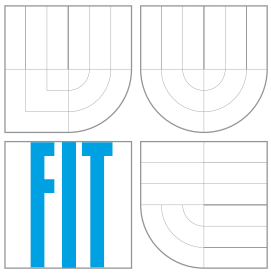
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

# NÁSTROJ PRO BEZPEČNOSTNÍ AUDIT OS LINUX/UNIX/AIX

TOOL FOR SECURITY AUDITING OF LINUX/UNIX/AIX OS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MARTIN KOPPON
AUTHOR

VEDOUCÍ PRÁCE — Ing. MAROŠ BARABAS
SUPERVISOR

BRNO 2016

*Zadání bakalářské práce/18865/2015/xkoppo00*

**Vysoké učení technické v Brně - Fakulta informačních technologií**

Ústav inteligentních systémů Akademický rok 2015/2016

# Zadání bakalářské práce

Řešitel: **Koppon Martin**
Obor: Informační technologie
Téma: **Nástroj pro bezpečnostní audit OS Linux/Unix/AIX**
**Tool for Security Auditing Of Linux/Unix/AIX OS**
Kategorie: Bezpečnost

Pokyny:

1. Nastudujte možnosti automatizovaného testování operačních systémů Linux, Solaris a AIX vzhledem k zavedeným standardům SCAP: CCE, CVE, XCCDF, OVAL, CIS a NVD specifikací.
2. Navrhněte nástroj na audit uvedených operačních systémů.
3. Navržený nástroj implementujte ve skriptovacím jazyku bash.
4. Nástroj otestujte na systémech RHEL a Solaris.
5. Diskutujte jeho rozšíření a další možnosti.

Literatura:

- Dle doporučení vedoucího

Pro udělení zápočtu za první semestr je požadováno:

- Bez požadavků.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Barabas Maroš, Ing.**, UITS FIT VUT
Datum zadání: 1. listopadu 2015
Datum odevzdání: 18. května 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav inteligentních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Dr. Ing. Petr Hanáček
*vedoucí ústavu*

# Abstrakt

Predmetom tejto bakalárskej práce je problematika automatizovaného testovania operačných systémov Linux, Solaris a AIX v kontexte bezpečnostného konfiguračného auditu, vzhľadom na platné normy a zavedené štandardy. Bakalárska práca sa zaoberá analýzou rizika, jeho posúdením a zmiernením a vyhodnocuje dodržiavanie zásad. Pre tento účel bol navrhnutý nástroj pre vyššie uvedené operačné systémy. Implementovaný je v skriptovacom jazyku bash. Nástroj rovnako umožňuje automatizovanú správu zraniteľností k zavedeným standardom SCAP: CCE, CVE, XCCDF, OVAL a k špecifikáciam CIS a NVD. V procese bezpečnostného auditu pomáha znížiť časové nároky, pričom zachováva integritu auditovaného systému.



# Abstract

The subject of this bachelor's thesis is in regards to an issue of automated testing of Linux, Solaris and AIX operating systems according to security configuration audit in consideration of applicable norms and established standards. The bachelor thesis deals with risk analysis, its assessment and risk mitigation and evaluation policy compliance. For this purpose, a tool was designed for operating systems mentioned earlier. It is implemented in the bash script language. The tool allows automated vulnerability management depending on established standards of SCAP: CCE, CVE, XCCDF, OVAL and CIS a NVD specifications. Moreover, it helps to reduce the time requirements during the auditing process while preserving an integrity of the auditing system.



# Kľúčové slová

informačná bezpečnosť, konfiguračný audit, analýza rizika, dodržiavanie zásad, zmiernenie rizika, náprava bezpečnosti konfigurácie, automatizovaná správa zraniteľností, posúdenie systému, ISO/IEC 27000, CIS, NVD, SCAP, CCE, CVE, XCCDF, OVAL

# Keywords

information security, configuration audit, risk analysis, policy compliance, risk mitigation, security configuration remediation, automated vulnerability management, system assessment, ISO/IEC 27000, CIS, NVD, SCAP, CCE, CVE, XCCDF, OVAL



# Citácia

KOPPON, Martin. *Nástroj pro bezpečnostní audit OS Linux/Unix/AIX*. Brno, 2016. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Barabas Maroš.

