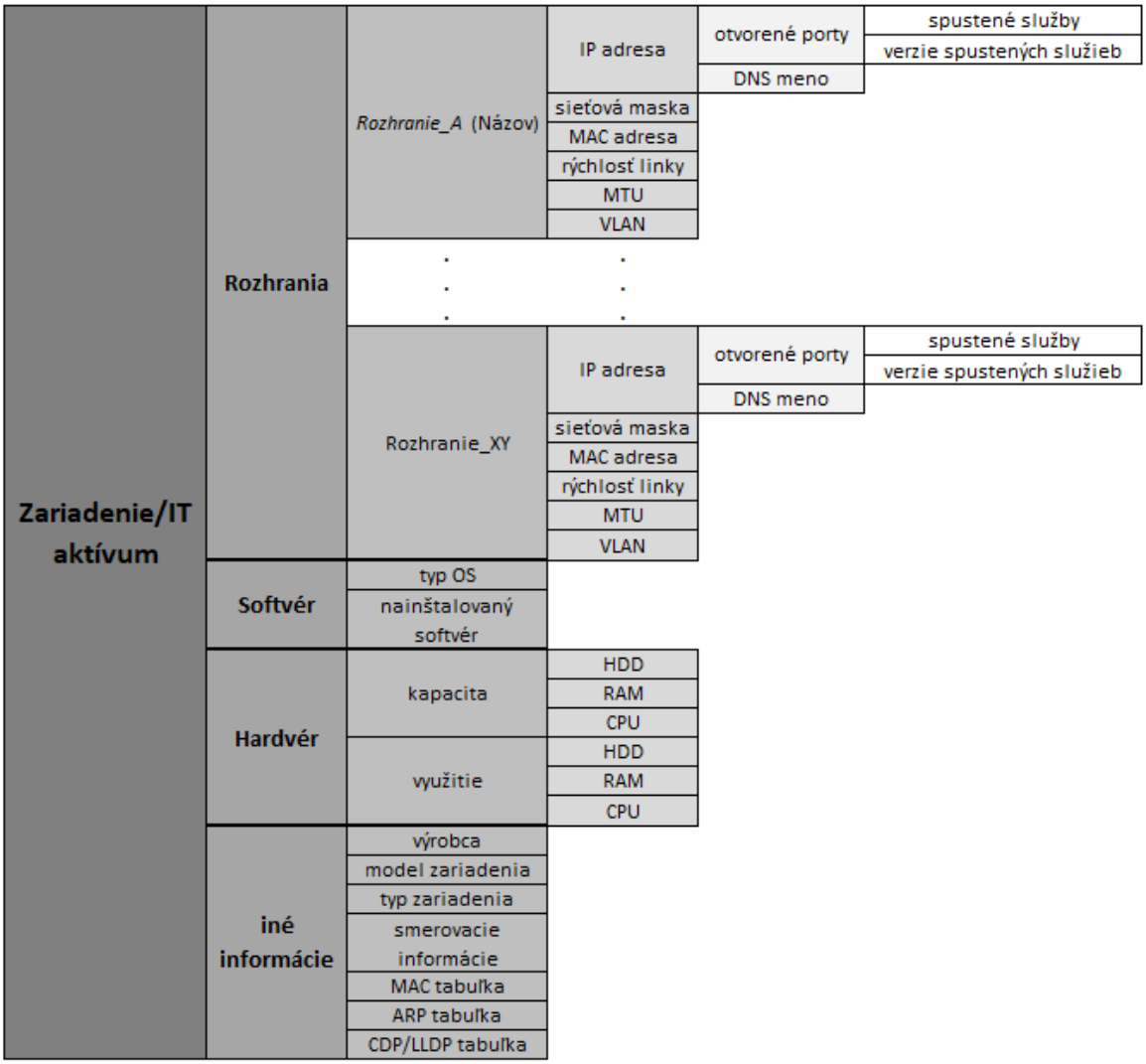
3.3.1 Definovanie atribútov ako vstupov pre automatizované riadenie rizík

Aby bolo možné vykonať výber vhodných a dostupných riešení pre úlohu automatizovaného zberu IT aktív, bolo potrebné definovať atribúty, ktoré vstupujú do ďalšieho podprocesu, a teda procesu riadenia rizík.

Na základe získaných skúseností sme navrhli zoznam dvadsiatich atribútov, ktoré poskytujú dostatočný obraz pre identifikáciu informačného aktíva a predstavujú vstup do ďalších podprocesov. Nami určené atribúty konkrétneho aktíva, ktoré budú zbierané zo siete sú:

- IP adresa,
- otvorené komunikačné TCP a UDP porty,
- spustené služby,
- verzie spustených služieb,
- aktívne sieťové rozhrania,
- IP adresa konkrétneho fyzického rozhrania,
- IP adresa susedného zariadenia pre konkrétne fyzické rozhranie,
- rýchlosť rozhrania/linky,
- MAC adresa sieťového rozhrania,
- maska siete do ktorej patrí konkrétna IP adresa,
- výrobca zariadenia či jeho značka,
- model zariadenia,
- typ operačného systému,
- typ zariadenia,
- doménové meno/názov zariadenia,
- osadená kapacita systémových zdrojov– disk, pamäť, procesor,
- využitie systémových zdrojov– disk, pamäť, procesor,
- maximálna veľkosť rámca (MTU) pre rozhranie,
- číslo virtualizovanej siete (VLAN) pre rozhranie,
- nainštalovaný softvér.

Z vyššie definovaných atribútov je možné vytvoriť jednoznačný model IT aktíva na základe kategorizácie definovaných atribútov. Model je znázornený na Obrázok 9.



Obrázok 9 Model IT aktíva

Z dôvodu vylepšenia ďalších podprocesov ISMS, ako napríklad hodnotenie IT aktív, výpočet celkového rizika pre primárne aktívum a dokazovanie nutnosti implementácie protiopatrení pre znižovanie rizika navrhujeme dodefinovať získavanie ďalších atribútov. Atribúty sa týkajú ďalších sieťových informácií, ktoré sú potrebné pre vytváranie topologickej mapy a vytvárania tzv. cesty vzájomných súvzťažností medzi aktívami organizácie. Informácie, ktoré definujú jedno konkrétne zariadenie je teda vhodné doplniť o informácie ohľadom susedných zariadení tohto hardvérového aktíva práve za účelom identifikácie vzájomných vzťahov medzi aktívami. Ako už bolo spomenuté v kapitole 1.2, ako doplnok riešenej automatizácie navrhujeme zároveň vytvárať model informačných aktív, tzv. topologickú mapu, ktorá bude znázorňovať vzájomné súvzťažnosti jednotlivých IT aktív. Návrhu vytvárania topologickej mapy a jej využitiu sa venujeme v kapitole 3.7.1. Medzi dodatočné zbierané atribúty aktíva patria:

- smerovacia tabuľka,
- prepínacia MAC tabuľka,
- tabuľka susedov (CDP/LLDP),
- tabuľka mapovaní IP a MAC adries (ARP tabuľka).

3.3.2 Definovanie porovnávacích kritérií pre výber vhodných nástrojov a protokolov skenovania siete

Pri definovaní porovnávacích kritérií pre výber vhodných čiastkových nástrojov využiteľných v systéme automatizovaného zberu aktív a ich používanie sme zvolili racionálny prístup založený na potrebách audítorov a bezpečnostných manažérov v dosahovaní relevantných informácií potrebných do procesu manažmentu rizík a auditu s ohľadom na informačnú bezpečnosť.

Z tohto dôvodu sme sa zamerali na vlastnosti ako jednoduchosť riešenia, plynulosť a efektivitu pre proces identifikácie IT aktív automatizovaným spôsobom a navrhli sme vhodné porovnávacie kritéria pre zabezpečenie týchto podmienok. Porovnávacie kritéria výberu sme si stanovili nasledovne:

- možnosť skenovať celé IP adresné rozsahy naraz,
- intuitívne rozhranie nástroja a možnosti jeho využitia,
- možnosť formátovať výstupný formát z nástroja (xml, yaml, json a iné),
- jednoduchosť pri používaní nástroja,
- potreba administrátorských práv pre spúšťanie nástroja,
- veľkosť komunity a podpora nástroja,
- dostupnosť nástroja (licencia vs. otvorený kód),
- počet zistených informácií z navrhovanej schémy,
- rýchlosť skenu pre jedno zariadenie,
- rýchlosť skenu siete o veľkosti približne 30 zariadení,
- podpora operačného systému Linux,
- využitie nástroja pre skenovanie informácií z viacerých OS (Windows, Linux, MacOS),
- použitie nástroja pre skenovanie informácií o medziľahlých sieťových zariadeniach (smerovač, prepínač, firewall a podobne),

- použitie nástroja pre skenovanie informácií z OS vybraných výrobcov. Pre potreby experimentálneho overenia sme vybrali výrobcov Mikrotik, Cisco, Fortinet, Juniper,
- podpora viacerých funkcionalít (ping, sken otvorených portov, odhad OS, zisťovanie zraniteľností a iné),
- náročnosť nástroja na hardvérové prostriedky (CPU, RAM),
- objem skenovaných dát pre jedno zariadenie,
- objem skenovaných dát pre celú sieť o veľkosti približne 30 zariadení.

3.3.3 Analýza nástrojov skenovania siete

V tejto fáze riešenia práce bolo cieľom vytvoriť porovnávaciu analýzu viacerých dostupných nástrojov, ktoré je možné využiť v procese zhromažďovania informácií automatizovaným spôsobom a finálne vybrať najvhodnejšie pre pilotné experimentálne nasadenie. Porovnávali sme nami vybrané nástroje tak, aby boli schopné získať čo najviac definovaných informácií, ktoré budú predstavovať vstupy do ďalších podprocesov v rámci manažmentu rizík a auditu.

Počas analýzy sme sa zamerali hlavne na nástroje s otvoreným kódom, ktoré sú podporované pre operačný systém Linux. Venovali sme pozornosť nástrojom vhodným pre každodenné potreby audítorov, čo súvisí s nárokmi nástroja na hardvérové prostriedky a čas nevyhnutný na jeho zvládnutie a intuitívne používanie, aby sa čo najviac zmiernila potreba disponovať nadmerným množstvom technických a teoretických poznatkov.

Celkovo sme analyzovali dvanásť nástrojov, ktoré sú Nmap, Fping, NetDiscover, Hping3, Masscan, Arp-scan, Ethtool, Nmcli, Netstat, PingSweep, Ping TcpDump. V ďalšej časti tejto podkapitoly si bližšie popíšeme len tie najrelevantnejšie, ktoré na základe analýzy najlepšie splnili požadovanú funkcionalitu. S využitím popisovaných nástrojov je možné zabezpečiť identifikáciu IT aktív z IKT infraštruktúry a zber požadovaných atribútov, pre ktoré sme následne navrhli algoritmy automatizovanej činnosti.

Prvým z analyzovaných nástrojov bol najpoužívanejší nástroj určený na skenovanie siete, a to Nmap [46]. Výhodou tohto nástroja je jeho rozsiahle rozšírenie medzi komunitou. Disponuje mnohými funkciami a nastaveniami, čo umožňuje jeho využitie pre získanie viacerých z definovaných atribútov. Menšou nevýhodou je jeho komplexnosť a pomerne dlhá časová odozva pri skenovaní veľkých sietí a v nich hlavne otvorených UDP portov. Ďalším z nástrojov bol Hping3 [47]. Pomocou tohto nástroja je možné

vykonávať viaceré činnosti, ako napríklad: testovanie firewallu, skenovanie otvorených portov, zisťovanie MTU, odhadovanie operačného systému a podobne. Výhodou nástroja Hping3, podobne ako u nástroja Nmap, je dostupnosť, dokumentácia, komunita a rýchlosť skenovania. Hlavnou nevýhodou je chýbajúca funkcionalita skenovania celých sieťových rozsahov a možnosť formátovania výstupov, ktoré nástroj ponúka. Netdiscover [48] je v poradí tretím analyzovaným nástrojom. Jeho primárne využitie spočíva v prieskume aktívnych IP adries v sieti a kontrole ARP prevádzky. Je vyvinutý hlavne pre bezdrôtové siete bez DHCP servera. Výhodou Netdiscover je jeho rýchlosť a sledovanie živej prevádzky a komunikácie. To je z časti aj jeho nevýhodou. Keďže skenuje aktuálnu komunikáciu v sieti, neposkytuje formátovateľné výstupy čo spôsobuje náročnosť implementácie do automatizačných procesov. Štvrtým a zároveň posledným popisovaným nástrojom je Masscan [49]. Nástroj je postavený na asynchrónnom skenovaní otvorených TCP portov. Jeho výhodou je možnosť prispôsobenie rýchlosti skenovania, avšak pri veľkých rýchlostiach skenovania portov sú výsledky výrazne odlišné od tých pomalších. Nevýhodou je jeho obmedzené použitie, a to iba na skenovanie otvorených TCP portov a časová náročnosť v prípade potreby detailných výstupov.

3.3.4 Analýza sieťových protokolov pre získavanie informácií

Okrem analýzy dostupných nástrojov, sme venovali pozornosť aj analýze manažmentových sieťových protokolov, ktoré je možné využiť pri automatickej identifikácií IT aktív. Tu sme sa zamerali na protokoly SSH, SNMP a WMI. Pre koncové zariadenia typu Windows sme otestovali aj využitie sady rozšírení k modelu ovládača Windows, a teda WMI, konkrétne softvérovú nadstavbu wmic [50]. Wmic poskytuje rozhranie príkazového riadku pre WMI. Na základe zistení môžeme povedať, že všetky skúmané sieťové protokoly sú využiteľné pre získanie všetkých definovaných atribútov, samozrejme s využitím natívnych výpisov relevantných k operačnému systému.

Výhodou využitia prístupu získavania informácií na základe sieťových protokolov je vysoká úspešnosť v získaní všetkých potrebných informácií na identifikáciu IT aktíva a taktiež na vytvorenie súvzťažností medzi jednotlivými aktívami.

Nevýhodou pri používaní protokolu SNMP je potreba konfiguračne zabezpečiť jeho funkčnosť. To znamená, že je nutný zásah do infraštruktúry a potreba konfigurácie protokolu SNMP na každom zariadení. Ďalšou nevýhodou sa javí široká škála výrobcov, ktorí poskytujú svoje zariadenia, ale len s určitou podporou MIB databáz pre SNMP, kde sú obsiahnuté zadefinované atribúty. Aby bolo navrhované riešenie generické a bolo ho

možné využiť pre rôzne zariadenia od rôznych výrobcov, museli sme definovať vhodné SNMP volania z verejnej časti stromu MIB databáz. Riešenie automatizovaného skenovania pomocou protokolu SNMP bližšie popisujeme v kapitole 3.4.

Využitie protokolu SSH so sebou prináša taktiež zopár nevýhod. Prvou nevýhodou je potreba dodatočnej réžie, rovnako ako pri protokole SNMP, a to nutnosť konfigurácie vzdialeného SSH prístupu na každé zariadenie v infraštruktúre. Dodatočná réžia je spojená aj s uchovávaním prihlasovacích údajov. Ďalšou komplikáciou pri využití SSH protokolu pre získavanie informácií je rôznorodosť operačných systémov a firmvérov, či jeho až chýbajúca podpora v niektorých OS. Pre podporované ale odlišné OS je nutné nadefinovať SSH volania a výpisy jednotlivých atribútov špecifické pre konkrétny operačný systém a jeho distribúciu. Taktiež je potrebné vyvinúť softvér, ktorý dokáže jednotlivé výstupy vhodne rozkladať (parsovať) aby sme získali požadované informácie v správnom tvare. Bližšiemu popisu využitia SSH protokolu popisujeme v kapitole 3.4.

Protokol WMI so sebou prináša podobné nevýhody, ako v prípade protokolu SSH. WMI je však prevažne určený pre využívanie so systémom Windows čo zjednodušuje jeho využitie a poskytuje jednotnú štruktúru volaní pre rôzne Windows distribúcie.

Všetky spomínané nevýhody vyššie popísaných protokolov, ktoré sa počas analýzy podarilo identifikovať nevnímame ako prekážky pre implementáciu a ich využitie. Skôr je potrebné zabezpečiť vhodný optimalizovaný návrh pri vytváraní metodiky a postupov automatizovaného skenovania siete s využitím týchto protokolov a podľa možností sa čo najviac vyhnúť zisteným obmedzeniam a komplikáciám. Taktiež vychádzame zo skúseností, že tieto manažmentové protokoly sú vo väčšine prípadov organizácií už implementované a využívané, čím sa výrazne zjednodušuje implementácia a využívanie navrhovaného riešenia. Môžeme teda predpokladať, že odpadá potreba rozsiahleho zásahu do infraštruktúry, čo sme v prípade agentových inventarizačných nástrojov a nástrojov správy majetku spomínaných v kapitole 3.2 považovali za značnú nevýhodu. V porovnaní s agentovými inventarizačnými nástrojmi a nástrojmi na správu majetku je možné využiť sieťové protokoly na všetky typy zariadení, a teda ako aj na koncové stanice tak aj na sieťové medziľahlé prvky, čo v prípade inventarizačných nástrojov predstavovalo značné obmedzenie.

Tabuľka 5 znázorňuje porovnanie analyzovaných nástrojov spomenutých v kapitole 3.3.3 a sieťových protokolov na základe definovaných porovnávacích kritérií popísaných

v kapitole 3.3.2. Tabuľka obsahuje vzorku z nášho pohľadu najvhodnejších nástrojov, ktoré je možné využiť v systéme pre proces zhromažďovania informácií o IT aktívach automatizovaným spôsobom.

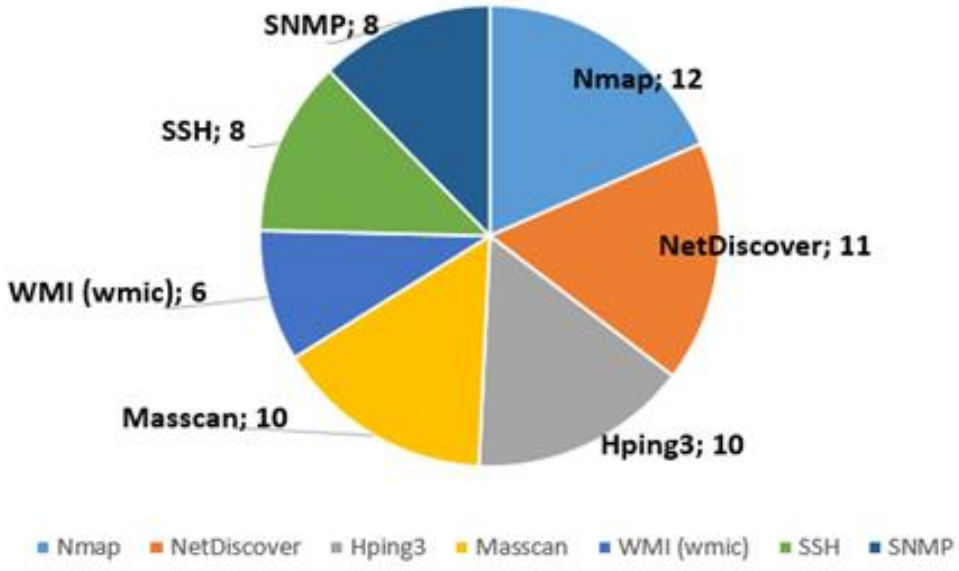
Tabuľka 5 Porovnanie nástrojov pre automatický sken IT aktív

Kritérium/Nástroj	Nmap	Hping3	Netdiscover	Masscan	SSH	SNMP	WMI
Možnosť skenovať celé IP rozsahy adries naraz.	✓	✗	✓	✓	✗	✗	✗
Intuitívne rozhranie nástroja a možnosti jeho využitia.	✓	✓✗	✓	✓	✓	✓	✓
Možnosť formátovať výstupný formát z nástroja (xml, yaml, json a iné).	✓	✗	✗	✓	✗	✗	✗
Jednoduchosť pri používaní nástroja.	✓	✓	✓	✓	✓	✓	✓
Potreba admin práv pre spúšťanie nástroja.	✓✗	✓	✓	✓	--	--	✓
Veľkosť komunity a podpora nástroja.	✓	✓	✓✗	✗	✓	✓	✓
Dostupnosť nástroja (open-source).	✓	✓	✓	✓	✓	✓	✓
Počet zistených informácií z navrhovanej schémy atribútov.	10/24	4/24	3/24	2/24	24/24	24/24	24/24
Rýchlosť skenu pre jedno zariadenie.	2,63s	<1s	nemerateľné	21s-1min	<2s	<2s	<2s
Rýchlosť skenu celej siete	58,57s	--	nemerateľné	1 min –	--	--	--

o veľkosti približne 30 zariadení.				30 min			
Podpora operačného systému Linux.	✓	✓	✓	✓	✓	✓	✓✗
Využitie nástroja pre skenovanie informácií z viacerých OS (Windows, Linux, MacOS).	✓	✓	✓	✓	✓	✓	Windows
Použitie nástroja pre skenovanie informácií o medziľahlých sieťových zariadeniach (smerovač, prepínač, firewall a podobne).	✓	✓	✓	✓	✓	✓	✗
Použitie nástroja pre skenovanie informácií z OS Mikrotik, Cisco, Fortinet, JunOS a iné.	✓	✓	✓	✓	✓	✓	✗
Podpora viacerých funkcionalít (ping, sken otvorených portov, odhad OS, zisťovanie zraniteľností a iné).	✓	✓	✓✗	✗	✗	✗	✗
Náročnosť nástroja na hardvérové prostriedky (CPU, RAM).	<1%	<1%	<1%	<1%	<1%	<1%	<1%
Objem skenovaných dát pre jedno zariadenie.	1,1 kB	1,4 kB	0,06 kB	0,32 kB	--	--	--

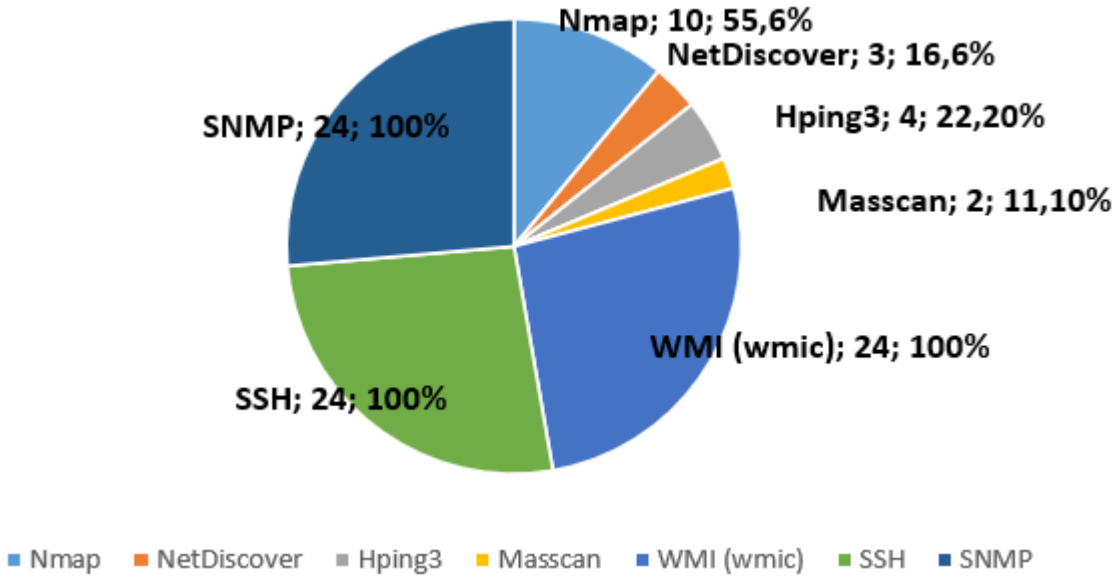
Objem skenovaných dát pre celú sieť o veľkosti približne 30 zariadení.	6,5 kB	--	0,9 kB	4,1 kB	--	--	--

Z porovnávacej analýzy na základe zvolených kritérií vyplynulo, že z pohľadu využívania hotových riešení sa najvhodnejšie pre automatizáciu procesu zberu ukazuje využiť nástroj Nmap. Hlavný dôvod, je ten, že oproti ostatným nástrojom spĺňa najviac porovnávacích kritérií. Porovnanie výsledkov zobrazuje graf na Obrázok 10.



