ŽILINSKÁ UNIVERZITA V ŽILINE

AUTOREFERÁT
DIZERTAČNEJ PRÁCE

Žilina, Máj 2023

Ing. Michal Šterbák

Žilinská univerzita v Žiline
Fakulta riadenia a informatiky

Ing. Michal Šterbák

Autoreferát dizertačnej práce

Systém automatizovaného zberu informačných aktív a ich hodnotenia

na získanie akademického titulu **„philosophiae doctor“ (v skratke PhD.)**
v študijnom programe doktorandského štúdia
aplikovaná informatika
v študijnom odbore:
informatika

Žilina, Máj 2023

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia na Katedre informačných sietí, Fakulte riadenia a informatiky Žilinskej univerzity v Žiline.

Predkladateľ:	**Ing. Michal Šterbák** Katedra informačných sieti Fakulta riadenia a informatiky Žilinská univerzita v Žiline
Školiteľ:	**doc. Ing. Pavel Segeč, PhD**. Katedra informačných sieti Fakulta riadenia a informatiky Žilinská univerzita v Žiline
Školiteľ špecialista:	**Mgr. Jana Uramová, PhD.** Katedra informačných sieti Fakulta riadenia a informatiky Žilinská univerzita v Žiline
Oponent 1:	**prof. Ing. Tomáš Loveček, PhD.** Katedra bezpečnostného manažmentu Fakulta bezpečnostného inžinierstva Žilinská univerzita v Žiline
Oponent 2:	**doc. Ing. Peter Feciľak, PhD.** Katedra počítačov a informatiky Fakulta elektrotechniky a informatiky Technická univerzita v Košiciach

Autoreferát bol rozoslaný dňa: 30.6.2023

Obhajoba dizertačnej práce sa koná dňa 22.8.2023 o 9:30 h. pred komisiou pre obhajobu dizertačnej práce schválenou pracovnou skupinou odborovej komisie v študijnom odbore **informatika** v študijnom programe **aplikovaná informatika**, vymenovanou dekanom Fakulty riadenia a informatiky Žilinskej univerzity v Žiline dňa 29.6.2023

prof. Ing. Karol Matiaško, PhD.
predseda pracovnej skupiny odborovej komisie
v študijnom odbore **informatika**
v študijnom programe **aplikovaná informatika**

Fakulta riadenia a informatiky
Žilinská univerzita
Univerzitná 8215/1
010 26 Žilina

OBSAH

Anotácia

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 automatizácii 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

Počet strán:	*140*	*Počet použitej literatúry:*	*59*
Počet obrázkov:	*36*	*Počet tabuliek:*	*7*

Annotation

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

Number of pages:	*140*	*Number of references:*	*59*
Number of figures:	*36*	*Number of tables:*	*7*

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.

Pre analýzu a nastavenie informačnej bezpečnosti na základe bezpečnostných štandardov a legislatíve existujú súhrny procesov medzi ktoré radíme systém riadenia informačnej bezpečnosti (ISMS) [1], riadenie rizík informačnej bezpečnosti (ISRM) [2] a kontinuitu podnikania (BCMS) [3]. 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.

Vzhľadom na vyššie spomenuté aspekty je preto cieľom predkladanej dizertačnej práce návrh riešení automatizácie vybraných procesov informačnej bezpečnosti, pôvodne vykonávaných manuálne s využitím navrhovaných algoritmov pre identifikáciu IT aktív. **Hlavný cieľ je teda návrh automatizovaného systému pre zber IT aktív a ich hodnotenia**.

1. Súčasný stav riešenej problematiky

Za účelom riešenia zabezpečenia IT aktív slúži systém riadenia informačnej bezpečnosti (ISMS). ISMS je systém, ktorý je definovaný v štandarde ISO/IEC 27001. Jeho rozšírením je štandard ISO/IEC 27005 [2], 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. 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.

1.1 Systém riadenia informačnej bezpečnosti

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.

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.

1.2 Riadenie rizík informačnej bezpečnosti

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 [4]. Bezpečnosť je teda komplex procesov a činností zameraných na odvrátenie alebo zmenšenie identifikovaných rizík, resp. prejavov hrozieb ktoré pôsobia na IT aktíva.