# Nástroj pro bezpečnostní audit OS Linux/Unix/AIX

## Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Ing. Maroša Barabasa. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

.....
Martin Koppon
18. mája 2016

## Poďakovanie

Ďakujem vedúcemu mojej bakalárskej práce, pánovi Ing. Barabasovi, za možnosť pracovať na individuálnu tému a za jeho čas strávený pri konzultáciach, za odborné rady, trpezlivosť a poskytnutú pomoc.

# Obsah

**Úvod** **3**

**1 Informačná bezpečnosť** **4**
1.1 Úvod do terminológie informačnej bezpečnosti . . . 4
1.2 Model informačnej bezpečnosti . . . 6
1.3 Životný cyklus informačnej bezpečnosti . . . 8
1.3.1 Fáza prípravy . . . 9
1.3.2 Fáza implementácia . . . 10
1.3.3 Fáza overovania . . . 10
1.3.4 Fáza používania a zlepšovania . . . 11
1.4 Proces manažérstva rizika informačnej bezpečnosti . . . 11
1.5 Bezpečnostný audit . . . 14
1.5.1 Manažérstvo bezpečnostného auditu . . . 15
1.5.2 Začatie bezpečnostného auditu . . . 17
1.5.3 Príprava na činnosti bezpečnostného auditu . . . 18
1.5.4 Realizácia činností bezpečnostného auditu . . . 19
1.5.5 Príprava a distribúcia správy z bezpečnostného auditu . . . 19
1.5.6 Vykonanie následného bezpečnostného auditu . . . 19
1.6 U.S. Government prístup k zabezpečeniu bezpečnosti informácií . . . 20
1.6.1 Security Content Automation Protocol (SCAP) . . . 20
1.7 Center for Internet Security (CIS) . . . 22
1.7.1 CIS Benchmarky . . . 22

**2 Prehľad existujúcich nástrojov** **24**
2.1 OpenSCAP . . . 24
2.2 CIS Configuration Assessment Tool (CIS-CAT) . . . 24
2.3 Nessus®, SecurityCenter™, SecurityCenter™ CV . . . 24
2.4 Qualys SCAP Auditor . . . 25
2.5 Ďalšie nástroje poskytujúce automatické testovanie OS . . . 25

**3 Nástroj pre bezpečnostný audit** **26**
3.1 Špecifikácia požiadavkov . . . 26
3.2 Analýza a návrh nástroja . . . 27
3.2.1 Architektúra nástroja . . . 27
3.2.2 Návrh tried . . . 28
3.3 Popis riešenia . . . 29
3.4 Popis implementácie . . . 29
3.4.1 Základné informácie o implementácii nástroja . . . 30

3.5 Testovanie . . . . . 31
3.5.1 Testovanie na systéme Red Hat Enterprise Linux 7.2 . . . . . 31
3.5.2 Testovanie na systéme Solaris 11.3 . . . . . 32
3.6 Možnosti rozšírenia a pokračovanie vývoja . . . . . 32

**Záver** **33**

**Literatúra** **34**

**Prílohy** **37**
Zoznam príloh . . . . . 38

**A Obsah CD** **39**

**B Návod na použitie** **40**

# Úvod

Informačné technológie zasahujú do všetkých oblastí nášho života. S tým úzko súvisí požiadavka na dostupnosť a správnosť informácii, ktoré sú priamo využívané alebo ďalej spracovávané. Všetky uchovávané a spracovávané informácie sú vystavené zraniteľnosti z pohľadu ich možného zneužitia, neúmyselných chýb, ale aj prírodnými vplyvmi ako sú prírodné živle. V poslednom období narastajú najmä úmyselné útoky hackerov do sietí významných inštitúcii ako banky, telekomunikácie, orgány štátnej správy, s cieľom získať informácie prípadne celé databázy údajov dôverného charakteru s možnosťou ich následného zneužitia. Tento trend naznačuje, že ochrane informácii na príslušných úrovniach riadenia nie je venovaná dostatočná pozornosť. Fakt zraniteľnosti uchovávaných informácii vyžaduje od majiteľa resp. správcu aktív prijať dostatočné opatrenia na ich ochranu v závislosti od ich hodnoty. Ochrana informácii v špecifických oblastiach života má podporu aj v príslušnej národnej legislatíve, napr. ochrana osobných údajov. Pre všetky organizácie spoločnosti ochrana informácii sa tak stáva právne záväznou a organizácie musia v zmysle príslušnej právnej normy zaviesť zodpovedajúce opatrenia.