Obrázok 10 Porovnanie nástrojov na základe počtu splnených kritérií

Ak však opomenieme potrebu tvorby nového softvéru skenera, môžeme po zvážení výsledkov konštatovať, že z hľadiska zberu samotných atribútov je najvhodnejšie využitie sieťových protokolov SNMP, SSH a WMI. Dôvodom tejto úvahy je fakt, že v prípade využitia týchto protokolov v novom softvérovom riešení je zaručené 100% pokrytie získavania požadovaných atribútov pre identifikáciu IT aktív a vizualizáciu ich vzájomných vzťahov. Porovnanie výsledkov na základe získavania atribútov aktív, ktoré možno pomocou nástroja získať, znázorňuje graf na Obrázok 11.



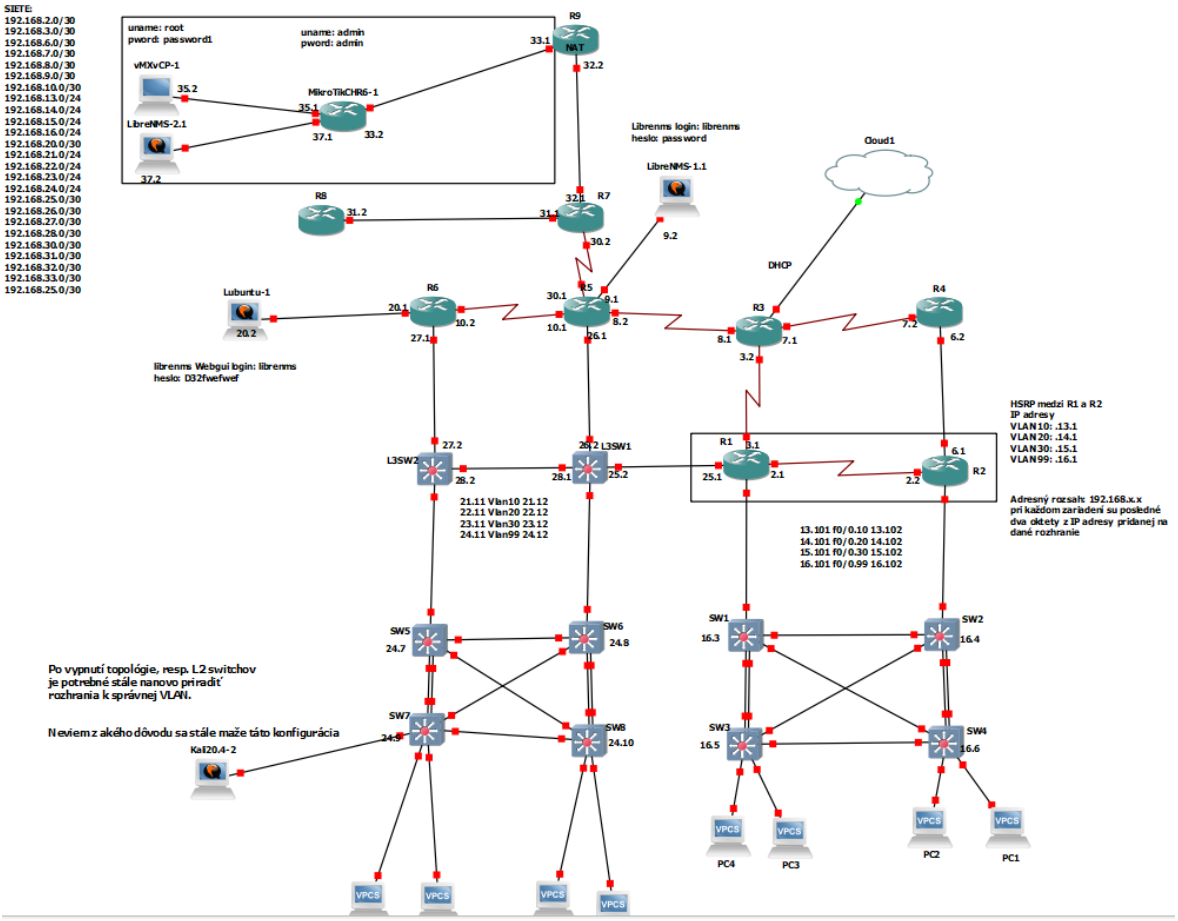
Obrázok 11 Porovnanie nástrojov na základe získavaných atribútov aktív

3.4 Návrh algoritmov skenovania siete

Paralelne s analýzou nástrojov a dostupných riešení sme sa zameriavali aj na rôzne prístupy k ich využitiu v procese skenovania siete a zberu zadefinovaných atribútov aktív. Prvým z prístupov bolo získavanie informácií a skenovanie na princípe tzv. black-box skenu. Black-box skenovanie je forma skenovania, ktorá sa vykonáva bez bližšej znalosti vnútorných častí systému, ako sú napríklad vnútorné štruktúry IKT infraštruktúry alebo autentifikačné údaje pre prístup na zariadenia. S víziou využitia tohto prístupu sme sa snažili zameriavať na riešenia nástrojov, pre ktoré nie je potrebné zadávať a zisťovať dodatočné autentifikačné a autorizačné údaje danej organizácie ako napríklad prihlasovacie údaje. Po analýze sme došli k záverom, že takýto typ zberu atribútov je možný, ale je pomerne časovo náročný a je tak neefektívny z pohľadu skenovania veľkých IKT infraštruktúr a ich služieb, najmä služieb nad protokolom UDP.

Druhým identifikovaným prístupom je tzv. white-box skenovanie s využitím prihlasovacích údajov a sieťových protokolov pre monitorovanie a manažment siete, ktoré zaručujú prístup na manažment rozhrania. Tento prístup má na jednu stranu nevýhodu v časovej náročnosti na počiatočnú inicializáciu a nastavenie celého procesu zberu, avšak v porovnaní výsledkov získaných informácií a náročnosťou na doby zberu je celý proces podstatne rýchlejší a dosahuje presnejšie výsledky ako black-box skenovanie.

Pri druhom prístupe sme na skenovanie siete a získavanie IT aktív zvolili nasledujúce sieťové protokoly. V prostredí IP sieti a koncových systémov je najrozšírenejší protokol SNMP [51] využívaný k jej správe, v prostredí serverových riešení a obzvlášť postavených nad OS Linux je protokol SSH [52], primárne určený k vzdialenému pripájaniu a správe, v prípade zariadení s OS Windows je na to zas určené riešenie WMI [53], kde SSH nie je tak podporovaný. Testovanie týchto prístupov získavania informácií o IT aktívach zo siete prebiehalo na heterogénnej topológii v emulovanom prostredí GNS3 [54] s využitím rôznych sieťových a koncových zariadení bežiacich s Cisco IOS, Linux OS, Mikrotik RouterOS, Juniper JunOS a Microsoft Windows. Testovacia topológia je znázornená na Obrázok 12.



Obrázok 12 Testovacia topológia v emulovanom prostredí GNS3

Po prechode z testovacej emulovanej topológie do reálnej siete sme identifikovali niekoľko nedostatkov druhého prístupu. Hlavný nedostatok je, že v reálnej sieti existujú aj nemanažované zariadenia, na ktorých nie je možné spustiť sieťové protokoly ako SNMP alebo SSH. Okrem takýchto nemanažovateľných zariadení sa v reálnej sieti nachádzajú aj ďalšie implementačné obmedzenia, ako napríklad aplikácia segmentácie a riadených

prístupov pomocou firewallov a pravidiel bezpečnostnej politiky, ktoré môžu obmedzovať presnosť a úspešnosť zberu atribútov zo siete a môžu brániť v dosahovaní presných výsledkov získavania informácií.

Z tohto dôvodu sme sa do finálneho návrhu rozhodli tieto dva prístupy spojiť, a tak aspoň čiastočne eliminovať problémy, ktoré môžu v reálnej prevádzke viesť k nedostatočným výsledkom a poskytnúť neúplné a skreslené informácie ako vstupy do procesu riadenia rizík alebo auditu. Pre implementáciu a otestovanie návrhov sme preto zvolili topológiu zloženú z reálnych zariadení v prostredí Katedry informačných sietí na FRI UNIZA, ktorá je bližšie popísaná v kapitole 3.5. V neposlednom rade proces riadenia rizík, ako aj audit slúži pre samotnú organizáciu za účelom internej identifikácie slabých a zraniteľných miest. To vedie k myšlienke, že v prípade skenovania by nemalo nikdy nastať, že sken neprebehne alebo bude blokovaný. Práve naopak, predpokladáme, že organizácia má vo vlastnej iniciatíve záujem o presné a úplné výsledky, a tak zabezpečí aby celý proces prebiehal bez komplikácií. S prijatím tejto hypotézy sme preto nepokračovali v riešení všetkých možných negatívnych scenárov a problémov, ktoré môžu v sieti nastať. Zamerali sme sa preto na návrh samotných algoritmov automatizovaného zberu atribútov aktív a dátového modelu pre ukladanie získaných informácií.

Nami navrhované algoritmy pre automatizovaný zber atribútov IT aktív počítajú s postupmi, v ktorých využívame viacero nástrojov a protokolov do jedného systému, ktorý vie reagovať na podmienky a obmedzenia v infraštruktúre tak, že zber atribútov sa prispôsobuje spôsobom, kde ak atribút nie je možné získať jedným spôsobom, použije sa záložný. Systém to zabezpečuje zoskupením protokolov SNMP, SSH, WMI a vybratých nástrojov, ktoré dokážu oskenovať otvorené sieťové porty. My sme zvolili nástroj Nmap a to hlavne z dôvodu, že v prvom kroku je nedostatočné oskenovať iba otvorené sieťové porty, ale je potrebné odhadnúť aj operačný systém za účelom vhodne zvoliť volania pri využití zberu atribútov o IT aktívach pomocou sieťových protokolov. Všetky tieto informácie budú nápomocné pre ďalšie kroky skenovania a rozhodovania sa pri voľbe vhodných volaní pre konkrétny typ zariadenia, výrobcu a distribúciu OS.

3.4.1 Algoritmus automatickej identifikácie IT aktív – variant A

Prvý variant nového algoritmu sme postavili na nástroji Nmap s dodatočným zberom nezozbieraných atribútov s využitím možností protokolov SNMP, SSH a WMI.

Postup automatizovaného zberu IT aktív začína prvým krokom zameraným na inicializáciu celého zberného systému, ktorý sa vykonáva len raz pred prvým behom. Tu je potrebné nadefinovať IP adresy, prípadne IP adresné rozsahy jednotlivých lokalít, v ktorých prebehne skenovací proces a zber atribútov IT aktív (oblasť skenu). Okrem definície adresných rozsahov je nevyhnutné definovať autentifikačné údaje umožňujúce vzdialený prístup na zariadenia pomocou protokolov SSH a WMI (OS Windows). Okrem autentifikačných údajov je potrebné pre potreby zberu zadať aj komunitný reťazec (community string) umožňujúci cez protokol SNMP vyčítavať atribúty aktív z MIB SNMP objektov. Aby sme predišli nadmernej záťaži dopytovaných zariadení, eliminovali možnosť detekcie regulárneho skenu ako tzv. brute-force útoku a zároveň optimalizovali vzdialený prístup na jednotlivé zariadenia, tak pre každý typ zariadenia a typ vzdialeného prístupu vytvoríme oddelený zoznam autentifikačných a autorizačných údajov. To znamená, že takéto prihlasovacie údaje je vhodné definovať v separovaných zoznamoch, napríklad nasledovne:

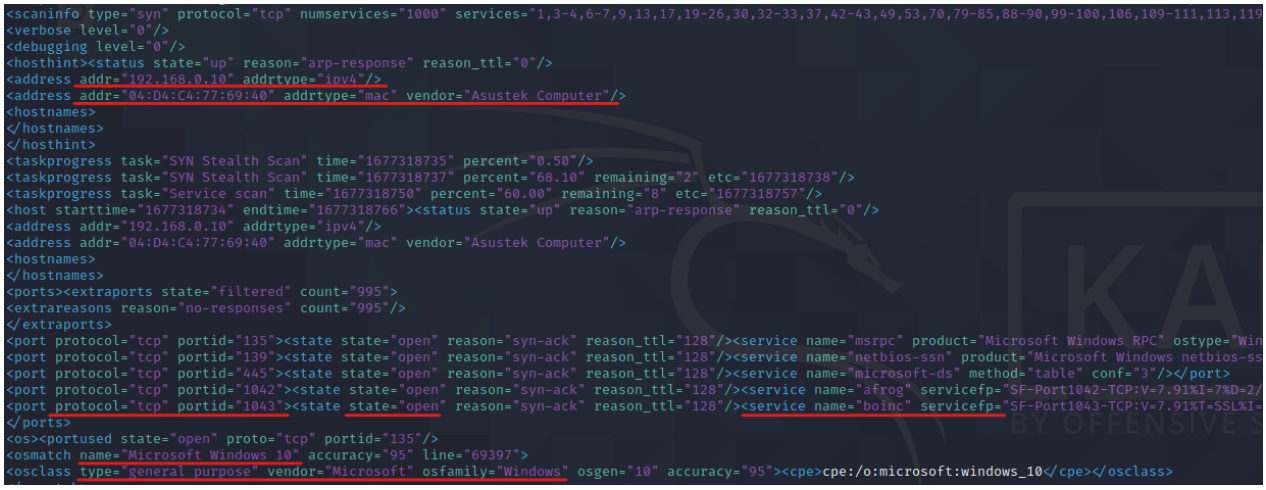
- *SSH_credentials_Servers*,
- *SSH_credentials_Routers*,
- *SSH_credentials_Switches*,
- *SSH_credentials_Firewals*,
- *SNMP_communityString_LocationServers*,
- a podobne.

Po inicializácií systému prebehne v druhom kroku aktívna identifikácia dostupných zariadení v IKT infraštruktúre a zber atribútov aktív podľa nami navrhnutého algoritmu. Nad identifikovanými aktívami je snahou pomocou black-box prístupu získať čo najviac informácií z vyššie definovaných atribútov. Tento hĺbkový zber sa vykonáva bez nutnosti vzdialeného prihlasovania na objavené zariadenia. Za týmto účelom používame nástroj Nmap, ktorý vykoná nami definovanú činnosť nad predkonfigurovanými IP adresnými rozsahmi. Pomocou Nmap-u tak vždy identifikujeme konkrétne IP adresy aktívnych zariadení, na nich otvorené komunikačné porty (TCP/UDP), na daných portoch následne bežiace služby a ich verzie. Nmap nám zároveň umožní získať MAC adresy (v prípade, že skenované zariadenie je na rovnakom segmente ako skenovacie zariadenie), sieťovú masku, výrobcu, model zariadenia, typ OS, typ zariadenia a DNS meno. Spustením Nmap-u pomocou príkazu:

nmap -O -v -sV -sS -sU *<IP adresa alebo IP adresa siete/maska>* **-oX** *<názov výstupného súboru>* dosiahneme požadovaný výsledok, pričom:

- **O:** detekcia operačného systému, jeho verzie,
- **v:** zvýšenie úrovne výpisov,
- **sV:** identifikácia verzie spustenej služby na danom porte,
- **sS:** skenovanie TCP SYP portov,
- **sU:** skenovanie UDP portov,
- **oX:** formátovateľný výstup vo formáte XML.

Ukážka výstupu z nástroja Nmap pre jedno oskenované zariadenie je znázornená na Obrázok 13.



Obrázok 13 Ukážka výstupu z nástroja Nmap

Tretí krok zberu závisí od množstva zozbieraných atribútov z predchádzajúcej činnosti black-box skenu. Na základe jeho výstupov sa vytvorí zoznam IT aktív podľa IP adresy. Aktíva sa následne roztriedia na základe operačného systému, typu zariadenia a zistených otvorených portov pre sieťové protokoly SSH, SNMP, WMI používané pre white-box zber. Pomocou protokolu SSH sa zberný systém následne vzdialene prihlási na tie zariadenia, pre ktoré sa pomocou Nmap nezozbierali všetky údaje a ktoré majú otvorený SSH port. S využitím dostupných autentifikačných údajov z inicializačného kroku sa vyberie na základe typu zariadenia vhodný zoznam prihlasovacích údajov a systém sa pokúsi prihlásiť na zariadenie. Po prihlásení sa na základe zisteného OS využijú jeho natívne výpisy, aby sa získali chýbajúce informácie o danom aktíve. Ukážka takéhoto zberu informácií pomocou protokolu SSH je popísaná nižšie. Pomocou

nasledujúceho príkazu sa systém vzdialene prihlási na zariadenie a získa hardvérové informácie o danom zariadení, pričom autentifikačné údaje *(meno, heslo)* sú získavané zo zoznamu z inicializačnej fázy a na základe zistení z predošlého kroku sa určuje výber vhodných výpisov na základe OS, typu zariadenia a výrobcu:

sshpass -p *<heslo>* **ssh -p** *<ssh port> <meno>@<IP adresa>* '*<echo <sudo heslo>| sudo <natívne volanie pre výpis(napr. sudo -S lshw -short, pre výpis hardvérových informácií na OS Linux)>>*'

V prípade, že nie je dostupná SSH komunikácia tak nasleduje ďalší alternatívny krok, v ktorom sa overí dostupnosť dohľadania chýbajúcich údajov pomocou SNMP alebo WMI. Pre protokol SNMP sme nadefinovali všetky volania potrebné na získanie požadovaných atribútov z verejnej časti SNMP MIB stromu (viď. Obrázok 16). Tento prístup uľahčuje výber vhodných volaní, pretože nie sú závislé od výrobcu, OS alebo typu zariadenia. Ukážku zberu informácií o IT aktíve pomocou protokolu SNMP popisuje nasledujúci príklad. Ak systém identifikoval otvorený UDP port 161 a o danej IP adrese neboli zistené požadované atribúty z predošlých krokov, tak systém použije sériu volaní pre zistenie chýbajúcich informácií. Pre ukážku volania napr. pre zistenie systémových informácií, ako výrobca, model zariadenia, verzia OS zariadenia je možné použiť príkaz:

snmpwalk *<verzia SNMP>* **-c** *<komunity reťazec> <IP adresa> <OID>*

Na Obrázok 14 môžeme vidieť ukážku výpisu, ktorý získame.

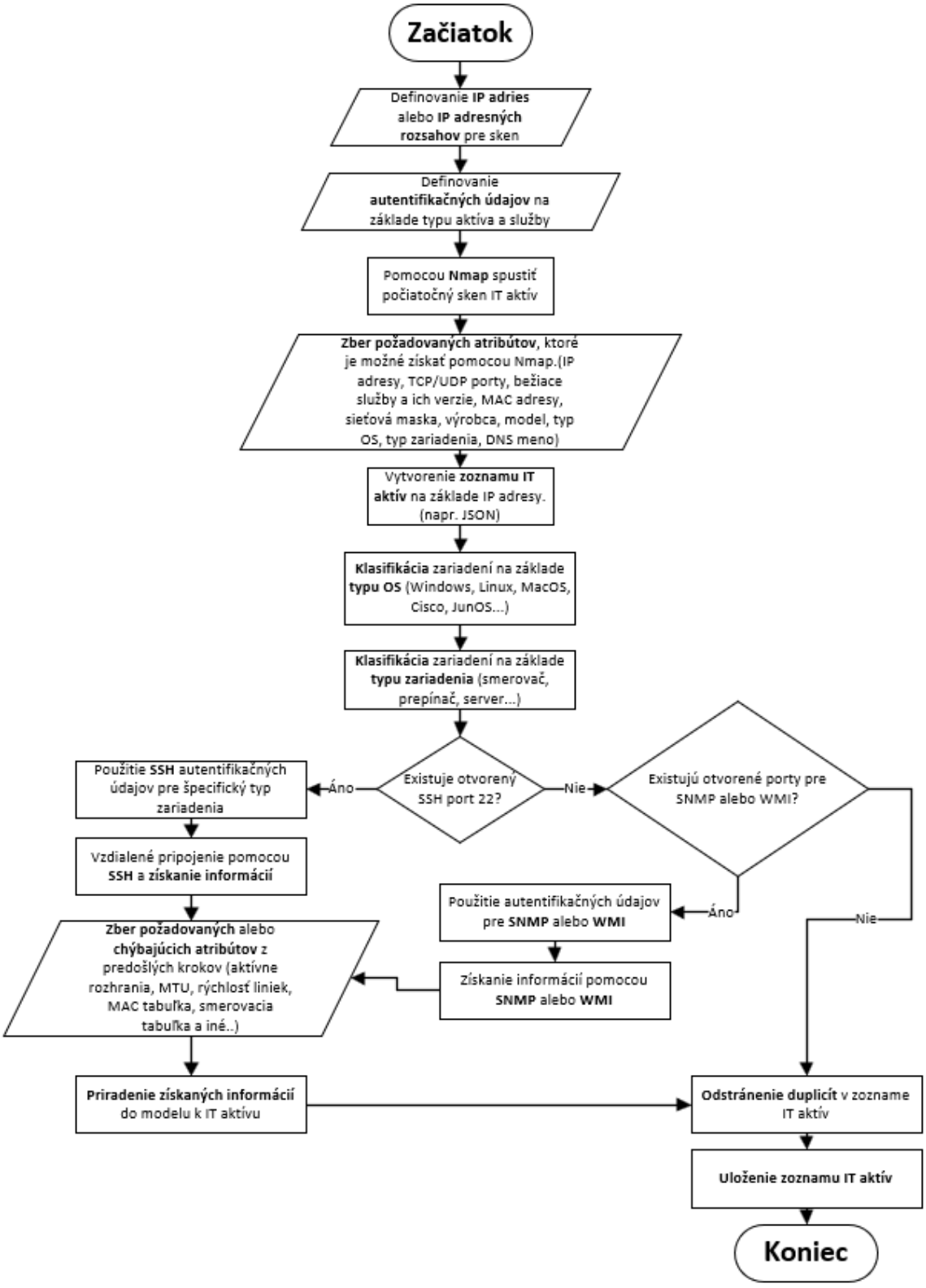
```
┌──(kali㉿kali)-[~]
└─$ snmpget -v2c -c KIS_public 192.168.255.14 1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 15.0(1)SE2, RELEAS
E SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 22-Dec-11 00:16 by prod_rel_team"
```

Obrázok 14 Ukážka zberu informácií pomocou protokolu SNMP

Systém pokračuje vo vykonávaní týchto krokov, kde na základe OS a jeho distribúcie, typu zariadenia a alternatívnej formy zberu informácií získava dodatočné informácie o IT aktívach. Výsledný model algoritmu varianty A v podobe vývojového diagramu je znázornený na Obrázok 15.

Posledným krokom je zoskupenie získaných informácií a vytvorenie modelu IT aktíva ako je znázornené na Obrázok 9, čím sa postupne vytvorí zoznamu IT aktív. Model hardvérového aktíva je vhodné vytvárať a mapovať jednotlivé informácie k sebe priebežne

už počas skenu. Takýmto spôsobom zabezpečíme to, aby sme získali dostatok informácií a vstupov do ďalších podprocesov pre ISMS.



Obrázok 15 Algoritmus automatickej identifikácie IT aktív – variant A

3.4.2 Algoritmus automatickej identifikácie IT aktív – variant B

Druhý navrhovaný variant algoritmu automatickej identifikácie IT aktív je optimalizovanou formou varianty A. Variant B využíva rovnaké nástroje a protokoly ako variant A, takisto rovnako prebieha úvodná inicializácia systému skenovania. To znamená, že je potrebné inicializovať IP adresy alebo adresné rozsahy a taktiež autentifikačné údaje pre vzdialený prístup k službám sieťových protokolov SNMP, SSH a WMI.

Odlišnosť varianty B od algoritmu varianty A je v tom, že sme optimalizovali postupy získavania informácií. Tento prístup bol zvolený z dôvodu zvýšenia efektívnosti a urýchlenia zberu. Na základe testov, diskusie, kritického rozboru problému a zistení sme dospeli k uvedomeniu, že organizácie zväčša majú implementované monitorovacie mechanizmy a manažment IKT infraštruktúry. Na základe tejto hypotézy sme upravili pôvodný algoritmus s predpokladanom rozšírenejšieho modelu správy sietí.