Riadenie rizík informačnej bezpečnosti (ISRM) je tretím, prípadne štvrtým podprocesom ISMS. Rovnako ako ISMS, aj riadenie rizík je nepretržitý, cyklický a kontinuálny proces, ktorý sa vykonáva za účelom

identifikácie problémov, testovaním potencionálnych riešení, kontrolu výsledkov testovania a implementácie najlepších riešení pre udržanie akceptovateľnej mieri rizika.

1.3 Vytýčenie riešeného problému

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 [5][6][7]. 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, manažéra kybernetickej bezpečnosti alebo audítora. S týmto zámerom sa venujeme automatizácii vybraných procesov ISMS a ISRM pre zefektívnenie procesov riadenia informačnej bezpečnosti.

2. Ciele práce

Hlavným cieľom práce je 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.

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 identifikovať procesy pre ich automatizáciu,
- navrhnúť hierarchický model skladania a rozkladania IT aktív,
- navrhnúť algoritmy automatizácie podprocesu identifikácie IT aktív a vytvárania hierarchickej štruktúry IT aktív,
- navrhnúť metódu pre automatické ohodnocovanie IT aktív,
- navrhnúť dátový model a algoritmy vyvárania komunikačných trás.

3. Metodika a metódy práce

Metodika riešenia vychádza z parciálnych cieľov dizertačnej práce. Etapy riešenia sú zostavené nasledovne:

1. Analyzovať dostupnú literatúru a metodiky pre jednotlivé podprocesy ISMS a na základe výsledkov vykonať identifikáciu a popis možných zlepšení a ich automatizácie pre vybrané podprocesy.
2. Analyzovať dostupné riešenia, ktoré je možné využiť v procese automatizovanej identifikácie IT aktív.
3. Navrhnúť hierarchický model skladania a rozkladania IT aktív na základe ich primárnosti a sekundárnosti, za účelom ich možného automatizovaného ohodnotenia.
4. Navrhnúť možnosti pre zlepšenie procesu vytvárania kontextu organizácie digitalizovaným spôsobom.
5. Navrhnúť algoritmy pre automatizáciu podprocesu identifikácie IT aktív, ako hlavný cieľ predkladanej dizertačnej práce.
6. Navrhnúť metódu pre automatické ohodnocovanie IT aktív.
7. Navrhnúť dátový model, na základe hierarchického modelu skladania a rozkladania IT aktív, pomocou ktorého by bolo možné vytvárať komunikačnú trasu a tým vizualizovať vzájomné vzťahy medzi primárnymi a sekundárnymi aktívami.
8. Navrhnúť metódy pre vytváranie simulácií za účelom predikcie zmeny rizika.
9. Porovnanie odporúčaní s existujúcimi riešeniami.

4. Návrhy a prínosy dizertačnej práce

4.1 Vytváranie kontextu organizácie

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 [8]. 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.

4.2 Vytváranie organizačnej štruktúry

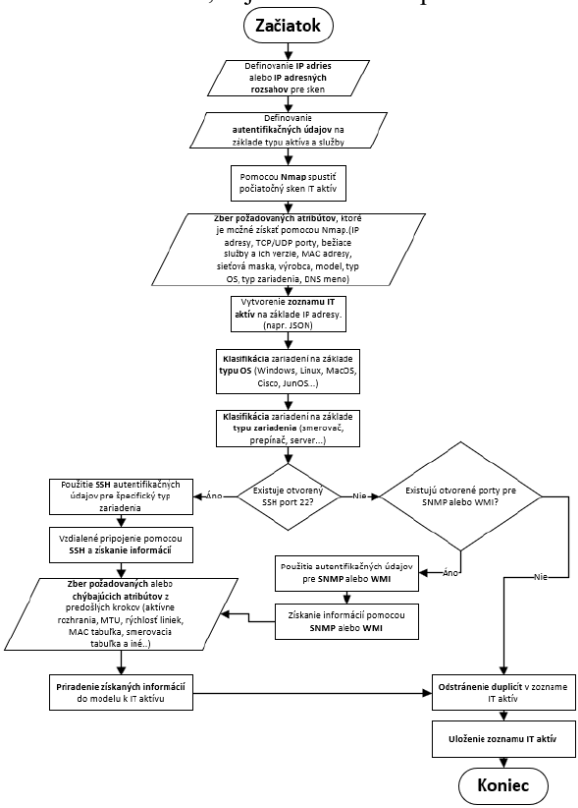
Keďže vzniká potreba mapovania IT aktív k ich vlastníkom, navrhli sme aj spôsob, ako by bolo vhodné takéto prepojenie vytvárať v širšom kontexte. Do navrhovaného digitalizovaného procesu vytvárania kontextu organizácie navrhujeme zakomponovať vytváranie digitalizovanej formy organizačnej štruktúry podniku. 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.