Táto bakalárska práca sa venuje problematike informačnej bezpečnosti a automatizovanému testovaniu konfigurácii operačných systémov v kontexte bezpečnostného auditu. Cieľom je navrhnúť a implementovať nástroj na takéto testovanie uvedených operačných systémov tak, aby bolo ho možné využiť s využitím Security Content Automation Protocol (SCAP) a odporúčaní CIS (Center for Internet Security). Účel je uľahčiť proces auditu a zautomatizovať prebeh testovania konfigurácii operačných systémov.

Bakalárska práca sa skladá z troch hlavných kapitol. Prvá kapitola sa zaoberá problematikou informačnej bezpečnosti, približuje terminológiu informačnej bezpečnosti, jej životný cyklus a briebeh bezpečnostného auditu. Venuje sa používaným štandardom a metódam u nás aj vo svete. Druhá kapitola sa zaoberá prehľadom známych nástrojov poskytujúcich automatizované testovanie operačných systémov. V tretej kapitole sa venujem analýzou a návrhom vlastného nástroja, popisom jeho implementácie a výsledkom z testovania.

# Kapitola 1

# Informačná bezpečnosť

Disciplína, ktorá sa systematickým prístupom zaoberá ochranou aktív v organizácii sa nazýva informačná bezpečnosť. Posudzovanie bezpečnosti nejakého prvku alebo systému je založené na analýze rizika. Daná entita je bezpečná ak nepredstavuje pre užívateľa alebo prostredie žiadne riziko alebo má všeobecne akceptovateľnú úroveň rizika. Organizácia bezpečnosti systému je založená na koordinovaných činnostiach manažérstva rizík aktív v organizácii.

Súčasťou systému informačnej bezpečnosti je aj vyhodnocovanie plnenia prijatých opatrení tak, aby boli splnené požiadavky dané vnútornými predpismi resp. externými normami. Tento dôkazový proces preukázania miery zhody systému s požiadavkami sa nazýva bezpečnostný audit. Pravidelné vykonávanie bezpečnostného auditu dáva dáva uistenie organizácii, že bezpečnosť systému je na úrovni zodpovedajúcej jej politike. V prípade auditu treťou stranou poskytuje nezávislý pohľad na informačnú bezpečnosť v organizácii a zlepšuje tak jej imidž. Výsledky z bezpečnostného auditu sú cenným zdrojom informácií pre zlepšovanie systému informačnej bezpečnosti.

Prístupy k vykonaniu bezpečnostného auditu vychádzajú z prostredia, v akom je systém informačnej bezpečnosti implementovaný. Bezpečnostný audit môže byť zameraný na preverenie rôznych prvkov systému informačnej bezpečnosti. Pre vykonanie bezpečnostného auditu sa aplikujú rôzne nástroje tak, aby sa zabezpečilo efektívne zhromažďovanie a analýza dôkazov auditu.

## 1.1 Úvod do terminológie informačnej bezpečnosti

Neoddeliteľnou súčasťou procesov v každej organizácii je zhromažďovanie, spracovávanie, uchovávanie a prenášanie informácii v informačnom systéme. Informačný systém sú aplikácie, služby, aktíva informačnej technológie alebo ďalšie komponenty pracujúce s informáciami. Definícia informačného systému je podľa normy ISO/IEC 27000 procesná: *„súbor súvisiaceho hardvéru a softvéru usporiadaný pre zber, spracovanie, archivovanie, komunikovanie a spravovanie informácii“* [9]. Informácie môžu mať rôznu formu. Môžu byť vytlačené, uložené na magnetických médiách alebo uložené v digitálnej forme ako elektronické záznamy. Z toho vyplýva, že k zabezpečeniu prístupu k určitým informáciám je potrebné mať príslušné technické vybavenie a v neposlednom rade aj oprávnenie na prácu s tzv. aktívami [4], t.j. s čímkoľvek, čo má pre organizáciu hodnotu.