V prvom kroku skenovania, podobne ako pri variante A, sa použije nástroj Nmap pomocou ktorého identifikujeme aktívne zariadenia *(IP adresy)* v sieti a vytvorí sa zoznam týchto aktívnych zariadení. Následne overíme dostupnosť nami používaných manažmentových služieb SNMP, SSH a WMI. Za účelom zrýchlenia algoritmu v tomto prvom kroku predpokladáme, že sú tieto služby spustené na predvolených TCP/UDP portoch 162 (SNMP), 22 (SSH), 135 (WMI). Okrem manažmentových služieb sa počas prvého kroku pomocou nástroja Nmap odhaduje aj typ OS a typ daného skenovaného zariadenia. Presný odhad distribúcie a verzie OS alebo typu zariadenia pomocou Nmap, nie je vždy 100% správny, avšak týmto zistením sme pristúpili k riešeniu tak, že sme nadefinovali generické natívne volania pre protokol SSH, ktoré sú nezávislé od verzie OS ale celkovo závisia iba od typu OS *(Linux, Windows, iOS a podobne)*. Zisťovanie týchto informácií prebieha paralelne so skenovaním otvorených TCP/UDP portov. Keďže základný Nmap sken už priamo poskytuje tieto informácie, v experimentoch sme nezistili vyššiu záťaž systému, ani objem zbieraných dát alebo časovú náročnosť skenu.

Druhý krok algoritmu je získavanie atribútov o oskenovaných IP adresách. Tento krok závisí od predošlého kroku. Systém sa na základe získaných informácií z predošlého kroku o spustených manažmentových službách na jednotlivých IP adresách rozhoduje, ktorý protokol využije na zber informácií. Algoritmus teda ďalej pokračuje podľa toho, aké manažmentové služby boli na danej IP adrese zistené. Algoritmus B totiž preferuje pre získavanie atribútov prednostne protokol SNMP s využitím pridelených komunity reťazcov zabezpečujúcich vyčítavanie MIB objektov (OID). Aby sme sa vyhli potrebe

kategorizovať zariadenia podľa typu a verzie operačného systému, ako aj typu a modelu zariadenia, prispôsobili sme naše SNMP dotazy. Na všetky potrebné atribúty sme využili definíciu všeobecných volaní z verejnej časti SNMP OID stromu. Ukážka definície volaní pre potreby zberu informácií znázorňuje Obrázok 16.

		Atribút	Je možné zistiť pomocu SNMP	formát GET/WALK metódy	OID	Výrobca (cisco, juniper, mikrotik, windows, ubuntu, fortinet)
verejná časť MIB stromu	1	IP adresa	✓	snmpget/snmpwak -v2c -c <komunity retazec> <IP adresa> {OID} snmpget/snmpwalk -<verzia SNMP> -c <komunity retazec> <IP adresa> {OID}	.1.3.6.1.2.1.4.20.1.1	cisco, juniper, mikrotik
	2	otvorené porty	✓		.1.3.6.1.2.1.6.13.1.1 / udp: .1.3.6.1.2.1.7.5.1.2 tcp: .1.3.6.1.2.1.6.13.1.3	juniper (cisco, mikrotik no data available)
	3	spustené služby *(SNMP, SSH, WMI, apache, ...)*	✓		.1.3.6.1.2.1.25.4.2.1.2	no data available
	4	verzie spustených služieb	✗			
	5	aktívne rozhrania	✓		.1.3.6.1.2.1.2.2.1.8	juniper, cisco, mikrotik
	6	IP adresa per rozhranie	✓		.1.3.6.1.2.1.4.20.1.1	juniper, cisco, mikrotik
	7	IP adresa suseda per zariadenie	✗			
	8	rýchlosť liniek	✓		.1.3.6.1.2.1.2.2.1.5	juniper, cisco, mikrotik
	9	MAC adresa	✓		.1.3.6.1.1.1.1.22 / .1.3.6.1.2.1.2.2.1.6	neda sa k nemu dostat
	10	Maska siete	✓		.1.3.6.1.2.1.4.20.1.3	juniper, cisco, mikrotik
	11	značka zariadenia/výrobca	✓		.1.3.6.1.2.1.1.1	juniper, cisco, mikrotik
	12	model zariadenia	✓		.1.3.6.1.2.1.1.1	juniper, cisco, mikrotik
	13	typ OS	✓		.1.3.6.1.2.1.1.1	juniper, cisco, mikrotik
	14	typ zariadenia (router, switch, server, ...)	✓		.1.3.6.1.2.1.1.2 .1.3.6.1.2.1.1.1	juniper, cisco, mikrotik
	15	DNS meno/názov zariadenia	✓		.1.3.6.1.2.1.1.5	juniper, cisco, mikrotik
	16	MTU per interface	✓		.1.3.6.1.2.1.2.2.1.4	juniper, cisco, mikrotik
	17	nainštalovaný SW *(SAP klient, nejaké sieťové služby, ktoré sú len nainštalované ale nie spustené)*	✓		.1.3.6.1.2.1.25.6.3.1.2	juniper (cisco, mikrotik no data available)
privátna časť stromu	18	kapacita - disk, pamäť, CPU...	✓		.1.3.6.1.4.1.43.29.4.1.6	cisco
	19	VLAN	✓		.1.3.6.1.4.1.9.9.46.1.3.1.1.4	cisco
	20	využitie - disk, pamäť, CPU...	✓		.1.3.6.1.4.1.2021.4 .1.3.6.1.4.1.2011.5.25.31.1.1.1.1.5	cisco
verejná časť MIB stromu	21	CDP	✓		1.3.6.1.4.1.9.9.23.1.2.1.1.4	cisco
	22	LLDP	✓		1.0.8802.1.1.2.1.3.7.1.3	cisco
	23	ARP	✓		1.3.6.1.2.1.4.22	cisco
	24	Routing table	✓		1.3.6.1.2.1.4.21.1	cisco
	24	MAC table	✓		1.3.6.1.4.1.9.9.46.1.3.1.1.2 1.3.6.1.2.1.17	cisco

Obrázok 16 Definovanie generických SNMP OID pre potreby zberu atribútov

Týmto prístupom sme zabezpečili získavanie informácií bez ohľadu na výrobcu a model zariadenia, keďže verejnú časť SNMP OID stromu majú implementované všetky manažovateľné zariadenia. Ako je znázornené na predošlom obrázku, niektoré z atribútov *(kapacita a využitie pamäte, disku a procesora alebo číslo virtuálnej LAN siete)* nie je možné získať z verejnej časti SNMP stromu a je potrebné pre tieto atribúty definovať konkrétne OID z privátnej časti SNMP OID stromu pre konkrétneho výrobcu. Postup zberu informácií s využitím protokolu SNMP vykonáva jednotlivé volania sekvenčne, a to práve z dôvodu odstraňovania duplicitných údajov. To znamená, že systém si vyberie zo zoznamu aktívnych IP adries prvú IP adresu, pomocou SNMP zozbiera požadované atribúty pre danú IP adresu a na základe zistených rozhraní a IP adries daného zariadenia, ktorému patrí vybraná IP adresa, odstráni tieto IP adresy zo zoznamu aktívnych IP adries a pokračuje až kým zoznam aktívnych IP adries z prvého kroku nie je prázdny. Paralelne popri zbere informácií sa zbierané atribúty klasifikujú a ukladajú do modelu IT aktíva.

V prípade, že protokol SNMP nebol nájdený alebo neboli zadané správne komunity reťazce nie je možné vyčítať z daného zariadenia požadované atribúty. Pre takéto IP adresy sa overí, či bola identifikovaná dostupnosť cez SSH. Ak áno tak sa použije prístup skenovania s využitím protokolu SSH, ktorý je najkomplexnejší a dodá všetky atribúty, avšak je pomalší a závislý od výrobcu a typu zariadenia, či jeho OS. To má za následok častejšie rozhodovanie v algoritme, a to pri hľadaní správnych autentifikačných údajov a voľbe natívnych výpisov v prípade koncových *(Linux, Windows)* a medziľahlých sieťových zariadení. V tomto prípade sa zopakuje celý postup ako v prípade algoritmu varianty A, kedy prebehne automatizované vzdialené pripojenie s využitím protokolu SSH a pomocou predefinovaných inštrukcií sa podľa typu OS prečítajú požadované chýbajúce atribúty. Zariadenia sa finálne kategorizujú podľa typu a verzie OS, ako aj typu a modelu zariadenia. Na roztriedené zariadenia sa použijú prispôsobené natívne výpisy a príkazy pre zisťovanie informácií z daného typu zariadenia.

V prípade, že v sieti sú identifikované zariadenia s OS Windows pre ktoré neboli nájdené otvorené porty pre SNMP alebo SSH, avšak našiel sa otvorený port pre WMI službu, použijú sa volania definované pre zisťovanie informácií pomocou protokolu WMI. S využitím softvérovej nadstavby wmic pre WMI a použitím definovaných volaní pre WMI sa spúšťajú jednotlivé volania. Definované volania všetkých atribútov pre protokol WMI sú znázornené na Obrázok 17.

Atribút	SELECT
Sysémové informácie zaraidenia	SELECT Name, Caption, , Username, SystemType, Domain, Manufacturer, Model FROM Win32_ComputerSystem
Informácie operačného systému	SELECT BuildNumber, SystemDirectory, Version FROM Win32_OperatingSystem
Hardvérové informácie (procesor)	SELECT DeviceID, Name, Caption, Manufacturer, NumberOfCores, CurrentClockSpeed, MaxClockSpeed FROM Win32_Processor
Hardvérové informácie (disk)	SELECT DeviceID, FreeSpace, Size, VolumeName FROM Win32_LogicalDisk
Sieťové nastavenia	SELECT Description, MACAddress, IPAddress, IPSubnet, DefaultIPGateway, DNSDomain, InterfaceIndex FROM Win32_NetworkAdapterConfiguration SELECT MACAddress, Speed, InterfaceIndex FROM Win32_NetworkAdapter
Nainštalovaný softvér/služby	SELECT Name, Status FROM Win32_Process SELECT Name, State, Satus FROM Win32_Service
Nainštalované aplikácie	SELECT Name, Vendor, Version, Caption FROM Win32_Product
Routing table	SELECT Destination, Mask, NextHop, InterfaecIndex FROM Win32_IP4RouteTable

Obrázok 17 Definovanie WMI volaní pre potreby zberu atribútov

Pre ukážku a zistenie konfiguračných nastavení sieťového adaptéra použijeme príkaz:

wmic --user=<*meno*> **--password=**<*heslo*> //<*IP adresa*> **“SELECT IPAddress, DefaultIPGateway, DNSDomain, Description FROM Win32_NetworkAdapterConfiguration“**

Ukážka kódu pre jednotlivé volania definované pre WMI sú znázornené na Obrázok 18.

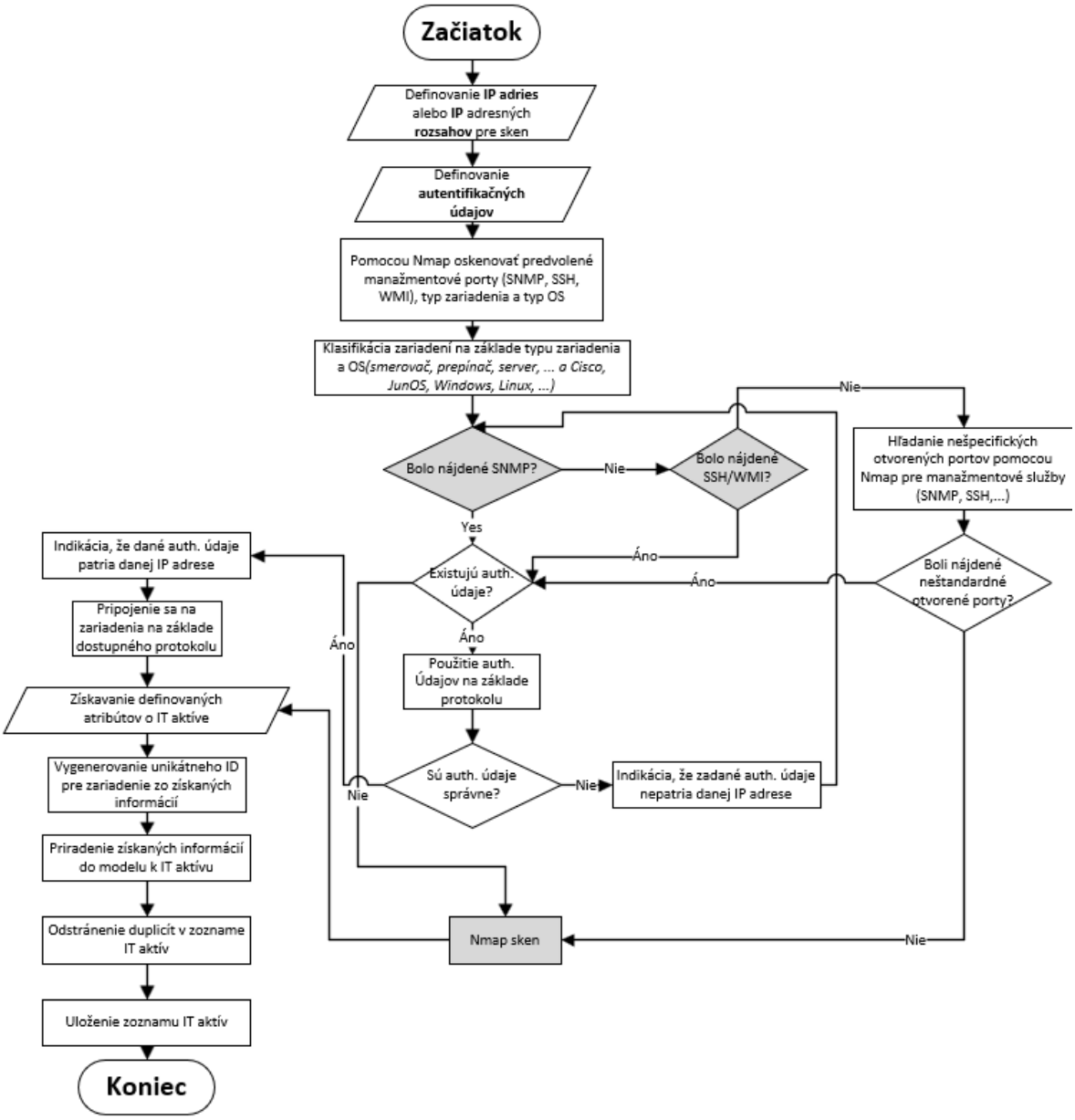
```
wmic = wmi.WmiClientWrapper(
    username=UserName,
    password=Password,
    host=IPAddress,
)

print("--------------------")
print("| COMPUTER SYSTEM |")
print("| INFORMATION     |")
print("--------------------")
#return JSON for DEVICE
ComputerSystem = wmic.query("SELECT Domain, Manufacturer, Model FROM Win32_ComputerSystem")
OperatingSystem = wmic.query("SELECT BuildNumber, SystemDirectory, Version FROM Win32_OperatingSystem")
#reading JSON for DEVICE
for item in ComputerSystem:
    print(
     "Name: {}\nDomain: {}\nManufacturer: {}\nModel: {}"
     .format(item['Name'], item['Domain'], item['Manufacturer'], item['Model'])
    )
for item in OperatingSystem:
    if item['Version'] in ('10.0.22000'):
     print("OS Running: Windows 11")
    if item['Version'] in ('10.0.19044','10.0.19043','10.0.19042','10.0.19041','10.0.18363','10.0.18362'
    '10.0.14393','10.0.10586','10.0.10240'):
     print("OS Running: Windows 10 --- Windows Server(20H2/1909/2004/2016/2019)")
    if item['Version'] in ('6.3.9600','6.3.9200','6.2.9200'):
     print("OS Running: Windows 8 --- Windows Server(2012R2/2012)")
    if item['Version'] in ('6.1.7601','6.1.7600'):
     print("OS Running: Windows 7 --- Windows Server 2008 R2")
    if item['Version'] in ('6.0.6002','6.0.6001','6.0.6000'):
```

Obrázok 18 Ukážka kódu pre zber informácií pomocou WMI

Štvrtý krok prebehne v prípade, že spomenuté manažmentové služby neboli identifikované na predvolených portoch. V tomto prípade sa spustí rozsiahly sken všetkých sieťových TCP a UDP portov všetkých aktívne objavených IP zariadení a zisťuje sa či tieto služby nie sú nasadené na neštandardných portoch. V prípade, že sa tieto služby nájdu spustené na neštandardných portoch, tak sa vykonáva druhý alebo tretí krok, a teda zber údajov s využitím protokolov SNMP, SSH alebo WMI.

V prípade, že nie sú identifikované žiadne manažmentové služby na žiadnom otvorenom porte alebo boli nesprávne zadané autentifikačné údaje a komunity reťazce, tak v piatom kroku sa spustí hĺbkový Nmap sken celej IKT infraštruktúry. Piaty krok tohto algoritmu je totožný ako prvý krok pri variante A. Hĺbkovým Nmap skenom sa systém snaží identifikovať čo najviac informácií o danom zariadení z definovaných atribútov, ako je popísané v prvom kroku algoritmu varianty A.

Posledný krok je pre obe varianty algoritmov rovnaký, a to zoskupenie a uloženie získaných informácií vo vhodnom formáte do dátových štruktúr. Výsledný model algoritmu varianty B v podobe vývojového diagramu je znázornený na Obrázok 19.

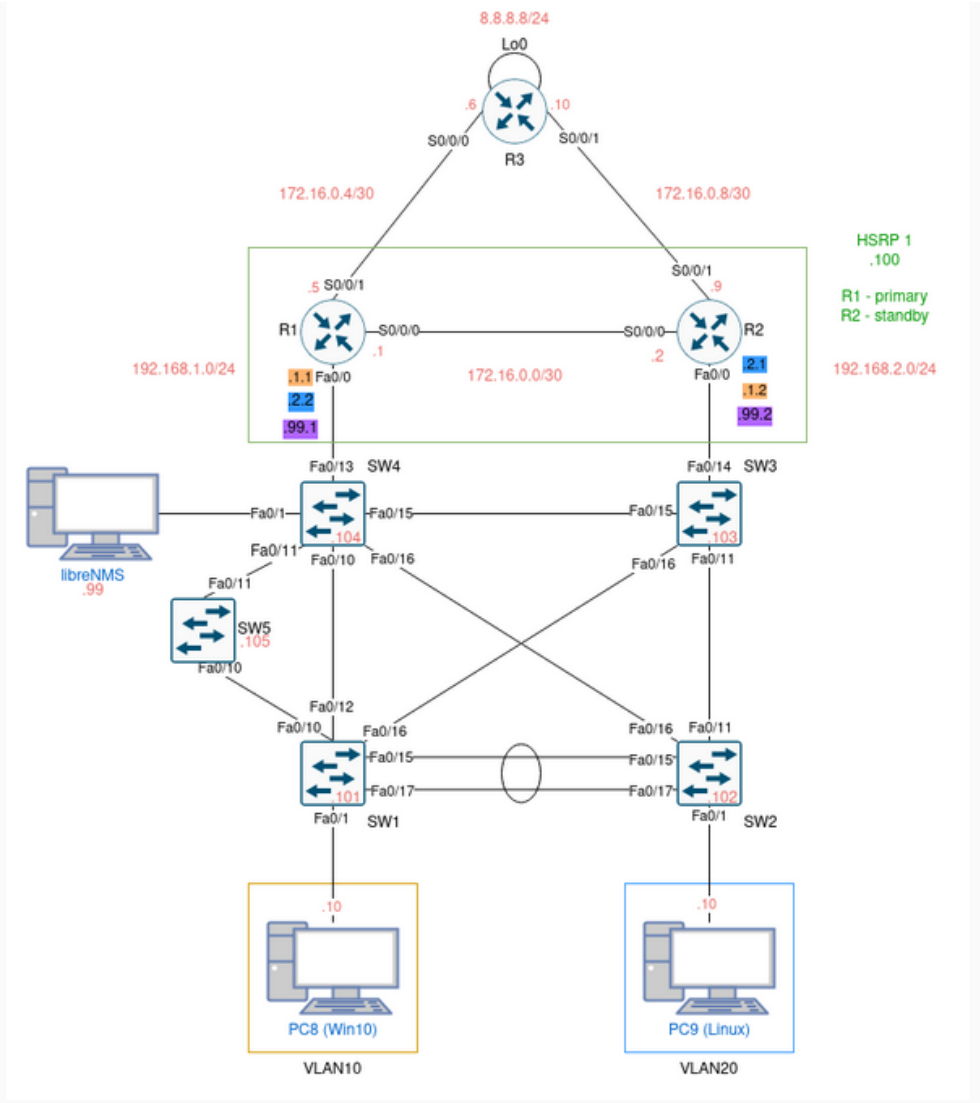


Obrázok 19 Algoritmus automatickej identifikácie IT aktív – variant B

3.5 Porovnanie navrhovaných algoritmov

Ako už bolo v kapitole 3.4 spomenuté, pre potreby implementácie a overenia navrhovaných algoritmov sme upustili od emulovanej topológie v prostredí GNS3 a zvolili sme reálnu topológiu v laboratóriu na Katedre informačných sietí na Fakulte riadenia a informatiky. Testovacia topológia je tvorená z desiatich zariadení od výrobcu Cisco, konkrétne tri smerovače R1, R2, R3 a päť prepínačov SW1, SW2, SW3, SW4 a SW5. Okrem sieťových medziľahlých zariadení sa v topológií nachádzajú aj koncové zariadenia PC8 s OS Windows a PC9 s OS Linux. Všetkým zariadeniam sú nakonfigurované IP

adresy podľa IP adresného návrhu, ktoré je možné vidieť na Obrázok 20. Na všetkých zariadeniach sú nakonfigurované sieťové protokoly SNMP a SSH. V prípade koncového zariadenia PC8 s OS Windows je nakonfigurovaný aj protokol WMI. Návrh testovacej topológie znázorňuje Obrázok 20.



Obrázok 20 Testovacia topológia pre overenie navrhovaných algoritmov

Pri návrhu algoritmov získavania informácií zo siete automatizovaným spôsobom za účelom informačnej bezpečnosti a vizualizácie vzájomných vzťahov primárnych a sekundárnych aktív sme dbali na viaceré aspekty:

- rýchlosť a časová náročnosť zberu údajov,
- hardvérové zaťaženie skenovacieho zariadenia,
- množstvo získavaných údajov,
- množstvo nástrojov potrebných pre získanie výsledkov,

- správnosť zbieraných údajov,
- všeobecnosť nástrojov pre podporu získavania informácií od zariadení širšieho množstva výrobcov,
- jednoduchosť použitia.

Všetky vykonané experimenty a overenie návrhov algoritmov prebiehalo na topológií znázornenej vyššie s využitím totožných sieťových protokolov a konfigurácie celej topológie. Testovanie výkonnosti navrhovaných riešení ako aj samotné experimenty sú riešené v bakalárskych prácach Romana Helisa a Petra Otrubu, ako aj diplomovej práci Dominika Bočka, všetkých troch mnou vedených.

V prípade prvého experimentu a overení algoritmu varianty A sme zistili, že samotný proces skenovania sieťových zariadení s využitím protokolu SNMP trval približne 19 minút na jedno zariadenie. Skenovanie koncového zariadenia s využitím protokolu SSH trvalo približne 3 minúty a s využitím protokolu WMI približne 9 minút. Pri experimente skenovania nemanažovaného zariadenia s využitím nástroja Nmap, trval sken taktiež približne 9 minút. Celkový proces skenovania celej testovacej topológie s využitím algoritmu varianty A trval približne 10485 sekúnd čo sú 2 hodiny a 54 minút. Overenie správnosti zbieraných údajov prebehlo na základe kontroly požadovaných atribútov a získaných údajov po skenovaní v databáze. Pomocou navrhnutého algoritmu sme získali viacero informácií, avšak nastali prípady kedy sme zo zariadení nezískali informácie ako napríklad: nainštalovaný softvér, smerovaciu tabuľku, LLDP tabuľku, dostupné miesto na pevnom disku, prípadne VLAN pre niektoré rozhrania. To môže byť spôsobené tým, že na zariadení bola smerovacia tabuľka prázdna, nebol nakonfigurovaný protokol LLDP alebo volanie pre kapacitu pevného disku nebolo implementované na danom operačnom systéme.