4.3 Automatická identifikácia IT aktív

Hlavným cieľom práce je navrhnúť riešenia automatizácie vybraných procesov ISMS, do čoho spadá aj proces identifikácie IT aktív. Na základe získaných poznatkov, ktoré vyplynuli z analýzy sme identifikovali potrebu riešenia automatickej identifikácie IT aktív. Aj napriek existencii nástrojov zameriavajúcich sa na skenovanie IKT infraštruktúry [9][10][11], 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).

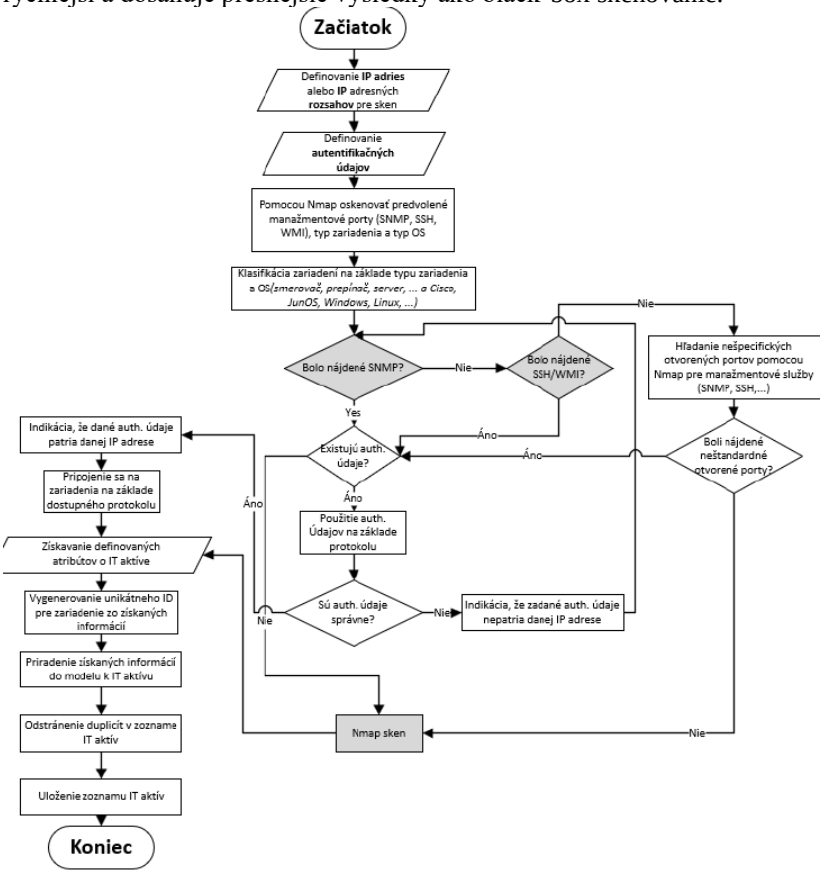
4.4 Návrh algoritmov automatickej identifikácie IT aktív

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 [9][12][13], 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 aktív je možný, ale iba v obmedzenom použití a je pomerne časovo náročný a neefektívny z pohľadu skenovania veľkých IKT infraštruktúr a ich služieb, najmä služieb nad protokolom UDP.