Všetky procesy v organizácii musia byť vykonávané takým spôsobom, aby bola zabezpečená ochrana informácii, takže ich bezpečnosť. V tejto súvislosti potom hovoríme

o informačnej bezpečnosti, teda o zachovaní dôvernosti, integrity a dostupnosti informácii. Dôvernosť je vlastnosť, na základe ktorej informácie nie sú sprístupňované a odhaľované neautorizovaným osobám, entitám alebo procesom, pričom integrita je vlastnosť zabezpečujúca presnosť a kompletnosť aktív. Informačné systémy v organizáciách sú neustále vystavené bezpečnostným hrozbám z rôznych zdrojov ako sú malware, útoky hackerov, podvody sociálneho inžinierstva a pod. Hrozbou teda nazývame potenciálnu príčinu nechceného incidentu, ktorého výsledkom môže byť poškodenie systému alebo organizácie. Incident informačnej bezpečnosti je jedna alebo viaceré neželané a neočakávané udalosti informačnej bezpečnosti, pri ktorých je vysoká pravdepodobnosť kompromitácie aktivít spoločnosti a ohrozenia informačnej bezpečnosti. Aktíva informačnej bezpečnosti môžu mať rôzny stupeň odolnosti voči incidentom. V tejto súvislosti potom hovoríme o zraniteľnosti systému informačnej bezpečnosti. Zraniteľnosť je definovaná ako slabé miesto aktíva alebo opatrenia, ktoré môže byť využité jednou alebo viacerými hrozbami. Dôsledkom vzniknutého incidentu môže byť zničenie aktíva, strata jeho dostupnosti alebo jeho utajenia. Dopadom môžu byť finančné a marketingové straty, straty dobrého mena atď. Štandard ISO/IEC 17000 charakterizuje následok ako výsledok udalosti pôsobiaci na ciele. Udalosť informačnej bezpečnosti chápeme ako identifikovaný výskyt stavu systému, služby alebo siete, ktorý signalizuje možnosť porušenia politiky informačnej bezpečnosti alebo zlyhania opatrení alebo doposiaľ nezaznamenanú situáciu, ktorá môže byť relevantná z hľadiska bezpečnosti a cieľom je výsledok, ktorý má byť dosiahnutý [4].

Zabezpečenie informačnej bezpečnosti nie sú len technické riešenia. Pre jej komplexné riešenie je potrebné prijať systémový prístup podobne ako pri iných manažérskych systémoch v zmysle stanovenia politík, procesov, postupov a pracovných inštrukcii, organizačných štruktúr, výberom hardvéru a softvéru atď. Pre efektívnu informačnú bezpečnosť je potrebné vytvoriť systém manažérstva informačnej bezpečnosti (SMIB). SMIB je časť celkového systému manažérstva, založená na prístupe k riziku organizácie, ktorej úlohou je zriadiť, implementovať, prevádzkovať, monitorovať, preskúmavať, udržiavať a zlepšovať informačnú bezpečnosť. Vybudovanie SMIB v organizácii je kľúčovým rozhodnutím vrcholového manažmentu. Vzťah vrcholového manažmentu k informačnej bezpečnosti je vyjadrená v politike. Politika podľa ISO/IEC 27000 je charakterizovaná ako celkový zámer a smerovanie organizácie formálne vyjadrené vrcholovým manažmentom [4]. Takto je definovaná politika pre všetky manažérske systémy. Možno nájsť aj iné, detailnejšie definície politiky informačnej bezpečnosti. Zdroj Baseline IT Security Policy S17 ju definuje ako *„zoznam manažérskych pokynov, ktoré podrobne popisujú správne používanie a riadenie počítačových a sieťových zdrojov s cieľom ochrániť tieto zdroje ako aj uchovávané alebo spracovávané informácie informačnými systémami pred neautorizovaním odhalením, modifikáciou alebo zničením“* [9].