V prípade druhého experimentu a overení algoritmu varianty B sme zistili, že celý skenovací proces testovacej topológie trval približne 1 hodinu a 42 minút. Všetky sieťové zariadenia boli skenované s využitím protokolov SNMP aj SSH. Koncové zariadenia v tomto prípade oskenované neboli, avšak aj napriek tomu môžeme tvrdiť, že s využitím algoritmu varianty B sme urýchlili proces skenovania o približne 1 hodinu a 12 minút. Overenie výsledkov získaných informácií taktiež prebehlo na základe kontroly požadovaných atribútov a získaných informácií po skenovacom procese v databáze. O oskenovaných zariadeniach sme získali všetky požadované informácie okrem verzie

spustených služieb. Nasledujúci Obrázok 21 znázorňuje identifikované zariadenia, ktoré boli použité v testovanej topológií s popisom ich OS, odhadovaného typu, modelu, typu OS a názvu zariadenia.

deviceID	device_name	device_descr	os	estimat	model	os_type
1	R1.public	Cisco IOS Softwar…	Cisco IOS Software	router	(C1841-ADVIP…	Version 15.3(3)XB12
2	roman-Leg…					
3						
4	SW4.public	Cisco IOS Softwar…	Cisco IOS Software	firewall	(C3560-IPSE…	Version 15.0(2)SE8
5	SW5.public	Cisco IOS Softwar…	Cisco IOS Software	firewall	(C3560-IPSE…	Version 15.0(2)SE8
6	SW1.public	Cisco IOS Softwar…	Cisco IOS Software	firewall	(C2960-LANB…	Version 15.0(2)SE8
7	R2.public	Cisco IOS Softwar…	Cisco IOS Software	router	(C1841-ADVIP…	Version 15.3(3)XB12
8						
9	SW2.public	Cisco IOS Softwar…	Cisco IOS Software	switch	(C2960-LANB…	Version 15.0(2)SE11
10	SW3.public	Cisco IOS Softwar…	Cisco IOS Software	switch	(C3560-IPSE…	Version 15.0(2)SE8
11	R3.public	Cisco IOS Softwar…	Cisco IOS Software	router	(C1841-ADVIP…	Version 15.3(3)XB12

Obrázok 21 Zoznam oskenovaných zariadení v testovanej topológií

Informácie ako spustené služby na zariadeniach, otvorené TCP/UDP porty a ARP tabuľka sú znázornené na Obrázok 22 a Obrázok 23.

service_ic	device_id	port	service
1	1	22	ssh
2	1	161	snmp
3	1	162	snmptrap
4	4	22	ssh
5	4	23	telnet
6	4	80	http
7	4	443	https
8	4	4786	smart-install
9	4	161	snmp
10	4	162	snmptrap

Obrázok 22 Tabuľka spustených služieb a otvorených TCP/UDP portov

arp_id	device_id	ip	mac	interface
1	1	192.168.1.1	001a.2f3e.b128	FastEthernet0/0
2	1	192.168.1.5	f875.a4a2.6f66	FastEthernet0/0
3	1	192.168.1.10	1caf.f770.ed2f	FastEthernet0/0
4	1	192.168.1.89	00d8.6109.5b20	FastEthernet0/0
5	4	192.168.1.5	f875.a4a2.6f66	Vlan1
6	4	192.168.1.10	1caf.f770.ed2f	Vlan1
7	4	192.168.1.89	00d8.6109.5b20	Vlan1
8	4	192.168.1.104	9c4e.20ae.3f40	Vlan1
9	5	192.168.1.5	f875.a4a2.6f66	Vlan1
10	5	192.168.1.10	1caf.f770.ed2f	Vlan1
11	5	192.168.1.89	00d8.6109.5b20	Vlan1
12	5	192.168.1.105	0017.9446.ad40	Vlan1
13	6	192.168.1.5	f875.a4a2.6f66	Vlan1
14	6	192.168.1.10	1caf.f770.ed2f	Vlan1
15	6	192.168.1.89	00d8.6109.5b20	Vlan1
16	6	192.168.1.101	001b.53a1.ab40	Vlan1

Obrázok 23 ARP tabuľka zariadení

Získané informácie ako smerovacia tabuľka, ktorá obsahuje cieľovú sieť, prefix danej siete a zariadenie, ktoré smeruje do cieľovej siete je znázornená na Obrázok 24. Tabuľka portov, ktorá obsahuje informácie o rýchlosti liniek, MTU, názve fyzických a virtuálnych rozhraní, typ rozhraní ako aj MAC adresy je znázornená na Obrázok 25.

route_id	device_i	destination	desti	nexthop
1	1	8.8.8.8	32	172.16.0.6
2	1	172.16.0.0	30	0.0.0.0
3	1	172.16.0.1	32	0.0.0.0
4	1	172.16.0.4	30	0.0.0.0
5	1	172.16.0.5	32	0.0.0.0
6	1	172.16.0.8	30	172.16.0.6
7	1	192.168.1.0	24	0.0.0.0
8	1	192.168.1.1	32	0.0.0.0
9	1	192.168.2.0	24	172.16.0.2

Obrázok 24 Smerovacia tabuľka konkrétneho zariadenia

port_ID	device_id	if_name	oper_status	type	mac_address	vlan_id	is_trunk	mtu	speed
1	1	FastEthernet0/0	1	ethernet-csmacd	001a.2f3e.b128	0	2	1500	100000000
2	1	FastEthernet0/1	2	ethernet-csmacd	0x001a2f3eb129	0	2	1500	100000000
3	1	Serial0/0/0	1	propPointToPointS…		0	2	1500	128000
4	1	Serial0/0/1	1	propPointToPointS…		0	2	1500	128000
5	1	FastEthernet0/1/0	2	ethernet-csmacd	0x002290d63517	0	2	1500	100000000
6	1	FastEthernet0/1/1	2	ethernet-csmacd	0x002290d63518	0	2	1500	100000000
7	1	FastEthernet0/1/2	2	ethernet-csmacd	0x002290d63519	0	2	1500	100000000
8	1	FastEthernet0/1/3	2	ethernet-csmacd	0x002290d6351a	0	2	1500	100000000
9	1	Null0	1	other		0	2	1500	4294967295
10	1	Vlan1	2	virtual interface	0x001a2f3eb128	0	2	1500	100000000

Obrázok 25 Tabuľka portov jednotlivých zariadení

Tabuľka obsahujúca CDP/LLDP susedstvá, ktorá obsahuje identifikátor lokálneho a vzdialeného fyzického portu na základe ktorého je vytvorené toto susedstvo je znázornená na Obrázok 26.

relation_id	local_port_id	remote_port_id	active
1	1	24	1
2	3	97	1
3	4	163	1
4	21	79	1
5	22	50	1
6	26	148	1
7	27	121	1
8	49	77	1
9	82	120	1
10	83	149	1
11	84	122	1
12	95	147	1
13	98	164	1
14	116	144	1

Obrázok 26 Tabuľka CDP/LLDP susedstiev

V obidvoch algoritmoch sú využívané rovnaké sieťové protokoly a nástroje, avšak aj napriek tomu je algoritmus variant B rýchlejší a efektívnejší. Dôvodom je práve výber postupnosti využívania jednotlivých protokolov a nástrojov využívaných pri získavaní informácií zo siete automatizovaným spôsobom.

Pri algoritme B sme v prvom kroku skenovania siete odľahčili využitie nástroja Nmap skenovaním iba predvolených portov manažmentových služieb, odhadom OS, zisťovaním typu zariadenia a aktívnych IP adries v sieti. Priemerný čas takéhoto skenu siete o veľkosti desať zariadení trval približne 3-4 minúty. Tento prístup je omnoho rýchlejší ako v prípade algoritmu A, kde sme sa snažili využiť komplexnosť nástroja Nmap. Pôvodne sme kombinovali viaceré prepínače a možnosti nástroja, pomocou ktorých sme sa snažili získať čo najviac požadovaných informácií, čo viedlo k zvýšeniu časovej náročnosti celého skenovacieho procesu. Pri pôvodnom návrhu využitia nástroja Nmap trvalo skenovanie rovnako veľkej siete v priemere desiatky minút.

Rovnako efektívnejší prístup sa osvedčilo využiť protokol SNMP ako primárny zdroj získavania informácií. SNMP volania sú podstatne rýchlejšie ako zisťovanie a skenovanie informácií pomocou Nmap-u alebo vzdialeného prístupu pomocou protokolu SSH.

V prípade, že organizácia má implementované manažmentové protokoly ako SNMP, SSH alebo WMI, úplne sa vyhneme potrebe náročného skenovania zariadení pomocou nástroja Nmap. V prípade, že niektoré zariadenia nie sú zahrnuté do týchto sieťových protokolov, aspoň eliminujeme časovú náročnosť hĺbkového skenovania všetkých zariadení iba na niektoré. Tento prístup podstatne urýchli čas a efektivitu získavania informácií. Aby sme sa vyhli nedostatočným výsledkov v prípadoch kedy v organizácií nie sú implementované všetky požadované manažmentové protokoly, výsledný systém zberu aktív poskytuje aj úpravu výsledkov a je doplnený o manuálne pridávanie IT aktív, pričom pre správne fungovanie je potrebné pri vytváraní aktíva zadať všetky nami požadované atribúty. Rovnako je systém možné nastaviť, aby sa vykonával v určitých časových intervaloch alebo na vyžiadanie, pričom výsledky nových zberov sa porovnávajú s predchádzajúcimi a musia sa akceptovať pred použitím v ďalších podprocesoch. Na základe získaných IT aktív sme teda prešli k návrhu dátového modelu pre ukladanie aktív a vytváranie topologickej mapy, pre vizualizáciu vzájomných vzťahov zozbieraných IT aktív, čomu sa venujú nasledujúce kapitoly.

3.6 Návrh dátového modelu pre ukladanie IT aktív

Po identifikácií IT aktív automatizovaným spôsobom a zistení všetkých definovaných atribútov, ktoré sme definovali v kapitole 3.3.1 je potrebné tieto dáta vhodne uložiť. Keďže v sieti existuje množstvo technológií, ktoré agregujú fyzické linky, umožňujú vytvárať virtuálne rozhrania alebo virtuálne stroje, je nutné dbať na všetky tieto aspekty a zohľadniť ich v dátových štruktúrach. Okrem virtualizácie do tejto kategórie patrí aj cloud computing a privátne cloudové riešenia, ktoré je taktiež potrebné zahrnúť do skenovacieho procesu a vhodne ukladať zistené údaje so zohľadnením virtualizácie a prepojení na fyzické hardvérové prvky.

Ako už bolo v úvode spomínané, nie je možné plne automatizovať procesy ISMS, riadenia rizík ani auditu. Existuje však priestor pre zlepšenie aj tých procesov, ktoré je nutné vykonávať manuálne, a to formou digitalizácie. Ako uvádzajú normy ISO 27xxx, IT aktíva je možné rozdeliť do viacerých skupín:

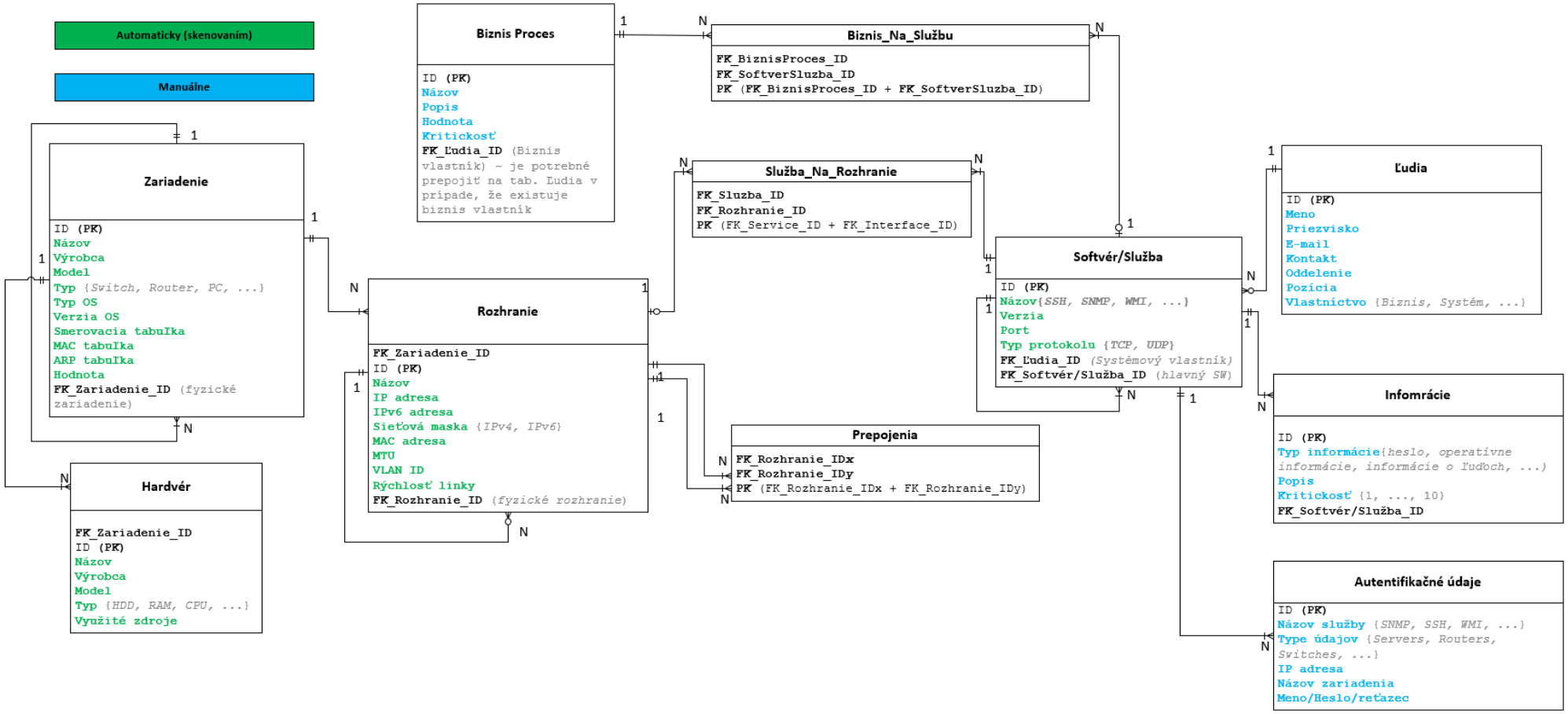
- biznis procesy,
- ľudia,
- aplikácie a databázy,

- informácie,
- IT, komunikačné a ostatné vybavenie,
- infraštruktúra,
- outsourcované služby.

Pri návrhu dátového modelu sme sa preto snažili pokryť všetky tieto skupiny a zakomponovať do nich naše definované atribúty. Dátový model znázorňuje aj rozdelenie získavania informácií či už manuálnym alebo automatizovaným spôsobom. Výsledný dátový model je znázornený na Obrázok 27. V navrhovanom dátovom modely sme pokryli všetky doposiaľ spomenuté podprocesy ISMS, pre ktoré navrhujeme ich zlepšenie alebo automatizáciu, a to:

- identifikáciu organizácie z pohľadu organizačnej štruktúry a identifikácie zainteresovaných ľudských zdrojov,
- popis biznis procesov organizácie, ktoré je potrebné manuálne prepojiť so zozbieranými IT aktívami,
- definícia spracovávaných informácií v biznis procesoch a ich premapovanie na automaticky zozbierané IT aktíva,
- definovanie autentifikačných údajov pre potreby správneho fungovania automatizačných algoritmov pre proces identifikácie IT aktív,
- definovanie dátových štruktúr pre potreby ukladania automatizovane získavaných IT aktív.

Navrhovaný dátový model vychádza z hierarchického modelu skladania a rozkladania IT aktív, ktorý je bližšie popísaný v nasledujúcej kapitole 3.7. Na základe spomínaného hierarchického modelu je možné z časti automatizovať aj proces ohodnocovania IT aktív, a to dedením hodnoty z primárneho aktíva na sekundárne čomu sa venuje nasledujúca kapitola.



Obrázok 27 Dátový model pre ukladanie informácií o IT aktívach

3.7 Ohodnotenie IT aktív

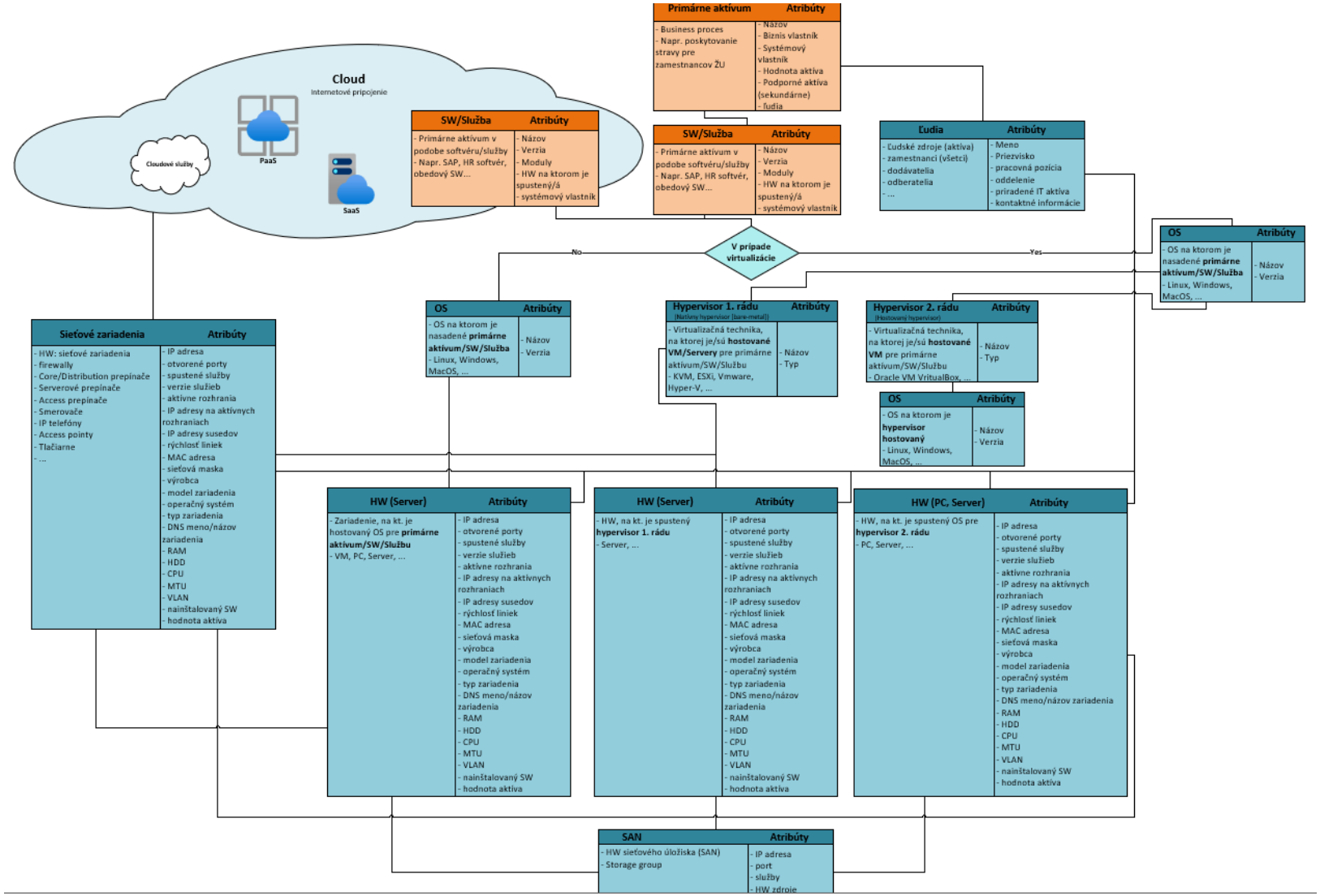
Ďalším podprocesom po identifikácii IT aktív je ich ohodnotenie. Pre tento podproces je potrebné všetkým identifikovaným IT aktívam *(primárnym aj sekundárnym)* priradiť hodnotu na základe ich významnosti pre danú organizáciu.

Norma ISO/IEC 27005 uvádza, že primárnymi aktívami sú informácie alebo obchodné (biznis) procesy a podpornými aktívami sú súvisiace IT systémy, infraštruktúra a ľudské zdroje. My sme si pre výpočet hodnoty IT aktíva upravili vnímanie a pohľad na primárnosť a sekundárnosť aktív, aby sme vedeli automatizovať proces ohodnocovania IT aktív. V našom prípade sme si pojem primárne aktívum rozšírili až na koncovú službu, prípadne koncovú aplikáciu, čiže softvér, ktorý je možné automatizovane oskenovať. Potom podporné *(sekundárne)* aktíva sú všetky tie, ktoré danú službu/aplikáciu podporujú, to znamená všetky IT systémy, infraštruktúra a podobne.

Na základe toho aby sme mohli aspoň z časti automatizovať podproces ohodnocovania IT aktív, sme navrhli a vytvorili hierarchický model skladu/rozkladu IT aktív, pomocou ktorého vieme určiť primárnosť a sekundárnosť aktív. Pomocou tohto hierarchického modelu je možné automatizovať proces ohodnocovania IT aktív. Návrh hierarchického modelu znázorňuje Obrázok 28.

Obrázok znázorňuje hierarchický model ako je primárne aktívum zložené z viacerých podporných/sekundárnych aktív. Koreň modelu je automatizovane oskenované aktívum, čiže softvér, ktoré je potrebné manuálne premapovať na manuálne zadané primárne aktívum *(manuálne zadaný biznis proces)*. Ako už bolo spomenuté, v našom prípade nazývame aj takto automaticky získané aktívum, ako primárne čo v tomto prípade predstavuje konkrétna softvérová služba. Takéto automaticky oskenované primárne aktívum sa potom automaticky mapuje na svoje hardvérové *(sekundárne)* aktíva, na ktorých je softvérová služba nasadená a taktiež na sieťové medziľahlé zariadenia cez ktoré prechádza komunikácia v sieti s touto službou. Na základe týchto mapovaní je možné vytvoriť topologickú mapu (viď. kapitola 3.7.1), ktorá znázorňuje vzájomné vzťahy medzi jednotlivými primárnymi a sekundárnymi aktívami, čo využívame pri ohodnocovaní aktív. Takto vytvorenú cestu, ktorú tvorí primárne aktívum *(softvérová služba)* a jeho podporné aktíva, nazývame aplikačná skupina. Podporné aktíva *(operačný systém, prvky IKT infraštruktúry, koncové zariadenia, a podobne)* na danej ceste nazývame aplikačné

komponenty. Výsledný návrh hierarchického modelu skladania a rozkladania IT aktív na primárne a sekundárne je znázornený na Obrázok 28.