Obrázok 1 Algoritmus variant A - black-box prístup

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, ako napríklad SSH [14], SNMP [15] a WMI [16]. Tento prístup má na jednu stranu nevýhodu v časovej náročnosti na počiatočnú inicializáciu a nastavenie celého procesu skenovania, avšak v porovnaní výsledkov získaných informácií a náročnosťou na doby zberu je celý proces podstatne rýchlejší a dosahuje presnejšie výsledky ako black-box skenovanie.



Obrázok 2 Algoritmus variant B - white-box prístup

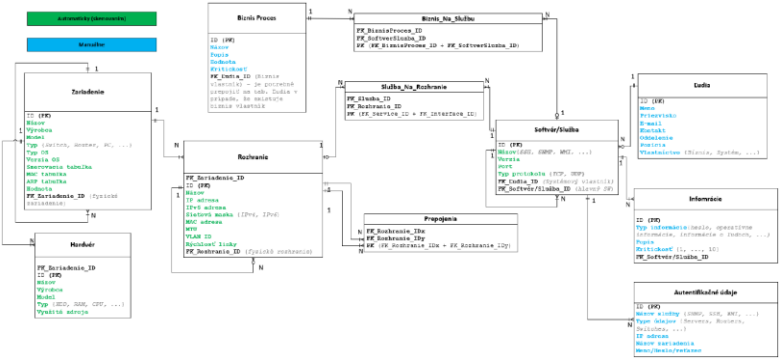
V obidvoch algoritmoch sú využívané rovnaké sieťové protokoly a nástroje, avšak aj napriek tomu je algoritmus variant B rýchlejší a efektívnejší. Dôvodom je práve výber postupnosti využívania jednotlivých

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. Na testovacej topológii s desiatimi zariadeniami s využitím algoritmu varianty B sme urýchlili proces skenovania o približne 1 hodinu a 12 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.

4.5 Návrh dátového modelu

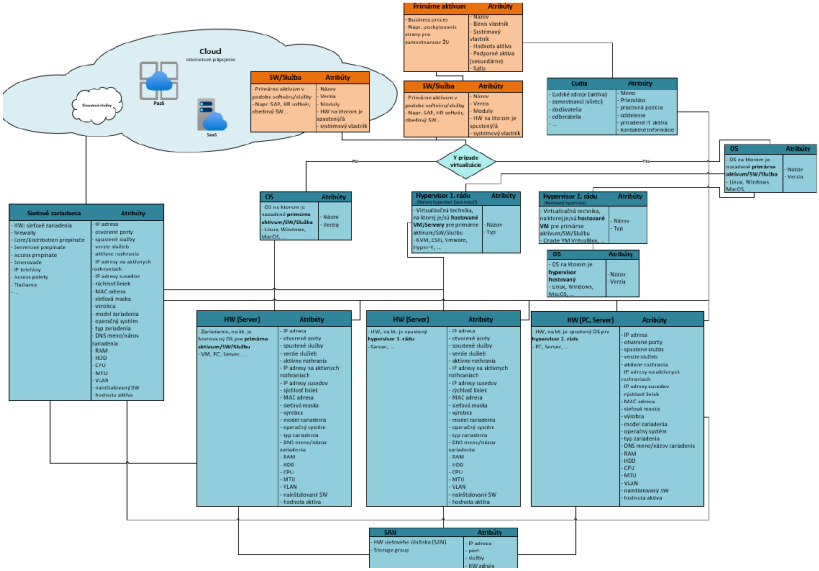
Po identifikácii IT aktív automatizovaným spôsobom je potrebné tieto dáta vhodne uložiť, čo znázorňuje dátový model na obrázku 3. Keďže v sieti existuje množstvo technológií, ktoré agregujú fyzické linky, umožňujú vytvárať virtuálne rozhrania alebo virtuálne stroje, je nutné dbať na všetky tieto aspekty a zohľadniť ich v dátových štruktúrach. Okrem virtualizácie do tejto kategórie patrí aj cloud computing, čo je taktiež potrebné zahrnúť do skenovacieho procesu a vhodne ukladať zistené údaje so zohľadnením virtualizácie a prepojení na fyzické hardvérové prvky.