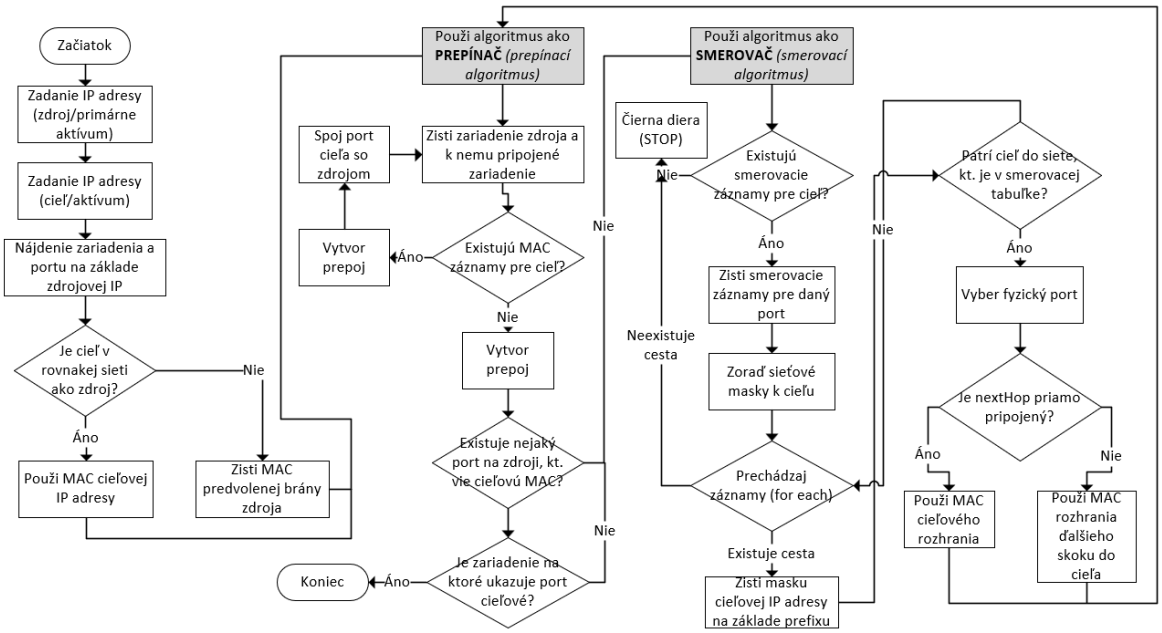
Obrázok 28 Hierarchický model skladu/rozkladu IT aktív

Na základe navrhnutého hierarchického modelu a zozbieraných informácii o IT aktívach, ktoré nám umožňujú vytvárať topologické mapy aktív je možné vizualizovať vzťahy *(vytvárať cesty)* medzi identifikovanými aktívami a automatizovať proces ohodnocovania IT aktív s využitím dedičnosti. To znamená, že manuálne sa ohodnotia iba primárne aktíva *(biznis procesy, prípadne aplikačný softvér)* a všetky podporné aktíva na danej ceste zdedia túto hodnotu. V prípade, že sekundárne/podporné aktívum leží na viacerých cestách a podporuje viacero primárnych aktív, zdedí najvyššiu hodnotu z možných. Ako už bolo popísané v kapitole 1.1.2, existuje viacero metód pre výpočet hodnoty IT aktíva. Keďže z viacerých štúdií (viď. kapitola 1.1.2) vyplýva, že závislosť IT aktív medzi sebou má vplyv na výslednú hodnotu aktíva, považujeme za dôležité na určovanie hodnoty IT aktív využiť práve navrhovaný hierarchický model. Po vytvorení vzájomných súvzťažností primárnych a sekundárnych aktív je potom možné na model aplikovať upravenú metódu výpočtu hodnoty aktíva na základe CIA s ohľadom na ROLFP dopady.

3.7.1 Vytváranie vzájomných súvzťažností IT aktív na základe cesty a topologickej mapy

Nami vypracovaný spôsob pre ohodnocovanie IT aktív vychádza z vytvorenia cesty *(aplikačnej skupiny)* určujúcej vzťah medzi dvomi alebo viacerými primárnymi aktívami a ich podpornými aktívami. Vytváranie cesty sa vykonáva na základe manuálneho vstupu, kde je potrebné definovať zdroj a cieľ tejto vytváranej komunikačnej cesty. Samotná cesta sa následne vytvorí automaticky na základe získaných informácií z predchádzajúceho kroku s využitím zozbieraných smerovacích záznamov, záznamov z MAC a ARP tabuliek, ako aj informácií z CDP/LLDP protokolov o susedských vzťahoch.

Následne sa tejto trase priradí hodnota, na základe manuálne zadanej hodnoty pre primárne aktívum a vybraného zdroja/cieľa, ktorá predstavuje hodnotu primárneho aktíva. Všetky sekundárne *(podporné)* aktíva na tejto ceste zdedia túto hodnotu. V prípade, že nastane situácia, keď cez podporné aktívum prechádza viacero ciest medzi viacerými primárnymi aktívami, tak aktívum zdedí najvyššiu *(maximálnu)* hodnotu cesty. Z dôvodu, že dané aktívum je sekundárne *(podporné)* aktívum pre viacero primárnych aktív *(procesov)*, stáva sa z neho kritické aktívum a jeho hodnota by preto mala odzrkadľovať túto skutočnosť.



Obrázok 29 Algoritmus pre vytváranie cesty vzájomných vzťahov IT aktív

Vytváranie komunikačnej cesty medzi aktívami prebieha na základe pravidiel, ktoré sa využívajú v sieťovej komunikácií a na základe zistených doplnkových informácií zisťovaných v procese automatickej identifikácie aktív a zberu ich atribútov vykonávaných podľa algoritmov z predošlej kapitoly. Pre vytvorenie cesty medzi definovanými aktívami sa použije nami vypracovaný algoritmus, ktorý je znázornený na Obrázok 29.

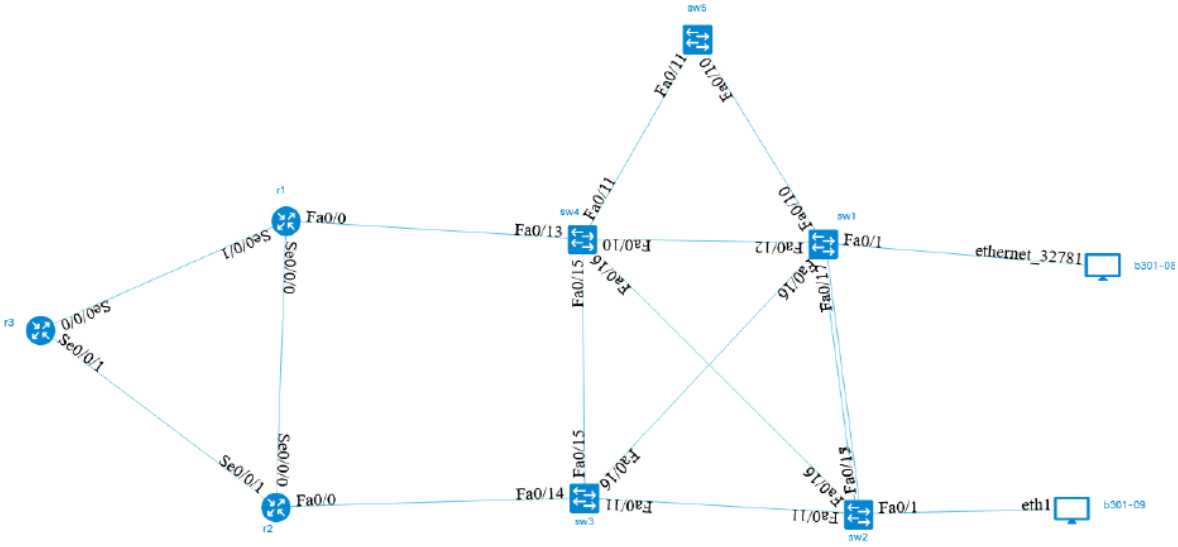
Algoritmus je postavený na pravidlách, ktoré sú bežne využívané v IP sieťovej prevádzke a komunikácii. Cesta a vizualizácia vzájomných vzťahov sa tak vytvára na základe zistených informácii o IT aktívach. Informácie potrebné pre vytvorenie cesty sú MAC tabuľky, ARP tabuľky, smerovacie záznamy jednotlivých aktív, CDP/LLDP tabuľky, IP adresy jednotlivých rozhraní, maska siete a MAC adresy rozhraní.

Inicializácia celého algoritmu pre vytváranie cesty spočíva v manuálnom zadaní IP adresy zdroja cesty a IP adresy cieľa cesty. Pod zdrojom a cieľom si môžeme predstaviť dve primárne aktíva alebo zdroj ako primárne aktívum a cieľ ako sekundárne aktívum.

Na základe IP adresy zadaného zdroja sa v zozname zozbieraných IT aktív nájde zariadenie, ktorému patrí daná IP adresa a rozhranie, ktoré ma nakonfigurovanú danú IP adresu. Na základe IP adresy cieľa sa prejde k rozhodovaciemu procesu a na základe IP adresy a masky siete sa zisťuje či adresa cieľa patrí do rovnakej siete ako zdrojová IP adresa. V prípade, že cieľová adresa je z rovnakej siete ako zdrojová IP adresa, prejde sa k tzv. prepínaciemu alebo L2 algoritmu. Tu sa použijú záznamy z ARP tabuľky, zistí sa

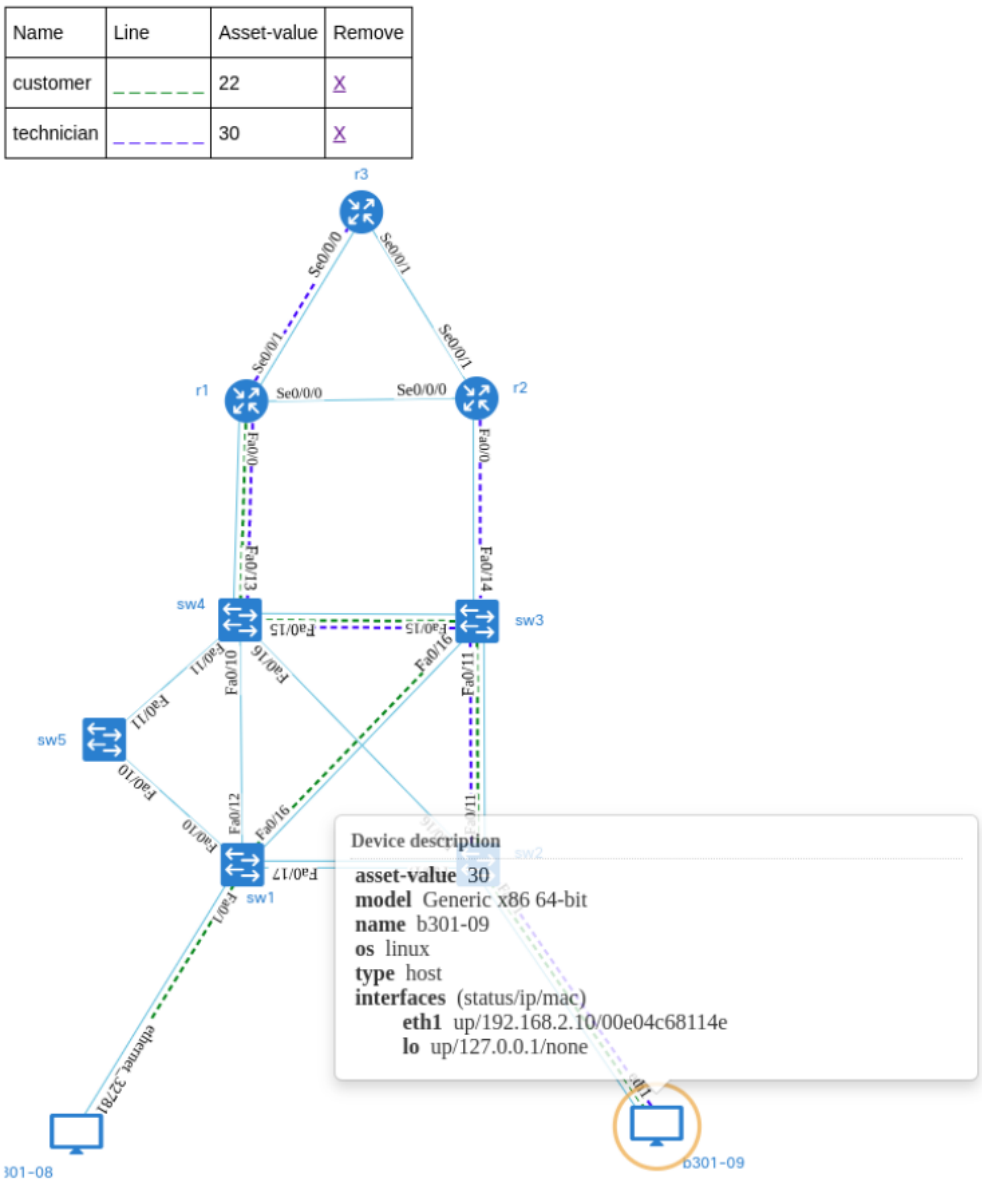
MAC adresa cieľa a v zozname IT aktív sa nájde zariadenie, ktoré má v MAC tabuľke záznam o MAC adrese cieľa, pričom sa kontroluje či vytvorením prepojenia sa končí na koncovom zariadení, alebo ešte existuje zariadenie medzi nimi. Tento proces *prepínacieho* algoritmu sa opakuje, kým sa neidentifikuje cieľové zariadenie a algoritmus končí. V prípade, že cieľová IP adresa nie je z rovnakej siete ako zdrojová IP adresa, na zdrojovom zariadení sa zistí IP adresa predvolenej brány a jej MAC adresa. Znova sa prechádza k *prepínaciemu* algoritmu a zisťujú sa zariadenia, ktoré majú záznamy v MAC tabuľkách o predvolenej bráne. Po vytvorení cesty od zdroja k predvolenej bráne na základe rovnakej logiky ako je popisovaná vyššie, sa prechádza k *smerovaciemu* algoritmu. Na zariadení, ktoré predstavuje predvolenú bránu sa hľadajú smerovacie záznamy, ktoré ukazujú na cieľovú IP adresu. Identifikuje sa sieť, do ktorej patrí cieľová IP adresa na základe sieťovej masky, a v prípade, že existuje záznam pre danú IP adresu, zistí sa výstupné rozhranie a overuje sa či ďalšie zariadenie je cieľové alebo je medzi nimi nejaké ďalšie zariadenie. V prípade, že cieľové zariadenie je priamo pripojené, použije sa MAC adresa cieľa na základe ARP záznamov a vráti sa na prepínací algoritmus, ktorý na základe popisovanej logiky vytvorí cestu k cieľu. V prípade, že cieľové zariadenie nie je priamo pripojené na zariadenie, ktoré predstavuje predvolenú bránu, použije sa MAC adresa ďalšieho zariadenia na ktoré poukazuje smerovací záznam a znova sa opakuje prepínací algoritmus, prípadne smerovací algoritmus ak stále nie je cieľové zariadenie na dosah. Algoritmus končí vždy prepínacím algoritmom.

V prípade, že sa v smerovacích záznamoch nenájde záznam o cieľovej sieti do ktorej patrí cieľová IP adresa zariadenia, vytvorí sa generické rozhranie na zariadení po ktoré sa algoritmus dostal a následne sa vytvorí generické zariadenie na ktoré sa pripojí cieľové zariadenie. Tento prístup sme zvolili z dôvodu, aby sme mali spojitý graf pre znázornenie vzájomných vzťahov IT aktív. Pre takéto umelo vytvorené generické prepojenia a zariadenia existuje možnosť ich úpravy a manuálneho dodefinovania potrebných informácií alebo pripojenia k reálnym zariadeniam. Overenie navrhovaného algoritmu, ako aj jeho implementácia je podrobne riešená v bakalárskej práci Romana Ďurajku vypracovanej pod mojím vedením. Overenie prebiehalo taktiež na testovacej topológii (viď. Obrázok 20) na KIS FRI UNIZA. Nasledujúci Obrázok 30 znázorňuje vytvorenú topologickú mapu, ktorá je tvorená na základe získaných údajov zo skenovacieho procesu, konkrétne z informácií získaných z CDP/LLDP tabuliek.



Obrázok 30 Graf vytvorenej topologickej mapy na základe oskenovaných informácií

Po porovnaní jednotlivých topologických grafov môžeme vidieť, že vytváranie vzájomných väzieb medzi zariadeniami prebehlo správne a vykreslenie výslednej topológie je podľa zostrojenej testovacej topológie. Môžeme teda konštatovať, že protokoly CDP/LLDP nám poskytli dostatočné informácie o vzájomných väzbách pre vizualizáciu susedských vzťahov jednotlivých zariadení pre ich grafické znázornenie do topologickej mapy. Obrázok 31 znázorňuje overenie riešenia navrhovaného algoritmu pre vytváranie komunikačnej cesty. Na obrázku môžeme vidieť vytvorenú topologickú mapu, v ktorej sú vykreslené komunikačné cesty medzi vybranými zariadeniami. Navrhovaný algoritmus a využívanie prepínacích a smerovacích záznamov získaných zo skenovacieho procesu sa ukázalo ako vhodné riešenie pri vytváraní takýchto komunikačných ciest. Proces vytvárania komunikačnej cesty, ktorá znázorňuje vzájomné vzťahy primárnych a sekundárnych aktív sa vytvára pomocou navrhnutého algoritmu na základe manuálne zadaných vstupov IP adries zdroja a cieľa. Takýchto ciest môže byť v topologickej mape vykreslených viacero, na základe počtu primárnych aktív, ktoré sa zobrazia v tabuľke ciest. Na základe takto vytvorených komunikačných ciest v topologickej mape je možné automatizovať aj ďalší proces, a to ohodnotenie IT aktív. Na základe dedenia hodnoty z primárneho aktíva na sekundárne *(podporné)* aktíva je možné proces automatizovať, a to tým, že sa ohodnotí cesta *(business proces)*, ktorá predstavuje komunikáciu primárneho aktíva a všetky podporné aktíva na danej ceste túto hodnotu zdedia. Obrázok 31 znázorňuje aj dedenie hodnoty aktíva *(asset-value)*, kde na základe zvolenej hodnoty cesty sa táto hodnota pretransformuje aj do hodnoty podporného aktíva, čo je vidieť v popise zariadenia na obrázku.



Obrázok 31 Graf topologickej mapy s vytvorenými komunikačnými cestami

Takto vytvorené cesty nazývame v tejto práci ako **aplikačné skupiny**, ktoré sú tvorené komponentami aplikačnej skupiny a predstavujú vstup pre podproces ohodnocovania aktív čomu sa venuje nasledujúca podkapitola.

3.7.2 Návrh metódy pre výpočet hodnoty aktíva

Keďže vychádzame z tvrdenia, že hodnota primárneho aktíva závisí od závislostí jednotlivých aktív, navrhujeme zjednodušenie podprocesu ohodnocovania IT aktív v podobe hodnotenia iba primárnych aktív, pričom táto hodnota sa prenesie (zdedí) na všetky podporné aktíva na vytvorenej ceste. To znamená, že všetky komponenty aplikačnej skupiny zdedia hodnotu celej aplikačnej skupiny do ktorej patria. V prípade, že patria do viacerých aplikačných skupín, zdedia vždy vyššiu hodnotu aplikačnej skupiny do ktorej

patria. V našom prípade sú primárne aktíva aplikácie, prípadne služby, ktoré bežia na koncových staniciach, spracovávajú informácie a priamo podporujú biznis proces.

Na výpočet výslednej hodnoty primárneho aktíva sme zvolili metódu výpočtu pomocou dopadov na tri základné aspekty informačnej bezpečnosti a to dôvernosť, integritu a dostupnosť (CIA) s ohľadom na reputačné, finančné, operatívne, právne a ľudské (ROLFP) vplyvy. Ako základ pre náš prístup sme zvolili metódu, ktorá je popísaná pre nástroj Monarc [55]. Tento nástroj je tvorený na základe metód, ktoré vychádzajú zo štandardu ISO/IEC 27005. Ako popisujú autori tohto nástroja, metóda výpočtu hodnoty aktíva pre Monarc je kvalitatívna metóda založená na ISO/IEC 27005 z dôvodu jej jednoduchosti pre pochopenie, najmä pre nehmotné kritéria z hľadiska dopadu a dôsledkov. Monarc pre vyčíslenie výslednej hodnoty aktíva pre CIA aspekty používa funkciu maxima v dvojrozmernej matici hodnôt definovaných tromi riadkami (tri CIA aspekty) a piatimi stĺpcami (ROLFP) (viď. Tabuľka 6). Vyčíslenie jednotlivých dopadov na CIA sa vykonáva manuálne, na stupnici od 0-4, pričom:

- 0 – žiadne následky,
- 1 – mierne následky,
- 2 – stredné následky,
- 3 – veľké následky,
- 4 – devastujúce následky.

Na vyčíslenie výslednej hodnoty aktíva sa použije funkcia maximum, pričom sa vyberá z vplyvov ROLFP na dopady CIA, kde:

$\boldsymbol{A_v}$ – hodnota aktíva,

MAX() – funkcia maxima,

CIA – dôvernosť/integrita/dostupnosť,

ROLFP – vplyv na CIA z pohľadu reputácie/operatívy/zákonov/financií/ľudí,

X – hodnota,

V – matica hodnôt CIA na základe ROLFP.

$$I = \{C, I, A\};\ J = \{R, O, L, F, P\};\ V = \{V_{ij}\ ; i \in I, j\ \in J\}$$

$$V = \begin{pmatrix} C \\ I \\ A \end{pmatrix} . \left(X_R X_0 X_L X_F X_p\right) \quad (1)$$

$$C = MAX\left(V_{Cj}\right) \quad (2)$$

$$I = MAX\left(V_{Ij}\right) \quad (3)$$

$$A = MAX\left(V_{Aj}\right) \quad (4)$$

$$A_v = [C, I, A]$$

Pre znázornenie výpočtu si uvedieme príklad, ktorý je popísaný v Tabuľka 6. Ako ukážku si predstavme aktívum, pre ktoré sme v tabuľke zadefinovali jednotlivé hodnoty pre dopady na aspekty bezpečnosti CIA z pohľadu ROLFP.

Tabuľka 6 Výpočet hodnoty aktíva podľa metódy Monarc

CIA/ROLFP	Reputácia (**R**)	Operatíva (**O**)	Právo (**L**)	Financie (**F**)	Ľudia (**P**)
C	2	0	1	4	2
I	2	3	3	1	1
A	2	4	0	2	0

Potom na základe tejto tabuľky sa vypočíta hodnota aktíva, ktorá na výpočet výslednej hodnoty využíva funkciu maxima. Výpočet výslednej hodnoty aktíva je nasledovný:

$C = MAX(2,0,1,4,2) = 4$

$I = MAX(2,3,3,1,1) = 3$

$A = MAX(2,4,0,2,0) = 4$

$\boldsymbol{A_V = [4, 3, 4]}$

Popísaná metóda počíta vždy s najhorším scenárom a dopadom pri výpočte hodnoty maxima, avšak pri využití funkcie maxima neberie do úvahy všetky dopady ROLFP ako pôsobia na aspekty CIA. Z uvedeného dôvodu sa nám javí nevhodné využívať funkciu maxima pre výpočet výslednej hodnoty aktíva. Použitá metóda môže udávať skreslené hodnoty v prípade veľkých rozptylov hodnôt, nakoľko funkcia vždy zvolí maximum. To môže viesť ku skresleniu výslednej hodnoty aktíva. Keďže v procese zmierňovania rizík sa primárne zmierňujú riziká pre najhodnotnejšie a najrizikovejšie aktíva a celkové riziko

závisí aj od hodnoty aktíva, práve pri tomto rozhodovaní môže nastať skreslený pohľad na potrebu zmierňovania rizík nesprávnym aktívam, ktoré môžu mať pre organizáciu v skutočnosti nižšiu hodnotu ako indikuje metóda.

Na základe týchto poznatkov sme sa snažili nájsť vhodnejší spôsob výpočtu výslednej hodnoty aktív a vyhladiť tak výslednú hodnotu IT aktíva pri veľkom rozptyle medzi jednotlivými hodnotami ROLFP.

Ako prvé sme skúšali výslednú hodnotu vypočítať pomocou aritmetického priemeru. Na základe príkladu z Tabuľka 6 s využitím priemeru je výsledná hodnota aktíva:

$$C, I, A = \frac{\sum X_i}{5} \qquad (5)$$

$$A_v = [C, I, A]$$

$$C = \frac{9}{5} = 1{,}8 \gg zaokrúhlime\ na\ najbližšiu\ vyššiu\ hodnotu => 2$$

$$I = \frac{10}{5} = 2$$

$$A = \frac{8}{5} = 1{,}6 \gg zaokrúhlime\ na\ najbližšiu\ vyššiu\ hodnotu => 2$$

$$\boldsymbol{A_v = [2, 2, 2]}$$

Tento prístup taktiež nepovažujeme za vhodný a to presne z opačného dôvodu, ako to bolo pri využití funkcie maxima. Ak si porovnáme hodnoty dopadov v tabuľke a výslednú hodnotu aktíva, vidíme, že výsledná hodnota pre dostupnosť (A) je výrazne nižšia. To by v procese zmierňovania rizík mohlo mať za následok zanedbanie potreby zmierňovania rizík pre dostupnosť tohto aktíva.

Skúmaním viacerých možností a metód výpočtu výslednej hodnoty aktíva sme dospeli k záveru, že najvhodnejšie bude skombinovať tieto dva prístupy dokopy. Pre výpočet hodnoty aktíva teda navrhujeme využiť aj funkciu priemeru aj funkciu maxima a výsledné hodnoty spriemerovať. Na základe príkladu z Tabuľka 6 s využitím tejto metódy je výsledná hodnota aktíva:

$$Maximum \rightarrow A_v = [4{,}3{,}4]$$

$$Priemer \rightarrow A_v = [2, 2, 2]$$

$$C, I, A = \frac{A_v MAX_i + A_v AVG_i}{2} \qquad (6)$$

$$C = \frac{4+2}{2} = 3$$

$$I = \frac{5}{2} = 2{,}5 \gg zaokrúhlime\ na\ najbližšiu\ vyššiu\ hodnotu => 3$$

$$A = \frac{6}{2} = 3$$

Výsledná hodnota aktíva potom bude

$$\boldsymbol{A_v} = [\mathbf{3}, \mathbf{3}, \mathbf{3}]$$

Využitím tejto metódy pre výpočet výslednej hodnoty aktíva dosiahneme vyhladenú hodnotu pri veľkých rozptyloch medzi jednotlivými hodnotami ROLFP. Výsledkom využitia tejto metódy je, že sa zníži riziko skreslených výpočtov a zefektívni sa pohľad na hodnotu jednotlivých aktív pri procese zmierňovania rizík. Okrem návrhu metódy presnejšieho výpočtu hodnoty aktíva navrhujeme výslednú hodnotu prenásobiť váhou daného oddelenia organizácie, ktorému aktívum patrí. Váhu oddeleniu by mal určovať top manažment organizácie v procese vytvárania kontextu a organizačnej štruktúry organizácie, ako je popísané v kapitole 3.1.3. Zmysel váhovania jednotlivých oddelení taktiež spočíva v rozhodovacom a dokazovacom procese použitom pri zmierňovaní rizík tak, aby organizácia vhodne navrhla prioritizáciu riešenia jednotlivých nápravných opatrení pri zmierňovaní rizík a vhodne vyčlenila potrebné zdroje na ich implementáciu.

3.8 Riadenie rizík

Ďalšia oblasť riešenia práce sa venovala možnostiam automatizácie procesov riadenia rizík informačnej bezpečnosti. Pre riadenie rizík sme identifikovali viaceré možnosti automatizácie a to:

- identifikáciu zraniteľností,
- identifikáciu hrozieb,
- výpočet hodnoty rizika,
- návrh odporúčaní pre zníženie rizika,
- návrh simulácií pre predikciu zmeny rizika.

Pri návrhu automatizácie jednotlivých podprocesov sme vychádzali z analýzy viacerých štúdií, ktoré pokrývajú danú oblasť [56]. Analyzovali sme dostupnú literatúru a normy pre identifikáciu zraniteľností a hrozieb, ako aj výpočet hodnoty rizika IT aktív. Skúmali sme dostupné riešenia a analyzovali rôzne nástroje [57][43][41], ktoré pokrývajú oblasť riadenia rizík.

Výsledkom analýzy dostupných nástrojov pre riadenie rizík, ktoré sú popísané v kapitole 3.2.2 bolo zistenie, že viaceré z nástrojov z nášho pohľadu nedostatočne pristupujú k identifikácií zraniteľností a hrozieb pre IT aktíva. Pre proces identifikácie zraniteľností a hrozieb poskytujú iba manuálny vstup od používateľov, ktorý si na základe vlastných skúseností musia identifikovať zraniteľnosti a hrozby alebo nástroje poskytujú len preddefinovaný zoznam zraniteľností alebo hrozieb, ktoré je potrebné manuálne priradiť danému aktívu taktiež na základe vlastného uváženia. Tento prístup je odzrkadlenie toho, ako informácie o zraniteľnostiach a hrozbách poskytujú normy alebo verejné katalógy hrozieb spomenuté v kapitole 1.2. My navrhujeme využiť podobný prístup ako popisuje norma ISO/IEC 27005 a s využitím kategorizácie aktív na základe normy ISO/IEC 27005 namapovať všeobecné riziká a hrozby k daným aktívam z viacerých zdrojov či už vytvorením vlastnej databázy na základe dostupných katalógov zraniteľností a hrozieb, alebo online pomocou otvorených API rozhraní dostupných databáz.

V ďalšej časti tejto kapitoly sa venujeme návrhom výpočtu celkového rizika tak, aby bolo možné vytvárať simulácie dopadov, pomocou ktorých vieme predikovať zmenu rizika pri implementácií vybraných opatrení. Koniec kapitoly je venovaný návrhom jednotlivých simulácií, ako aj popisu prínosu tohto princípu pre proces dokazovania potreby implementácie vybraných opatrení pred manažmentom spoločnosti a vyčlenení prostriedkov pre implementáciu vybraných nápravných opatrení na znižovanie rizika.

3.8.1 Automatizovaná identifikácia zraniteľností a hrozieb

Proces identifikácie zraniteľností a hrozieb je individuálny proces, ktorý závisí od druhu organizácie a od úrovne implementovaného ISRM v danej organizácii. Z tohto vyplýva, že nie je možné plne automatizovať tento podproces z dôvodu, že organizácia už môže mať implementované určité opatrenia na zmiernenie rizík. Aj napriek uvedomeniu si tohto faktu si myslíme, že rovnako ako v predošlých procesoch, aj v podprocese identifikácie zraniteľností a hrozieb vidíme priestor pre jeho čiastočné zlepšenie. Zlepšenie vidíme v čiastočnej automatizácií tohto procesu, vytvorením vlastnej alebo s využitím

dostupných databáz zraniteľností a hrozieb, ktoré na základe kategórie aktíva automaticky priradia aktívu zraniteľnosť, prípadne priradia zraniteľnosti hrozbu. Manuálnou úpravou by si tak používatelia systému vedeli pridať alebo odobrať automaticky namapovanú zraniteľnosť/hrozbu. Zjednodušenie a teda čiastočná automatizácia tohto podprocesu spočíva v návrhu vlastnej databázy zraniteľností a hrozieb ako aj s využitím externých dostupných databáz zraniteľností a hrozieb pre IT aktíva.

Ohľadne tvorby vlastnej databázy zraniteľností a hrozieb predpokladáme zoskupovanie informácií na základe podkladov z dostupných katalógov hrozieb a noriem, ktoré sú spomenuté v kapitole 1.2. Táto databáza by bola prepojená *(prelinkovaná)* so zoznamom IT aktív, ktoré máme automaticky získané z predošlých krokov a na základe kategórie a typu aktíva sa po zbere aktív automaticky vykoná priradenie známych zraniteľnosti a hrozieb danému aktívu. Týmto by bolo možné zabezpečiť automatickú identifikáciu zraniteľností a hrozieb pre IT aktíva a eliminovať tak potrebu osobných skúseností a rozhľadenosti bezpečnostného manažéra, manažéra kybernetickej bezpečnosti, prípadne audítora. Databázu by bolo vhodné zakomponovať do spomínaného informačného systému, ktorý by predstavoval centralizované riešenie pre ISMS a ISRM. Na základe týchto informácií by bolo možné pristúpiť k výpočtu rizika pre dané IT aktíva. Vytvorená databáza by okrem zraniteľností a hrozieb mohla obsahovať aj odporúčané nápravné opatrenia ktoré je potrebné vykonať pre zmierňovanie identifikovaných rizík, čím by sa znova zabezpečilo uľahčenie a čiastočná automatizácia tohto procesu. Výhodou a zároveň aj nevýhodou tohto návrhu je potreba spravovať si vlastnú databázu zraniteľností a hrozieb, kde je možné ľubovoľne dopĺňať záznam a upravovať hodnoty pravdepodobností pre hrozby a hodnoty pre kritickosť zraniteľností. Nevýhodou je práve aspekt subjektivity pri dopĺňaní vlastných záznamov do databázy.

Druhá možnosť automatizácie spočíva vo využívaní externých dostupných databáz a katalógov zraniteľností a hrozieb [58]. Riešením je využívanie ponúkaných otvorených REST API rozhraní týchto dostupných databáz, ktoré umožňujú ich softvérové prepojenie so zoznamom IT aktív. Na základe kategórie aktíva by bolo možné čerpať informácie z externých databáz. Rovnako ako v predošlom prípade, aj toto riešenie má svoje výhody a nevýhody. Hlavnou výhodou je aktuálnosť záznamov a obohatenie subjektívneho pohľadu na možné zraniteľnosti a hrozby od tretích strán. Nevýhodou je obmedzené využívanie a potreba prispôsobiť sa kategorizácií aktív z pohľadu týchto databáz, aby ich bolo možné aplikovať na IT aktíva danej organizácie.

Výsledkom tohto procesu je však automatizovane vytvorený zoznam IT aktív, ku ktorým sú automaticky priradené zraniteľnosti a hrozby na základe kategórie a typu aktíva. Všetko ponúkané v jednom systéme a v ucelenej forme.

3.8.2 Návrh výpočtu hodnoty celkového rizika

Po získaní všetkých potrebných informácií ako zoznam IT aktív, hodnota IT aktív, zraniteľnosti a hrozby a ich namapovannie na podnikové aktíva, je možné pristúpiť k procesu výpočtu rizika. Základný princíp výpočtu a hodnotenia rizika popisujeme v kapitole 1.2. V tejto kapitole sa zameriavame na upravený výpočet hodnoty rizika s ohľadom na možnosť predikcie zmeny hodnoty rizika v prípade aplikovania vybraných nápravných opatrení.

Na základe analýzy dostupných metód sme identifikovali najbežnejšie používaný spôsob výpočtu rizika ako súčin pravdepodobnosti, že hrozba využije zraniteľnosť a celkového dopadu zneužitej zraniteľnosti z pohľadu CIA, teda hodnoty aktíva. Ako inšpiráciu pre návrh výpočtu rizika sme vychádzali z metódy používanej v systéme Monarc [59]. Ako už bolo spomenuté, metóda Monarc je postavená na základe princípov a metód štandardu ISO/IEC 27005. Tento prístup sa nám javí lepší na výpočet rizika, a to z dôvodu zakomponovania hodnoty pre zavedenú kontrolu s cieľom určiť úroveň zraniteľnosti. Spôsob výpočtu aktuálneho rizika popisuje nasledujúca funkcia:

$$\boldsymbol{R = A_v \cdot p \cdot q} \qquad (7)$$

kde: $\boldsymbol{R}$ – aktuálne riziko, $\boldsymbol{A_v}$ – hodnota aktíva, $\boldsymbol{p}$ – pravdepodobnosť naplnenia hrozby, $\boldsymbol{q}$ – úroveň zraniteľnosti. Zvyškové riziko sa potom prepočíta na základe aplikovaného opatrenia a teda znížením úrovne zraniteľnosti. Postup pre riadenie rizík, ktorý popisujú normy, počíta s výpočtom rizika pre každé aktívum osobitne. Prioritizácia zmierňovania rizík potom závisí od celkového rizika pre dané aktívum a nastavených prahových hodnôt. Proces zmierňovania rizík potom prebieha taktiež pre každé aktívum osobitne.

My navrhujeme rozšírený spôsob výpočtu rizika za účelom predikcie zmeny hodnoty rizika pre primárne aktívum. Na základe hierarchického modelu a vytvorenej komunikačnej trasy, tzv. cesty, máme vytvorenú aplikačnú skupinu, ktorá je tvorená aplikačnými komponentami. Pre pochopenie zavádzame nasledovnú terminológiu:

- **aplikačná skupina** je aplikácia, softvér alebo služba, ktoré v našom prípade predstavujú primárne aktívum, ktoré je namapované na biznis proces na základe organizačnej štruktúry a oskenovaných IT aktív.
- **komponenty aplikačnej skupiny** sú všetky podporné/sekundárne aktíva, ktoré ležia na vytvorenej komunikačnej trase *(sieťové medziľahlé zariadenia, softvérové komponenty ako webové či databázové servery a podobne)*.

Postup pre výpočet hodnoty rizika je rovnaký ako vyššie popísaný. To znamená, že sa vypočíta hodnota aktuálneho rizika pre každé aktívum *(primárne aj sekundárne)* osobitne. Okrem toho sa vypočíta rozšírená hodnota celkového aktuálneho rizika *(R_A)* pre celú aplikačnú skupinu, teda primárne aktívum, čo predstavuje súčet hodnôt všetkých rizík komponentov aplikačnej skupiny, ktoré ležia na komunikačnej trase.

$$\boldsymbol{R_A = \sum_{i=1}^{n} Ri} \qquad (8)$$

Výsledkom je agregovaná hodnota rizika aplikačnej skupiny ako súčtu rizík jej komponentov. Týmto prístupom dostaneme pohľad na najrizikovejšie primárne aktíva, pre ktoré je potrebné prioritne zabezpečiť zmierňovanie rizík a to z dôvodu, že primárne aktíva sú pre organizáciu najhodnotnejšie. Keďže v našom prístupe využívame systém dedenia hodnoty aktíva z primárneho na sekundárne, mohlo by nastať, že v prípade neagregovania hodnôt rizík by vzniklo rizikovejšie sekundárne aktívum ako primárne, čím by sa skreslil pohľad na hodnotu a rizikovosť primárnych aktív. Po ohodnotení rizík môžeme prejsť k procesu zmierňovania rizík a predikcie zmeny rizika v prípade aplikovania určitého opatrenia.

3.8.3 Návrh simulácií pre predikciu zmeny rizika a finančných strát

Pre proces zmierňovania rizík a výber vhodných opatrení navrhujeme doplniť tento proces o možnosť simulácie stavov, kedy dochádza k zmene hodnoty rizika aplikačnej skupiny pri implementovaní vybraných nápravných opatrení pre zmiernenie rizík. Simuláciou je možné dosiahnuť pohľad na zmenu hodnoty rizika pre viaceré aplikačné skupiny *(primárne aktíva)*, keďže jeden aplikačný komponent *(sekundárne aktívum)* môže patriť do viacerých aplikačných skupín. Tento prístup poskytuje širšie možnosti bezpečnostnému manažérovi, manažérovi kybernetickej bezpečnosti alebo audítorovi pri rozhodovaní sa pri výbere a návrhu vhodných nápravných opatrení pre zmierňovanie rizík či ich postupnosti.

V práci identifikujeme dva prístupy pre vytváranie simulácií. V nich navrhujeme možnosť simulovať zmenu hodnoty rizika aktív na základe zmierňovania ich zraniteľností a hrozieb, ktoré môžu zraniteľnosti využiť. Týmto prístupom je možné simulovať zmenu hodnoty rizika IT aktíva, ktorá sa premietne do výslednej agregovanej hodnoty rizika. Druhou simuláciou je simulácia finančných dopadov v prípade aplikovania alebo neaplikovania nápravných opatrení. Na základe zvolených opatrení vieme vyčísliť finančnú hodnotu potrebnú pre implementáciu nápravných opatrení, prípadne vyčísliť hodnotu strát v prípade neaplikovania nápravného opatrenia.

Predikcia na základe zmierňovania hrozieb – HROZBY

Prvý prístup budovania a behu simulácie je založený a zameraný na zmierňovanie identifikovaných hrozieb. Simulácia ponúka odpovede na otázku: *„Čo nastane, ak danú hrozbu (ktorá môže využívať viaceré zraniteľnosti) zmiernime? Ktoré zraniteľnosti a aktíva to ovplyvní? Ako sa zmení hodnota celkového rizika pre aktívum (primárne aj sekundárne)?“*

Navrhovaná metodika postupu pre simuláciu so zameraním sa na hrozby teda spočíva v týchto krokoch a je znázornená na Obrázok 32:

1. **krok**
   a. Východiskovým bodom pre simuláciu sú:
      i. zoznam ohodnotených IT aktív *(v tomto prípade hlavne z pohľadu finančných dopadov)*,
      ii. priradené zraniteľnosti k ohodnoteným IT aktívam,
      iii. hrozby namapované na zraniteľnosti.
   b. Simulujeme iba nápravné opatrenia na zmierňovanie hrozieb.
   c. Na základe zvolenej hrozby, ktorú chceme zmierňovať je potrebné:
      i. vyfiltrovať všetky zraniteľnosti, ktoré daná hrozba využíva,
      ii. vyfiltrovať všetky aktíva, ktoré vlastnia danú zraniteľnosť, ktorú môže daná hrozba využiť.
2. **krok**
   a. Východiskový bod pre krok 2 je vyfiltrovaný zoznam na základe zvolenej hrozby.
   b. Definujeme postup pre nápravné opatrenie na zmiernenie hrozby *(výber z dostupného zoznamu alebo manuálne)*.

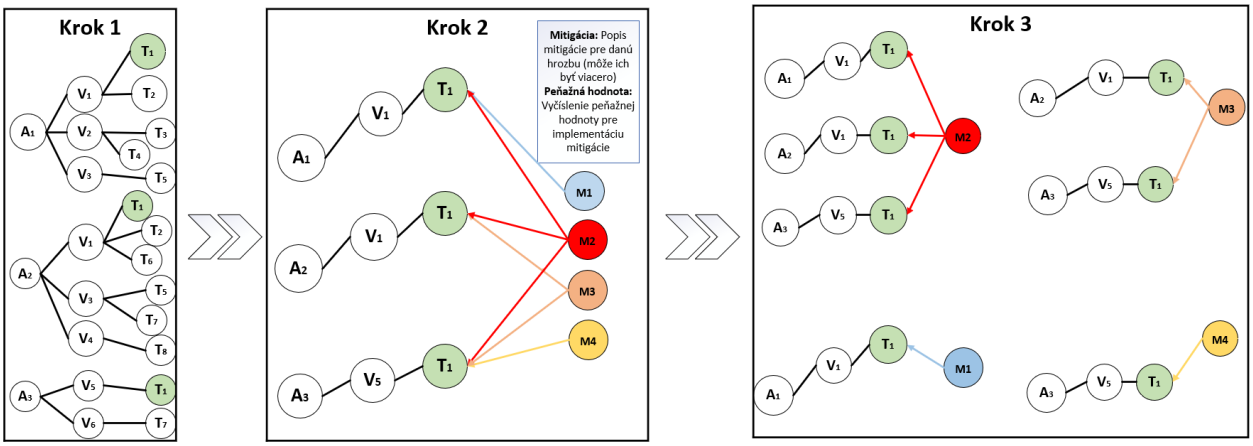
c. Vyčíslime peňažnú hodnotu nápravného opatrenia *(manuálne)*.
d. Vyfiltrujeme výsledný zoznam nápravných opatrení.

3. krok

a. Východiskový bod pre krok 3 je zoznam nápravných opatrení a zobrazenie ich dosahu na hrozby.
b. Vyčíslime si o koľko sa znížila pravdepodobnosť výskytu hrozby po aplikovaní nápravného opatrenia.
c. Prepočítame hodnotu výsledného rizika *(na základe zmenenej hodnoty pravdepodobnosti hrozby)* pre aplikačný komponent *(sekundárne aktívum)* aj aplikačnú skupinu *(primárne aktívum)* do ktorej patrí tento komponent.
d. Reprezentácia výsledkov
    i. Zoznam aplikačných skupín a aplikačných komponentov, ktoré majú vyjadrenú finančnú hodnotu a hodnotu rizika.
    ii. Vybranú hrozbu, jej nápravné opatrenie a finančnú hodnotu nápravného opatrenia.
    iii. Reprezentácia výsledkov simulácie
        1. Pre implementovanie nápravného opatrenia pre vybranú hrozbu je potrebné vyčleniť „X“ finančných prostriedkov, ale pravdepodobnosť výskytu hrozby sa zníži o *„Δp“* čím sa ušetria finančné straty všetkých aktív „$\Delta \sum A_v(F)$“, ktoré vlastnia zraniteľnosť, ktorú daná hrozba môže využiť. Okrem toho, tým, že hrozba vplýva na viaceré aktíva, jej zmiernením dosiahneme zabezpečenie pre všetky tieto aktíva *(aplikačné skupiny aj komponenty aplikačných skupín)*. Zmenou pravdepodobnosti vzniku danej hrozby sa prepočíta hodnota rizika pre všetky aktíva na ktoré daná hrozba pôsobí v prípade, že aktívum je komponent aplikačnej skupiny, tak sa zmení aj hodnota rizika aplikačnej skupiny.

2. Rozhodnutím, že nápravné opatrenie, pre ktoré je potrebné vyčleniť *„X“* finančných prostriedkov, pre vybranú hrozbu sa neimplementuje, nastane nejaká udalosť, ktorá môže spôsobiť finančné straty vo výške *„ΔX“*. Okrem toho, táto hrozba vplýva na viaceré aktíva *(aplikačné skupiny aj komponenty aplikačných skupín)*, čo znamená, že táto finančná strata bude vyššia a rovná sa súčtu finančných strát všetkých aktív *„$\Delta\sum A_v(F)$“* postihnutých naplnením hrozby. Zmena hodnoty rizika nenastane, zostáva pôvodná ako bola vypočítaná na základe analýzy.

Grafické znázornenie jednotlivých krokov simulácie zameranej na zmierňovanie hrozieb predstavuje graf na Obrázok 32. V prvom kroku je znázornený zoznam aktív ku ktorým sú namapované ich zraniteľnosti a k zraniteľnostiam hrozby. Druhý krok znázorňuje voľbu nápravných opatrení a definíciu finančných prostriedkov pre ich implementáciu pre znižovanie pravdepodobnosti vzniku hrozieb. V poslednom treťom kroku sú znázornené zvolené nápravné opatrenia a ich pokrytie a dopad na hrozby.