Obrázok 3 Dátový model pre ukladanie informácií o IT aktívach

4.6 Návrh hierarchického modelu

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. 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 nasledujúci obrázok 4.

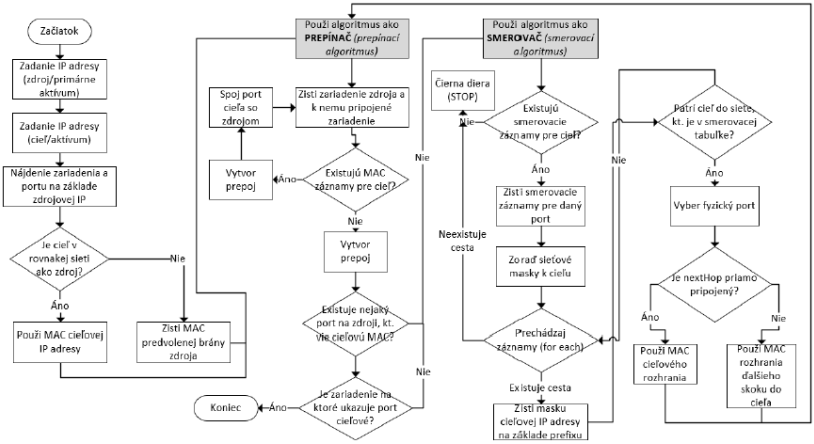


Obrázok 4 Hierarchický model skladu/rozkladu IT aktív

4.7 Návrh algoritmu vytvárania vzájomných vzťahov primárnych a sekundárnych aktív

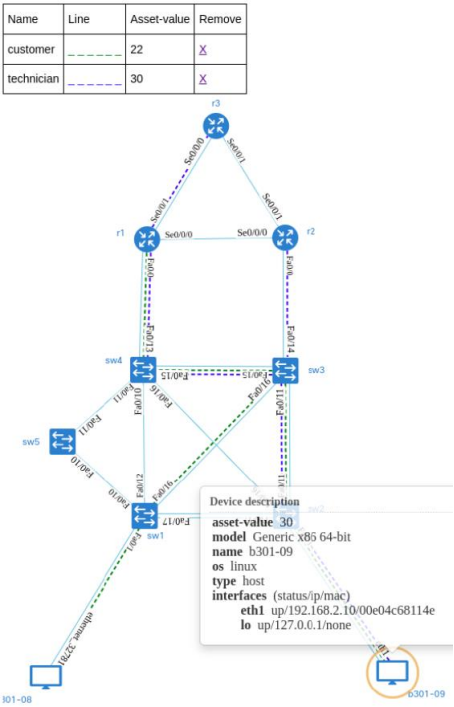
Jedným z čiastkových cieľov dizertačnej práce je aj návrh metódy automatického ohodnocovania IT aktív, ako sme už naznačili v kapitole 4.6. Nami vypracovaný spôsob pre ohodnocovanie IT aktív vychádza z vytvorenia cesty určujúcej vzťah medzi dvomi alebo viacerými primárnymi aktívami a ich podpornými aktívami. 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. Algoritmus pre automatické vytváranie cesty vzájomných vzťahov na základe hierarchického modelu skladu a rozkladu je znázornený na obrázku 5.



Obrázok 5 Algoritmus vytvárania cesty vzájomných vzťahov IT aktív

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. Vytvorenú komunikačnú cestu s priradením hodnoty a jej zdedením na sekundárne aktíva zobrazuje obrázok 6.



Obrázok 6 Topologická mapa s komunikačnými cestami

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. 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. Pri návrhu metódy pre určenie hodnoty primárneho aktíva sme zvolili kombináciu viacerých metód, ktoré vychádzajú zo štandardu ISO/IEC 27005. Skúmaním viacerých možností a metód výpočtu výslednej hodnoty aktíva sme dospeli k záveru, že najvhodnejšie bude skombinovať dva prístupy dokopy. Pre výpočet hodnoty aktíva teda navrhujeme využiť aj funkciu priemeru aj funkciu maxima a výsledné hodnoty spriemerovať.