Obrázok 32 Simulácia zameraná na zmierňovanie hrozieb

Predikcia na základe zmierňovania zraniteľností – ZRANITEĽNOSTI

Druhý prístup simulácie je založený a zameraný na zmierňovanie identifikovaných zraniteľností. Simulácia odpovedá na otázku: *„Čo nastane, ak danú zraniteľnosť (ktorú môžu vlastniť viaceré aktíva) zmiernime? Ktoré aktíva a ako to ovplyvní? Ako sa zmení hodnota celkového rizika pre aktívum (primárneho aj sekundárneho)?“*

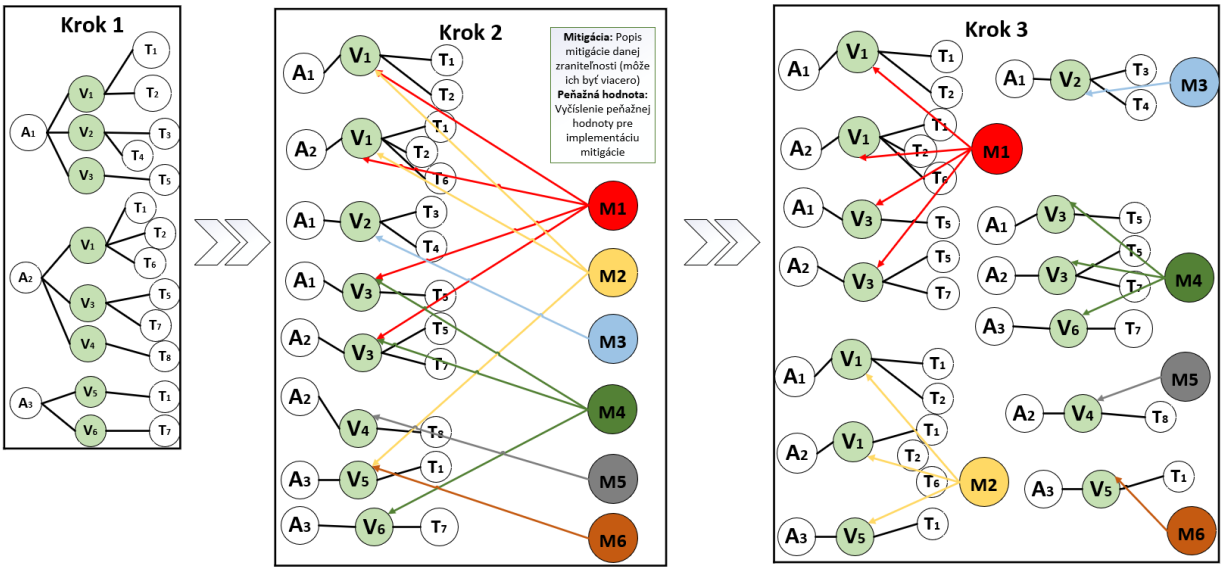
Navrhovaná metodika postupu pre simuláciu so zameraním sa na zraniteľnosti je v princípe rovnaká ako pri simulácií zmierňovania hrozieb s rozdielom, že sa zameriavame na zmierňovanie zraniteľností. Postup teda spočíva v týchto krokoch:

1. **krok**
   a. Východiskovým bodom pre simuláciu sú:
      i. zoznam ohodnotených IT aktív *(v tomto prípade hlavne z pohľadu finančných dopadov)*,
      ii. priradené zraniteľnosti k ohodnoteným IT aktívam,
      iii. hrozby namapované na zraniteľnosti.
   b. Simulujeme iba nápravné opatrenia na zmierňovanie zraniteľností.
   c. Na základe zvolenej zraniteľnosti, ktorú chceme zmierňovať je potrebné:
      i. vyfiltrovať všetky aktíva, ktoré vlastnia danú zraniteľnosť,
      ii. vyfiltrovať všetky hrozby, ktoré môžu využiť danú zraniteľnosť.
2. **krok**
   a. Východiskový bod pre krok 2 je vyfiltrovaný zoznam na základe zvolenej zraniteľnosti.
   b. Definujeme postup pre nápravné opatrenie na zmiernenie zraniteľnosti *(výber z dostupného zoznamu alebo manuálne)*.
   c. Vyčíslime peňažnú hodnotu nápravného opatrenia *(manuálne)*.
   d. Vyfiltrujeme výsledný zoznam nápravných opatrení.
3. **krok**
   a. Východiskový bod pre krok 3 je zoznam nápravných opatrení a zobrazenie ich dosahu na zraniteľnosti.
   b. Vyčíslime si o koľko sa znížila úroveň zraniteľnosti po aplikovaní nápravného opatrenia.
   c. Prepočítame hodnotu výsledného rizika *(na základe zmenenej hodnoty úrovne zraniteľnosti)* pre aplikačný komponent *(sekundárne aktívum)* aj aplikačnú skupinu *(primárne aktívum)* do ktorej patrí tento komponent.
   d. Reprezentácia výsledkov
      i. Zoznam aplikačných skupín a aplikačných komponentov, ktoré majú vyjadrenú finančnú hodnotu a hodnotu rizika.
      ii. Vybranú zraniteľnosť, jej nápravné opatrenia a finančnú hodnotu nápravného opatrenia.

iii. Reprezentácia výsledkov simulácie

1. Implementovaním nápravného opatrenia pre vybranú zraniteľnosť je potrebné vyčleniť „*X*“ finančných prostriedkov, ale zmierni/odstráni sa účinok zraniteľnosti o *„Δq“* čím sa ušetria finančné strany všetkých aktív „$\Delta\sum A_v(F)$“, ktoré vlastnia danú zraniteľnosť. Okrem toho, tým, že zraniteľnosť vlastnia viaceré aktíva, jej zmiernením/odstránením dosiahneme zabezpečenie pre všetky tieto aktíva *(aplikačné skupiny aj komponenty aplikačných skupín)*. Zmenou úrovne danej zraniteľnosti sa prepočíta hodnota rizika pre všetky aktíva, ktoré danú zraniteľnosť vlastnia v prípade, že aktívum je komponent aplikačnej skupiny, tak sa zmení aj hodnota rizika aplikačnej skupiny.
2. Rozhodnutím, že nápravné opatrenie, pre ktoré je potrebné vyčleniť *„X“* finančných prostriedkov, pre vybranú zraniteľnosť sa neimplementuje, nastane nejaká udalosť, ktorá môže spôsobiť finančné straty vo výške *„ΔX“*. Okrem toho zraniteľnosť vlastnia viaceré aktíva *(aplikačné skupiny aj komponenty aplikačných skupín)*, čo znamená, že táto finančná strata bude vyššia a to súčet finančných strát všetkých aktív *„Δ∑Av(F)“*. Zmena hodnoty rizika nenastane, zostáva pôvodná ako bola vypočítaná na základe analýzy.

Grafické znázornenie jednotlivých krokov simulácie zameranej na zmierňovanie zraniteľností predstavuje graf na Obrázok 33. V prvom kroku je znázornený zoznam IT aktív, ku ktorým sú namapované ich zraniteľnosti a k zraniteľnostiam hrozby. Druhý krok znázorňuje voľbu nápravných opatrení a definíciu finančných prostriedkov pre ich implementáciu pre znižovanie úrovne rizika. V posledkom treťom kroku sú znázornené zvolené nápravné opatrenia a ich pokrytie a dopad na zraniteľnosti.

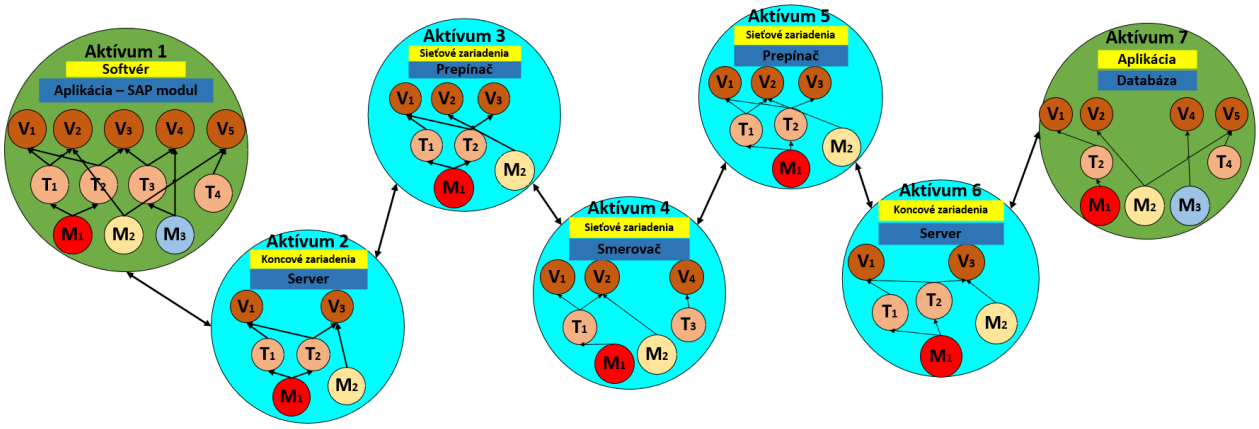


Obrázok 33 Simulácia zameraná na zmierňovanie zraniteľností

Výsledky navrhovaných simulácií popísaných vyššie môžu byť prepočítané a odzrkadlené v navrhovanej topologickej mape a vytvorených komunikačných trasách, čo popisujeme v kapitole 3.7.

3.8.4 Tvorba vzájomného vzťahu aktív (komunikačná trasa)

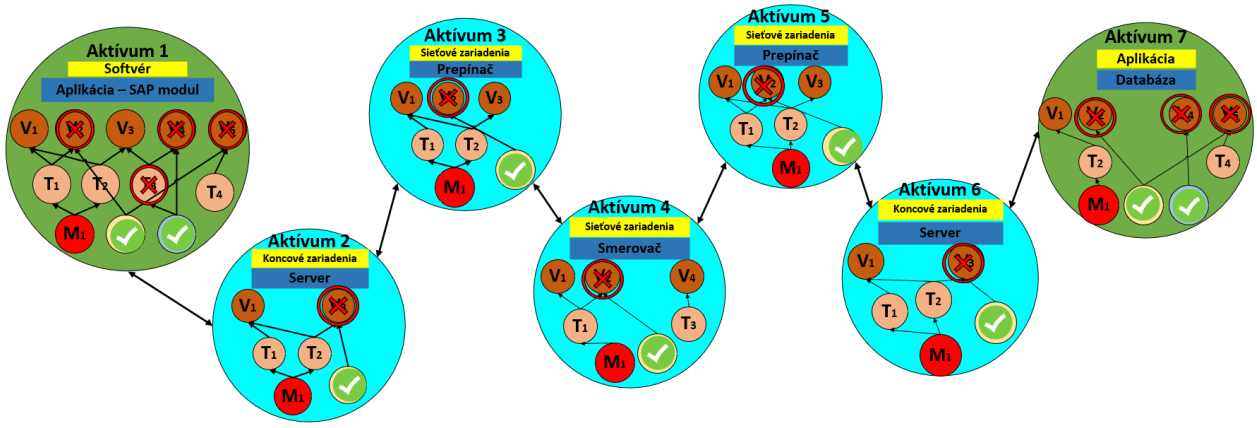
V topologickej mape sú zobrazené všetky IT aktíva, ktoré sú z predošlých krokov ohodnotené na základe CIA s ohľadom na ROLFP, ku ktorým sú namapované zraniteľnosti, hrozby a nápravné opatrenia pre ich zmiernenie a teda zmiernenie celkových rizík pre dané aktíva. Vzorový príklad takejto komunikačnej trasy, ktorá tvorí aplikačnú skupinu znázorňuje Obrázok 34. Na obrázku vidíme aplikačnú skupinu vytvorenú na základe vytvorenej cesty medzi aktívom 1 a aktívom 7. Aplikačná skupina predstavuje primárne aktívum *(v tomto prípade aktívum 1 - aplikácia SAP modul)*, ktorú tvorí šesť aplikačných komponentov *(sekundárnych aktív, aktívum 2 – aktívum 7)*. Na základe vytvorenej cesty vieme určiť všetky podporné aktíva pre toto primárne aktívum. Na vytvorenej ceste teda máme vyfiltrované všetky aktíva, ktoré podporujú konkrétny biznis proces, ktorý je namapovaný na aktívum 1 *(v tomto prípade SAP modul)* a ku všetkým aktívam máme namapované zraniteľnosti, hrozby a nápravné opatrenia.



Obrázok 34 Vzor komunikačnej trasy (aplikačnej skupiny)

Znázornenie simulácií zmierňovania hrozieb a zraniteľností

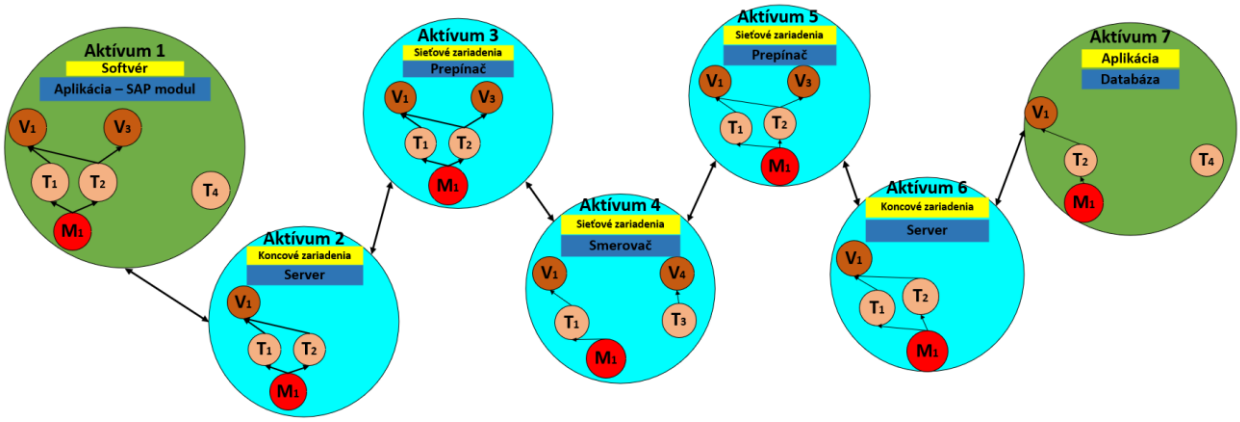
Súčasťou topologickej mapy je návrh a výber vhodných nápravných opatrení a vizualizácia ich dopadu na aktíva *(aplikačné skupiny alebo komponenty aplikačných skupín)*. Pri výbere opatrení sa automaticky prepočítajú hodnoty rizík a prostriedkov potrebných pre implementáciu zvolených nápravných opatrení. Výsledkom simulácie sú aj zdroje potrebné pre ich implementáciu vyčíslené vo finančných hodnotách alebo straty, ktoré môžu nastať v prípade neaplikovania nápravných opatrení. Vzorový príklad je znázornený na Obrázok 35. Obrázok znázorňuje výber nápravných opatrení *(M_x)*, ktoré majú dopad buď na zraniteľnosti *(V_x)* alebo hrozby *(T_x)*, čím znižujú pravdepodobnosť výskytu hrozby alebo účinok zraniteľnosti a tým sa znižuje výsledná hodnota rizika. Všetky prepočty a simulácie prebiehajú v topologickej mape a sú znázornené pre danú aplikačnú skupinu a jej komponenty.



Obrázok 35 Vzor simulácií a výber nápravných opatrení

Znázornenie výsledku simulácie

Výsledok simulácie bude odzrkadľovať stav z predošlého kroku. To znamená znázornenie dopadov v prípade implementácie vybraného nápravného opatrenia na zraniteľnosti, hrozby a výsledné riziká. Vzorový príklad je znázornený na Obrázok 36. Obrázok znázorňuje aplikačnú skupinu a jej komponenty po výbere vhodných nápravných opatrení, pričom pre jednotlivé komponenty ostávajú namapované zraniteľnosti a hrozby, prípadne nápravné opatrenia, ktoré boli definované ale neboli vybrané pre implementáciu.



Obrázok 36 Vzor výsledku simulácie

Výsledky simulácií môžu byť reprezentované ako v topologickej mape, tak vo výslednej správe. Výsledná správa môže byť použitá ako podkladový prezentačný materiál pre potreby dokazovania nutnosti implementácie nápravných opatrení pre zmierňovanie rizík pred manažmentom spoločnosti. Výsledná správa by mala obsahovať:

- zvolené nápravné opatrenia
  - vyčíslenú hodnotu zvolených nápravných opatrení
    - jednotlivo za konkrétne nápravné opatrenie
    - v súčte v prípade, že ich je viacero
- zoznam IT aktív, ktorých sa opatrenia týkajú
  - vyčíslenú finančnú hodnotu IT aktív
    - na základe informácií z predošlých krokov a ohodnotenia IT aktív biznis vlastníkom
- dôkazy pre odporúčania
  - porovnanie finančných dopadov
    - hodnota aktív a hodnota nápravných opatrení

- aktívum - premapovanie aktíva na biznis proces, hodnota aktív z pohľadu CIA, vlastníctvo aktíva, celkové riziko aktíva, peňažná hodnota aktíva
- opatrenie – dopad na zraniteľnosť/hrozbu, dopad na hodnotu celkového rizika pre aktívum, peňažná hodnota implementácie opatrenia.

Vzorový príklad generovanej výslednej správy popisuje Tabuľka 7.

Tabuľka 7 Vzorový príklad výslednej správy po simulácií dopadov

Aktívum 1		**Výsledok**
Vlastnosti	**Opatrenia**	
Biznis proces: *„Text“* **Oddelenie:** *„Text“* **Hodnota aktíva:** A_{1v}=[C,I,A] **Finančná hodnota aktíva:** *„Číslo,- €“*	**M_1:** *Opatrenie 1 – „Text“* **T_1:** *Hrozba 1 – „Text“* **T_2:** *Hrozba 2 – „Text“* **Finančná hodnota opatrenia hrozby:** *„Číslo,- €“* **M_2:** *Opatrenie 2 – „Text“* **V_2:** *Zraniteľnosť 1 – „Text“* **Finančná hodnota opatrenia zraniteľnosti:** *„Číslo,- €“*	Implementáciou opatrenia *(M_1)* sa zníži pravdepodobnosť výskytu hrozieb T_1 a T_2 a celkové riziko *Aktíva 1* sa zmení z hodnoty *„X“* na hodnotu *„Y“*. Na implementáciu opatrenia je potrebné vyčleniť finančné prostriedky vo výške *Z,- €*. Implementáciou opatrenia *(M_2)* sa zníži účinok zraniteľnosti V_2 a celkové riziko *Aktíva 1* sa zmení z hodnoty *„X“* na hodnotu *„Y“*. Na implementáciu opatrenia je potrebné vyčleniť finančné prostriedky vo výške *Z,- €*. V prípade, že nastane udalosť T_1 alebo T_2 a nie je aplikované opatrenie M_1, organizácia sa môže dostať do straty *X,- €*.
Aktívum 2		**Výsledok**
Vlastnosti	**Opatrenia**	
Biznis proces: *„Text“*	**M_3:** *Opatrenie 3 – „Text“* **T_4:** *Hrozba 4 – „Text“*	Implementáciou opatrenia *(M_3)* sa zníži pravdepodobnosť výskytu

Oddelenie: *„Text“* **Hodnota aktíva:** $A_{2v}=[C,I,A]$ **Finančná hodnota aktíva:** *„Číslo,- €“*	**T_5:** *Hrozba 5 – „Text“* **Finančná hodnota opatrenia hrozby:** *„Číslo,- €“*	hrozieb T_4 a T_5 a celkové riziko *Aktíva 2* sa zmení z hodnoty *„X“* na hodnotu *„Y“*. Na implementáciu opatrenia je potrebné vyčleniť finančné prostriedky vo výške *Z,- €*. V prípade, že nastane udalosť T_4 alebo T_5 a nie je aplikované opatrenie M_3, organizácia sa môže dostať do straty *X,- €*.

Prínosom navrhovaných simulácií je poskytnutie širšieho pohľadu na proces výberu vhodných opatrení pre zmierňovanie rizík jednotlivých IT aktív. S využitím topologickej mapy a komunikačnej trasy je zreteľne vidieť vzájomné súvzťažnosti jednotlivých IT aktív, čo je možné využiť či už v procese ohodnocovania IT aktív alebo v procese analýzy rizík. Simuláciou vieme dosiahnuť optimálnejší pohľad pre výber vhodných nápravných opatrení tým, že je možné vidieť zmenu rizík a potrebných finančných prostriedkov v reálnom čase. Pomocou simulácie tak vieme optimalizovať výber nápravných opatrení, ktoré majú dopad na viaceré aplikačné skupiny *(primárne aktíva)* a tým šetriť čas implementácie ako aj finančné prostriedky organizácie. Okrem väčšieho nadhľadu na celý proces zmierňovania rizík je výhodou automatizácie aj generovanie výslednej správy a zobrazenie simulácií priamo za behu v topologickej mape, čo môže pomôcť pri procese plánovania, schvaľovania a dokazovania potreby implementácie nápravných opatrení pred manažmentom organizácie.

4 Diskusia výsledkov práce

Hlavným cieľom tejto dizertačnej práce, tak ako bol definovaný v kapitole 2, je vytvoriť návrh riešení automatizácie vybraných procesov pre ISMS a ISRM, pôvodne vykonávaných manuálne. Za týmto účelom bola vykonaná hĺbková analýza štandardov a aktuálnych publikovaných prác zameraných na ISMS a ISRM procesy a podprocesy, ako aj analýza relevantných softvérových riešení pre túto oblasť. Výsledky získané z vykonaných analýz potvrdili, že táto oblasť je v súčasnosti stále primárne doménou manuálnych činností, ktoré majú obmedzenú podporu zo stany IT prostriedkov. Oblasť však nie je riešená komplexne tak, aby odpovedala súčasným nárokom a dobe digitalizácie, či nástupu využívania online IT prostriedkov ako cloudy a virtualizácia. Odhalený stav nás preto viedol k vytýčeniu smeru riešenia zameraného na zlepšenie ISMS, ako aj ISRM procesov aplikáciou automatizácie s využitím dostupných IT podporných softvérov na vybrané procesy či podprocesy tak, aby nami navrhnuté riešenia efektívne podporili prácu bezpečnostných manažérov, manažérov kybernetickej bezpečnosti, či audítorov smerom k častejším a efektívnejšie vykonávaným činnostiam súvisiacim s riadením bezpečnosti organizácie. Uvedená problematika riešenia bezpečnosti je rozsiahla, a ako z analýzy vyplynulo, nie všetky procesy je možné plne automatizovať. Preto sme sa v riešení zamerali na zlepšenie procesov vytvárania kontextu organizácie, identifikáciu informačných aktív, ohodnocovanie informačných aktív. Pre túto oblasť sme navrhli aj dve nové simulačné metódy využívajúce získane výsledky z nami navrhnutého automatizovaného zberu a klasifikácie aktív. Tieto simulačne algoritmy sa následne zameriavajú na simuláciu zmeny rizika pri aplikovaní vybraných nápravných opatrení.

Za prínos riešenej problematiky a obohatenie procesov ISMS a ISRM radíme návrh procesu vytvárania kontextu organizácie cez nami navrhnutý dotazník spojený s vytváraním digitalizovanej organizačnej štruktúry. S využitím digitalizovaného prístupu v tomto úvodnom podprocese je možné zabezpečiť plynulejší a efektívnejší priebeh identifikácie základných informácií organizácie a zároveň tak poskytnúť digitalizovaný a spracovateľný vstup do ďalších podprocesov. S využitím digitálnych vstupov následne vieme algoritmizovane a automaticky vykonávať identifikáciu IT aktív organizácie, kde na základe digitalizovanej organizačnej štruktúry a vďaka spomínanej digitalizácii je možné následne priradiť konkrétne IT aktíva k ich vlastníkom a začleniť ich do správnych oddelení. Od toho sa nasledovne odvíjajú ďalšie procesy, ako napríklad možné

prelinkovanie konkrétnych biznis procesov k automaticky zozbieraným IT aktívam a identifikácia ich zraniteľností, hrozieb a výpočet rizika.

Čo však považujeme za hlavný prínos riešenej problematiky je, že pre proces identifikácie IT aktív sme navrhli systém pre plne automatizovaný zber IT aktív, ktorý prebieha na základe nami navrhovaných a overených algoritmov. Aplikácia a verifikácia algoritmov prebehla experimentálne vo forme vyvinutého softvérového systému zberu aktív, ktorý môže pracovať samostatne alebo môže byť súčasťou širšieho informačného systému, ktorý spomíname v našej práci. Naše algoritmy a teda aj softvér zberu IT aktív podporujú otvorené a integrovateľné riešenia, nakoľko jednak využívajú slobodný softvér a sú primárne založené na otvorených sieťových manažmentových protokoloch *(SNMP, SSH, WMI)*. Pomocou vytvoreného finálneho algoritmu a integrácie nástrojov a protokolov vieme automatizovane identifikovať všetky potrebné atribúty o IT aktívach organizácie, ktoré sú využiteľné v neskorších procesoch ISMS a ISRM. Navrhovaný systém poskytuje aj funkcionalitu manuálnej úpravy a doplnenia zbieraných informácií. Je to pre prípad neočakávaných obmedzení, ktoré v IKT infraštruktúre môžu nastať z dôvodu nasadených bezpečnostných politík a postupov, ako je bežné v podnikovej praxi. Výsledný systém zberu ma slúžiť ako podpora procesu identifikácie IT aktív pre potreby ISRM alebo auditu. Účelom a prínosom automatizácie v tomto procese je zabezpečiť plynulejší, presnejší a časovo efektívnejší priebeh pre získavanie podkladov a vstupných informácií pre proces riadenia rizík informačnej bezpečnosti a auditu. S využitím navrhovaného automatizovaného systému sa podstatne urýchli čas potrebný pre identifikáciu IT aktív a zníži sa potreba pre organizáciu disponovať technicky zdatným personálom. Okrem automatizácie zberu informácií pre potreby riadenia rizík, sme tento proces doplnili o zber ďalších atribútov aktív, pomocou ktorých následne vieme vytvoriť topologickú mapu aktív a siete organizácie. V mape je zas možné nájsť medzi dvomi aktívami komunikačnú cestu. Prínosom vytvárania topologickej mapy a komunikačnej cesty v tomto procese je jej využitie v ohodnocovaní IT aktív a vizualizácií vzájomných súvzťažností jednotlivých aktív. Vizualizácia pomáha v procese rozhodovania a optimalizácii riadenia rizík a je to úplne nová vlastnosť procesu ISRM, ktorá doteraz nebola nikde použitá.