Výpočet výslednej hodnoty primárneho aktíva pre CIA aspekty používame funkciu priemeru a funkciu maxima v dvojrozmernej matici

hodnôt definovaných tromi riadkami (tri CIA aspekty) a piatimi stĺpcami (ROLFP) (viď. Obrázok 7).

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

Obrázok 7 Tabuľka pre výpočet výslednej hodnoty primárneho aktíva

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 základe príkladu z obrázka 7 s využitím tejto navrhovanej metódy je výsledná hodnota aktíva nasledovná, pričom sa vyberá z vplyvov ROLFP na dopady CIA, kde:

Av – hodnota aktíva,
MAX() – funkcia maxima,
AVG() – funkcia priemeru,
CIA – dôvernosť/integrita/dostupnosť,
ROLFP – vplyv na CIA z pohľadu reputácie, operatívy, zákonov, financií a ľudí,
X – hodnota,
V – matica hodnôt CIA na základe ROLFP.

$Maximum \rightarrow Av = [4,3,4]$
$Priemer \rightarrow Av = [2,2,2]$
$C,I,A = (AvMAXi + AvAVGi)/2$
Výsledná hodnota aktíva potom bude $\boldsymbol{Av} = [\mathbf{3},\mathbf{3},\mathbf{3}]$

4.8 Návrh simulácií predikcie 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

Navrhovaná metodika postupu pre simuláciu so zameraním sa na hrozby 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 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.
   c. Vyčíslime peňažnú hodnotu nápravného opatrenia.
   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 sekundárne aj primárne aktívum.
d. Reprezentácia výsledkov
    i. Zoznam primárnych a sekundárnych aktív, 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 „ΔΣAv(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. Zmenou pravdepodobnosti vzniku danej hrozby sa prepočíta hodnota rizika pre všetky aktíva na ktoré daná hrozba pôsobí v prípade, že aktívum je sekundárne a patrí primárnemu aktívu, tak sa zmení aj hodnota rizika primárneho aktíva.
        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 primárne aj sekundárne aktíva, čo znamená, že táto finančná strata bude vyššia a rovná sa súčtu finančných strát všetkých aktív „ΔΣAv(F)“ postihnutých naplnením hrozby. Zmena hodnoty rizika nenastane, zostáva pôvodná ako bola vypočítaná na základe analýzy.

Predikcia na základe zmierňovania hrozieb

Druhý prístup simulácie je založený a zameraný na zmierňovanie identifikovaných zraniteľností. 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.

Záver

Za účelom dosiahnutia vytýčeného cieľa 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. Na základe toho sme sa v riešení zamerali na zlepšenie procesov vytvárania kontextu organizácie, identifikáciu informačných aktív a 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 simulačné 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 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.

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. 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.

Zoznam použitej literatúry

[1] "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).

[2] "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).

[3] "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).

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

[5] S. V. Aleksandrova, V. A. Vasiliev, and M. N. Aleksandrov, "Problems of Implementing Information Security Management Systems," *2020 Int. Conf. Qual. Manag. Transp. Inf. Secur. Inf. Technol.*, pp. 78–81, Sep. 2020, doi: 10.1109/ITQMIS51053.2020.9322896.

[6] 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.

[7] 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.

[8] 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.

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

[10] “Message from Lansweeper.” https://www.lansweeper.com/it-network-discovery/ (accessed Feb. 22, 2023).
[11] “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).
[12] “masscan | Kali Linux Tools.” https://www.kali.org/tools/masscan/ (accessed Feb. 24, 2023).
[13] “hping3 | Kali Linux Tools.” https://www.kali.org/tools/hping3/ (accessed Feb. 24, 2023).
[14] “What is SSH (Secure Shell)? | SSH Academy.” https://www.ssh.com/academy/ssh (accessed Feb. 24, 2023).
[15] “Net-SNMP.” http://www.net-snmp.org/ (accessed Sep. 21, 2022).
[16] “wmic - Win32 apps | Microsoft Learn.” https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmic (accessed Feb. 24, 2023).