V rámci ďalšieho riešenia podprocesu sme pre proces ohodnocovania IT aktív navrhli nový hierarchický model skladu a rozkladu IT aktív. Pomocou prístupu skladu a rozkladu IT aktív vieme následne čiastočne automatizovať proces ohodnocovania aktív a zabezpečiť, že po manuálnom vykonanom ohodnotení primárnych aktív systém podľa

našej metodiky automaticky urči hodnoty pre podporné aktíva, ktoré dané primárne aktívum podporujú. Vytváranie hierarchického modelu sa vykonáva práve na základe vytvorenej topologickej mapy a komunikačnej cesty medzi dvomi a viacerými aktívami. Proces ohodnocovania aktív sme navrhovanou metódou zjednodušili iba na ohodnocovanie primárnych aktív, pričom podporné aktíva túto hodnotu dedia, čím sa čiastočne automatizuje proces hodnotenia aktív organizácie. Nami navrhnutý systém, rovnako ako pri identifikácií IT aktív, aj pri ich ohodnocovaní ponúka možnosti úpravy zdedených hodnôt. Upravenou metódou pre vytváranie hodnoty aktíva a výpočet celkovej hodnoty aktíva sme dosiahli objektívnejší pohľad na hodnotu aktíva. Pre vytváranie hodnoty aktíva sme metódu doplnili o zvažovanie viacerých dopadov *(ROLFP)* na aspekty bezpečnosti *(CIA)*. Tým sa čiastočne odstránil subjektívny pohľad pre určovanie hodnoty aktíva. Metódu pre výpočet výslednej hodnoty aktíva sme upravili tak, aby pri veľkých rozptyloch hodnôt jednotlivých dopadov na aspekty bezpečnosti nevznikali skreslené výsledky pre celkovú hodnotu aktíva. Prínosom pre proces riadenia rizík považujeme návrh v podobe prepojenia dostupných databáz zraniteľností a hrozieb s automaticky vytvoreným zoznamom IT aktív. Toto prepojenie umožní na základe kategórie aktív automaticky priradiť zraniteľnosti, ku ktorým sú zas automaticky namapované hrozby. Ďalším prínosom v procese riadenia rizík tiež považujeme návrh simulácií a generovanie výslednej správy. Prínos v podobe simulácie zmeny rizika na základe zvolených opatrení je poskytnutie širšieho pohľadu pre proces výberu vhodných opatrení, čo môže pomôcť pri plánovaní, schvaľovaní a dokazovaní potreby implementácie nápravných opatrení. Výsledná správa tak môže poskytovať podklad pre dokazovanie potreby nápravných opatrení a plánovanie finančných prostriedkov pred manažmentom organizácie.

Výsledky riešenia tejto dizertačnej práce, ako aj navrhované riešenia pre implementačnú časť boli konzultované s audítorom a bezpečnostným manažérom. Čiastkové riešenia sú súčasťou vedecko-výskumného projektu NFP313010S242, Vytvorenie zariadenia na automatický a manuálny zber informačných aktív a ich následné hodnotenie pomocou Monte Carlo metódy, UNIZA 35800593, 2020 – 2023, riešeného na ministerstve hospodárstva. Veríme, že všetky vyššie spomenuté prínosy a návrhy na zlepšenie jednotlivých podprocesov pomôžu a zefektívnia proces implementácie a udržiavanie ISMS, ISRM alebo pri procese auditu.

Záver

Transformáciou informácií, podnikových štruktúr a procesov organizácie do digitálnej podoby a ich presunom do kybernetického priestoru sa im výrazne rozšírilo portfólio zraniteľností, hrozieb a rizík, ktoré na tieto podnikové informačné aktíva vplývajú. Na základe dôležitosti IT aktív pre spoločnosť sa naskytá otázka systematického riadenia informačnej bezpečnosti a auditovania bezpečnosti organizácie za účelom zabezpečenia IT aktív a plynulého dosahovania podnikových cieľov. Náš záujem upútala hlavne otázka podpory automatizácie jednotlivých procesov systému riadenia informačnej bezpečnosti. Keďže informačná a kybernetická bezpečnosť, ako aj auditovanie podliehajú časovej náročnosti a potrebe disponovať technickými zručnosťami, práve z toho dôvodu sme sa venovali možnostiam ich automatizácie. Konkrétne sme sa zamerali na počiatočnú fázu implementácie a vykonávania ISMS, a to zjednodušenie procesu vytvárania kontextu organizácie, automatickej identifikácií IT aktív a ich ohodnocovaniu a navrhli sme simulácie pre proces riadenia rizík a výber vhodných opatrení pre ich zmierňovanie.

V úvode práce sme načrtli potrebu systematicky riadiť informačnú bezpečnosť, ako aj potrebu zvýšenia jej efektívnosti. Keďže hlavnými faktormi pri riadení bezpečnosti v kybernetickom priestore sú čas a finančné prostriedky, venovali sme sa prevažne automatizácií procesov riadenia informačnej bezpečnosti a riadeniu rizík.

V prvej kapitole sme sa venovali popisu jednotlivých procesov a princípov riadenia informačnej bezpečnosti, kde sme načrtli možné zlepšenia a priestor pre využitie automatizácie. Venovali sme pozornosť aj popisu procesu riadenia rizík, čo spadá do celého procesu riadenia informačnej bezpečnosti. V závere kapitoly popisujeme zabezpečenie kontinuity podnikania, práve s využitím systému riadenia informačnej bezpečnosti, ako aj kontrolu dodržiavania súladu, a teda proces auditovania bezpečnosti.

Druhá kapitola popisuje ciele dizertačnej práce ako aj metodiku riešenia, prečo je potrebné riešiť načrtnutý cieľ a aký to prináša prínos. Kapitola uvádza aj čiastkové ciele potrebné pre splnenie hlavného cieľa práce.

V tretej a zároveň hlavnej kapitole tejto práce sa venujeme samotnému riešeniu. Kapitola je rozdelená do viacerých podkapitol ktoré riešia jednotlivé podprocesy riadenia informačnej bezpečnosti. Prvá časť tretej kapitoly je venovaná návrhu pre zlepšenie podprocesu vytvárania kontextu organizácie pomocou navrhnutého dotazníka a vytvárania

digitalizovanej organizačnej štruktúry. Druhá časť popisuje analýzu dostupných riešení systémov pre automatizáciu podprocesov identifikácie IT aktív a riadenia rizík informačnej bezpečnosti. Tretia a štvrtá časť navrhuje algoritmy pre zber IT aktív automatizovaným spôsobom zo siete. Detailne popisuje postupy pre implementáciu a využívanie automatizovaného systému zberu ako aj problémy, ktoré bolo potrebné vyriešiť pre dosiahnutie požadovanej funkčnosti. V šiestej časti popisujeme metódu pomocou ktorej je možné dosiahnuť urýchlený a čiastočne automatizovaný podproces ohodnocovania IT aktív s využitím rozšíreného pohľadu pre vytváranie hodnoty aktíva, aj na základe hierarchického modelu skladania a rozkladania IT aktív. Siedma časť kapitoly je venovaná riadeniu rizík, návrhom výpočtu hodnoty rizika, ako aj návrhu možných simulácií zmeny hodnoty rizika po aplikovaní vybraných nápravných opatrení na základe vytvárania komunikačnej cesty pre znázornenie vzájomných vzťahov medzi IT aktívami.

Ako ďalšie možnosti a rozšírenia pre budúci rozvoj riešenia tejto problematiky odvíjajúci sa od výsledkov tejto práce vidíme možnosť vytvorenia uceleného informačného systému, ktorý by implementoval navrhované riešenia a pokrýval by celý životný cyklus riadenia informačnej bezpečnosti. Po implementácií navrhovaných riešení v IS by bolo možné porovnať prínosy odporúčaní stanovených na základe tejto dizertačnej práce v reálnej praxi. Rozšírením navrhovaných riešení by do budúcna mohlo predstavovať návrh a doplnenie kvantitatívneho hodnotenia IT aktív pre oblasť informačnej a kybernetickej bezpečnosti, ako aj doplnenie podpory pre plne automatizovaný proces identifikácie a mapovania IT aktív na konkrétne ľudské zdroje organizácie.

Zoznam použitej literatúry

[1] S. V. Aleksandrova, V. A. Vasiliev, and M. N. Aleksandrov, “Problems of implementing information security management systems,” *Proc. 2020 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2020*, pp. 78–81, Sep. 2020, doi: 10.1109/ITQMIS51053.2020.9322896.

[2] M. N. Aleksandrov, V. A. Vasiliev, and S. V. Aleksandrova, “Implementation of the Risk-based Approach Methodology in Information Security Management Systems,” *Proc. 2021 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. T QM IS 2021*, pp. 137–139, 2021, doi: 10.1109/ITQMIS53292.2021.9642767.

[3] T. Y. Khashirova, I. I. Mamuchiev, M. I. Mamuchieva, M. I. Ozhiganova, A. D. Kostyukov, and I. Shumeiko, “Assessment of Information Security in Integrated Systems,” *Proc. 2021 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. T QM IS 2021*, pp. 201–205, 2021, doi: 10.1109/ITQMIS53292.2021.9642824.

[4] “ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements.” https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en (accessed Feb. 08, 2023).

[5] “ISMS (Information Security Management System) - ManagementMania.com.” https://managementmania.com/sk/isms-information-security-management-system (accessed Feb. 22, 2023).

[6] “Systém řízení bezpečnosti informací – Wikipedie.” https://cs.wikipedia.org/wiki/Systém_řízení_bezpečnosti_informací (accessed Feb. 22, 2023).

[7] “ISO - ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements.” https://www.iso.org/standard/82875.html (accessed Feb. 22, 2023).

[8] “STN EN ISO/IEC 27002.” https://normy.unms.sk/eshop/public/standard_detail.aspx?id=119075 (accessed Feb. 22, 2023).

[9] "ISO/IEC 27005:2022(en), Information security, cybersecurity and privacy protection — Guidance on managing information security risks." https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-4:v1:en (accessed Feb. 08, 2023).

[10] "Audit Plan & Process | Audit Services | Case Western Reserve University." https://case.edu/auditservices/audit-plan-process (accessed Aug. 31, 2021).

[11] M. K. Hogan, "How to Conduct an Internal Audit at an Opening Meeting." https://smallbusiness.chron.com/conduct-internal-audit-opening-meeting-12948.html (accessed Aug. 31, 2021).

[12] "ISO/IEC 27001:2013(en), Information technology — Security techniques — Information security management systems — Requirements." https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (accessed Aug. 31, 2021).

[13] "ISO/IEC 27002:2022(en), Information security, cybersecurity and privacy protection — Information security controls." https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en (accessed Feb. 08, 2023).

[14] Národný bezpečnostný úrad, "Metodika auditu kybernetickej bezpečnosti." .

[15] M. Shaw, "Best Practices for IT Asset Discovery and Inventory Management | Ivanti," Sep. 05, 2019. https://www.ivanti.com/blog/best-practices-for-it-asset-discovery-and-inventory-management (accessed Aug. 31, 2021).

[16] "Records Management Standard for the New Zealand Public Sector," 2014.

[17] O. M. Al-Matari, I. M. A. Helal, S. A. Mazen, and S. Elhennawy, "Cybersecurity tools for IS auditing," *Proc. - 2018 6th Int. Conf. Enterp. Syst. ES 2018*, pp. 217–223, Dec. 2018, doi: 10.1109/ES.2018.00040.

[18] "IT Asset Management (ITAM) Software | Lansweeper.com." https://www.lansweeper.com/ (accessed Sep. 03, 2021).

[19] "Protect Your Company's Most Valuable Asset with an Inventory Management System." https://www.spiceworks.com/it-articles/inventory-management-system/ (accessed Feb. 22, 2023).

[20] "Try the Demo - Snipe-IT Free open source IT asset management." https://snipeitapp.com/demo (accessed Feb. 22, 2023).

[21] International Organization for Standardization, "ISO/IEC 19770-1:2017 - Information technology -- IT asset management -- Part 1: IT asset management systems -- Requirements," 2017. https://www.iso.org/standard/68531.html%0Ahttps://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en (accessed Aug. 31, 2021).

[22] U. Tatar, "An hierarchical asset valuation method for information security risk analysis," 2012.

[23] I. Loloei, H. R. Shahriari, and A. Sadeghi, "A model for asset valuation in security risk analysis regarding assets' dependencies," *ICEE 2012 - 20th Iranian Conference on Electrical Engineering*, May 2012. https://www.researchgate.net/publication/261348080_A_model_for_asset_valuation_in_security_risk_analysis_regarding_assets'_dependencies (accessed Aug. 31, 2021).

[24] M. Sajko, K. Rabuzin, and M. Bača, "How to calculate information value for effective security risk assessment," *Journal of Information and Organizational Sciences*, Dec. 2006. https://www.researchgate.net/publication/26596362_How_to_calculate_information_value_for_effective_security_risk_assessment (accessed Aug. 31, 2021).

[25] Ü. Tatar and B. Karabacak, "IEEE Xplore Full-Text PDF:," *International Conference on Information Society (i-Society 2012)*, 2012. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6284977 (accessed Aug. 31, 2021).

[26] "IT Asset Valuation, Risk Assessment and Control Implementation Model." https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model (accessed Feb. 08, 2023).

[27] X. Yang, P. Yang, and H. Lin, "Research on Information Security Asset Value Assessment Methodology," *Commun. Comput. Inf. Sci.*, vol. 1699 CCIS, pp. 162–174, 2022, doi: 10.1007/978-981-19-8285-9_12/TABLES/7.

[28] “How to Evaluate Information Assets in ISMS (ISO27001)? | HENNGE Taiwan 部落格.” https://hennge.com/tw/blog/how-to-evaluate-information-assets-in-isms-en.html (accessed Feb. 22, 2023).

[29] “Method Guide - MONARC.” https://www.monarc.lu/documentation/method-guide/ (accessed Sep. 03, 2021).

[30] “The Benefits of Implementing an ISMS | IT Governance Ireland.” https://www.itgovernance.eu/en-ie/isms-benefits-ie (accessed Feb. 23, 2023).

[31] “Riadenie rizík v informačnej bezpečnosti | Preventista.sk.” https://preventista.sk/info/riadenie-rizik-v-informacnej-bezpecnosti/ (accessed Feb. 23, 2023).

[32] “Metodika analýzy rizík kybernetickej bezpečnosti.”

[33] “ISO 22301:2019(en), Security and resilience — Business continuity management systems — Requirements.” https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en (accessed Feb. 23, 2023).

[34] “Audit - ManagementMania.com,” Feb. 27, 2017. https://managementmania.com/sk/audit (accessed Aug. 31, 2021).

[35] “What is a security audit? - Definition from TechTarget.” https://www.techtarget.com/searchcio/definition/security-audit (accessed Feb. 23, 2023).

[36] “Kybernetická bezpečnosť & ISMS | TAYLLORCOX.” https://www.tx.sk/kyberneticka-bezpecnost-isms (accessed Feb. 14, 2023).

[37] “How to Prepare for an Annual Audit - GRF CPAs & Advisors.” https://www.grfcpa.com/resource/how-to-prepare-for-an-annual-audit-1/ (accessed Feb. 14, 2023).

[38] M. Sterbak, P. Segec, and J. Jurc, “Automation of risk management processes,” *ICETA 2021 - 19th IEEE Int. Conf. Emerg. eLearning Technol. Appl. Proc.*, pp. 381–386, 2021, doi: 10.1109/ICETA54173.2021.9726596.

[39] “iTop: softvér s otvoreným zdrojom ITIL ITSM CMDB.” https://www.combodo.com/itop-193 (accessed Feb. 24, 2023).

[40] “Asset management-Management systems-Requirements Gestion d’actifs-Systèmes

de management-Exigences COPYRIGHT PROTECTED DOCUMENT," 2014.

[41] "Eramba - Open IT GRC." https://www.eramba.org/ (accessed Sep. 21, 2022).

[42] "Archer GRC Solution." https://www.archerirm.com/content/grc (accessed Feb. 24, 2023).

[43] "Governance | SimpleRisk GRC Software." https://www.simplerisk.com/solutions/governance?gclid=Cj0KCQjw7KqZBhCBARIsAI-fTKJFyftG9rQ8LIZWHIGoh1oX8IJl9zFGngej5KSCatC9NyZGKG4wNvwaAtzZEALw_wcB (accessed Sep. 21, 2022).

[44] "PTA Professional Reviews & Pricing 2023 - GoodFirms." https://www.goodfirms.co/software/pta-professional (accessed Feb. 24, 2023).

[45] O. M. Al-Matari, I. M. A. Helal, S. A. Mazen, and S. Elhennawy, "Cybersecurity tools for IS auditing," *Proc. - 2018 6th Int. Conf. Enterp. Syst. ES 2018*, pp. 217–223, Dec. 2018, doi: 10.1109/ES.2018.00040.

[46] "Nmap: the Network Mapper - Free Security Scanner." https://nmap.org/ (accessed Feb. 24, 2023).

[47] "hping3 | Kali Linux Tools." https://www.kali.org/tools/hping3/ (accessed Feb. 24, 2023).

[48] "netdiscover | Kali Linux Tools." https://www.kali.org/tools/netdiscover/ (accessed Feb. 24, 2023).

[49] "masscan | Kali Linux Tools." https://www.kali.org/tools/masscan/ (accessed Feb. 24, 2023).

[50] "wmic - Win32 apps | Microsoft Learn." https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmic (accessed Feb. 24, 2023).

[51] "Net-SNMP." http://www.net-snmp.org/ (accessed Sep. 21, 2022).

[52] "SSH Secure Shell home page, maintained by SSH protocol inventor Tatu Ylonen. SSH clients, servers, tutorials, how-tos." https://www.ssh.com/academy/ssh (accessed Sep. 21, 2022).

[53] "Windows Management Instrumentation - Win32 apps | Microsoft Learn." https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page (accessed

Sep. 21, 2022).

[54] “GNS3 | The software that empowers network professionals.” https://www.gns3.com/ (accessed Sep. 21, 2022).

[55] “Method Guide.” https://www.monarc.lu/documentation/method-guide/#impacts-appreciation (accessed Feb. 22, 2023).

[56] O. Kalugina, I. Barankova, and U. Mikhailova, “Development of a Tool for Modeling Security Threats of an Enterprise Information System,” *2nd Int. Conf. Electr. Commun. Comput. Eng. ICECCE 2020*, Jun. 2020, doi: 10.1109/ICECCE49384.2020.9179449.

[57] “What is MONARC? - MONARC.” https://www.monarc.lu/ (accessed Sep. 03, 2021).

[58] “MOSP.” https://objects.monarc.lu/ (accessed Sep. 03, 2021).

[59] “Method Guide.” https://www.monarc.lu/documentation/method-guide/#evaluation-and-treatment-of-risks (accessed Feb. 24, 2023).

Zoznam príloh

Prílohy

Príloha A: Prehľad publikačnej činnosti autora

Remote practice exam testing on docker [electronic] / J. Jurc, M. Sterbak, P. Segec. In: ICERI2022 [electronic] : conference proceedings. - ISSN 2340-1095 (online). - 1. vyd. - Valencia: IATED, 2022. - ISBN 978-84-09-45476-1 (online). - s. 4784-4788 [online].

Virtualization in education using the virtual router tool [electronic] / J. Jurc, M. Sterbak. In: ICERI2022 [electronic] : conference proceedings. - ISSN 2340-1095 (online). - 1. vyd. - Valencia: IATED, 2022. - ISBN 978-84-09-45476-1 (online). - s. 1631-1636 [online].

Tools for automatic collection of IT assets supporting information security process [electronic] / Michal Šterbák, Pavel Segeč, Ján Jurč. In: ICETA 2022 [electronic] : 20th Anniversary of IEEE International Conference on Emerging eLearning Technologies and Applications : proceedings. - 1. vyd. - Piscataway: Institute of Electrical and Electronics Engineers, 2022. - ISBN 979-8-3503-2032-9 (online). - s. 601-606 [online]. Zaradené v: SCOPUS

Automation of risk management processes / Michal Sterbak, Pavel Segec, Jan Jurc. In: ICETA 2021 : 19th IEEE International Conference on Emerging eLearning Technologies and Applications : proceedings : 19th IEEE International Conference on Emerging eLearning Technologies and Applications : proceedings / zost. František Jakab. - 1. vyd. - Denver : Institute of Electrical and Electronics Engineers, 2021. - 441 s. [online, USB-key]. - ISBN 978-1-6654-2101-0. - s. 381-386 [online, USB-key]. Zaradené v: SCOPUS

Design of algorithms for automated collection of IT assets [electronic] / Michal Šterbák, Pavel Segeč, Ján Jurč. In: ICETA 2022 [electronic] : 20th Anniversary of IEEE International Conference on Emerging eLearning Technologies and Applications : proceedings. - 1. vyd. - Piscataway: Institute of Electrical and Electronics Engineers, 2022. - ISBN 979-8-3503-2032-9 (online). - s. 595-600 [online]. Zaradené v: SCOPUS

Effective supervision od students‘ activity during online distance learning and testing [online] / J. Uramová, M. Moravčík, M. Šterbák, J. Remeň. In: ICERI 2022 [electronic] : conference proceedings. - ISSN: 2340-1079 (online). IATED, 2022. - ISBN: 978-84-09-37758-9 (online). s. 4815-4826 [online].

Information systems of virtual laboratories and their development / Ján Jurč, Martin Kontšek, Michal Šterbák. In: ICETA 2021 : 19th IEEE International Conference on Emerging eLearning Technologies and Applications : proceedings : 19th IEEE International Conference on Emerging eLearning Technologies and Applications : proceedings / zost. František Jakab. - 1. vyd. - Denver : Institute of Electrical and Electronics Engineers, 2021. - 441 s. [online, USB-key]. - ISBN 978-1-6654-2101-0. - s.

144-149 [online, USB-key].
Zaradené v: SCOPUS

Survey of the monitoring tools suitable for CC environment / Martin Kontsek ... [et al.]. In: ICETA 2020 : 18th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning : proceedings : 18th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning : proceedings / zost. František Jakab. - 1. vyd. - Denver : Institute of Electrical and Electronics Engineers, 2020. - 789 s. [online]. - ISBN 978-0-7381-2366-0. - s. [1-6] [online].
Zaradené v: SCOPUS

System of automated collection of information assets and their evaluation / Michal Šterbák. In: Mathematics in science and technologies : proceedings of the MIST conference 2021 : proceedings of the MIST conference 2021 / Katarína Bachratá, Alžbeta Bohiniková. - 1. vyd. - [S.l.] : [s.n.], 2021. - 73 s. [online]. - ISBN 9798748088183. - s. 68-73 [online].

Virtual laboratories and their usage in university environment / Jan Jurc, Michal Sterbak, Martin Kontsek.
In: ICETA 2020 : 18th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning : proceedings : 18th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning : proceedings / zost. František Jakab. - 1. vyd. - Denver : Institute of Electrical and Electronics Engineers, 2020. - 789 s. [online]. - ISBN 978-0-7381-2366-0. - s. [1-6] [online].
Zaradené v: SCOPUS

Príloha B: Prehľad pedagogickej činnosti autora

Prehľad riešených záverečných prác

Inžinierske práce:

1. Automatický zber informačných aktív zo sieťovej infraštruktúry pre podporu informačnej bezpečnosti.
2. Mapovanie vzťahov sieťových entít na základe zberu údajov zo siete.

Bakalárske práce:

1. Analýza dostupných metód získavania informácií o medziľahlých zariadeniach a koncových staniciach v sieti s OS Linux.
2. Analýza dostupných metód získavania informácií o medziľahlých zariadeniach a koncových staniciach v sieti s OS Windows.
3. Analýza možností využitia hypervízorov pre potreby zberu informácií zo siete.
4. Porovnávacia analýza dostupných techník a nástrojov automatizovaného zhromažďovania informácií zo siete.
5. Tvorba skriptov pre automatické získavanie informácií zo siete.
6. Tvorba vizualizácie vzájomných väzieb medzi sieťovými zariadeniami a koncovými stanicami v sieti.

Prehľad pedagogickej činnosti

Roky 2020/2021, 2021/2022, 2022/2023

- vedenie cvičení pre predmet Počítačové siete 1

- vedenie cvičení pre predmet Bezpečnosť informačných sietí

- vedenie cvičení pre predmet Princípy IKS

- vedenie študentov na predmetoch Projekt 1, Projekt 2, Projekt 3

Príloha C: Obsah DVD

Priložené DVD obsahuje:

- Práca v elektronickej podobe (formát PDF)