Riešenie informačnej bezpečnosti znamená poznať a riadiť riziká, ktoré vyplývajú z hrozieb súvisiacich s používanou technológiou a z vplyvu ľudského faktora. Podľa ISO/IEC 27000 riziko je dôsledok neistoty na dosiahnutie cieľov [4]. Pragmatickejšie definuje riziko Ing. Renata Janošcová PhD. v Princípoch informačnej bezpečnosti ako *„potenciál, že daná hrozba využije zraniteľnosti na spôsobenie poškodenia aktíva alebo skupiny aktív a nakoniec priamo alebo nepriamo aj organizácii“* [15]. Ak chceme riadiť riziká, musíme vedieť riziká kvantifikovať. Riziko charakterizujeme atribútmi ako úroveň rizika, závažnosť následkov hrozby a pravdepodobnosť následkov hrozby. Úroveň rizika je veľkosť rizika vyjadrená ako kombinácia následkov a ich pravdepodobnosti. Závažnosť následkov hrozby je veľkosť škody pre organizáciu v prípade uskutočnenia hrozby. Pravdepodobnosť je možnosť, že sa niečo stane [4].

Systematické uplatňovanie politík riadenia, postupov a praktík pre oznamovanie, konzultovanie, určovanie kontextu a zisťovanie, analyzovanie, hodnotenie, ošetrovanie, monitorovanie a preskúmavanie rizika nazývame proces manažérstva rizika. Proces manažérstva rizika rozdeľujeme na proces analýzy rizika, proces posúdenia rizika, proces ošetrenia rizika a proces akceptácie zostatkového rizika. Analýza rizika je proces pochopenia povahy rizika a určenie úrovne rizika, proces posúdenia rizika je celkový proces identifikácie rizika, analýzy rizika a ohodnotenia rizika. Identifikácia rizika je proces zisťovania, a popisovania rizika a ohodnotenie rizika je proces porovnania výsledkov analýzy rizika s kritériami rizika k určeniu či riziko a/alebo jeho závažnosť sú prijateľné alebo tolerovateľné. Kritériami rizika nazývame daný rámec, na základe ktorého sa hodnotí závažnosť rizika [4]. Pred vykonaním ohodnotenia rizika musíme vykonať tzv. ocenenie rizika t.j. určiť hodnotu pravdepodobnosti a následkov rizika [2]. Riziká, ktoré boli vyhodnotené ako neakceptovateľné je potrebné ošetriť tak, aby boli tolerovateľné. Ošetrenie rizika je teda proces vedúci k modifikácii rizika [4]. Výsledkom ošetrenia rizika je jedno alebo viac ochranných (bezpečnostných) opatrení. Ochranné opatrenia sú praktiky, procedúry, a mechanizmy, ktoré môžu pomôcť chrániť pred nejakou hrozbou, znížiť zraniteľnosť, obmedziť vplyv nechcenej udalosti, odhaliť nechcenú udalosť a umožniť zotavenie alebo odškodnenie [15]. Riziko zostávajúce po ošetrení rizika sa nazýva zostatkové riziko. Ak zostatkové riziko je tolerovateľné, teda ošetrenie rizika bolo efektívne, potom hovoríme, že zostatkové riziko je akceptovateľné. Akceptácia rizika je rozhodnutie prijať určité riziko. Ošetrenie všetkých relevantných rizík na akceptovateľnú úroveň, aplikovateľných pre organizáciu podľa prílohy A štandardu ISO/IEC 27001 sa vykoná Vyhlásením o aplikovateľnosti. Vyhlásenie o aplikovateľnosti je dokumentované vyhlásenie opisujúce ciele riadenia a opatrenia, ktoré sú relevantné a platné pre SMIB organizácie [4].

Proces manažérstva rizika je zameraný na identifikáciu ochranných opatrení na ochranu informačných aktív. Tieto ochranné opatrenia musia byť neustále kontrolované, aby sa preukázalo, že sú riadne implementované a efektívne. Nástrojom na preverovanie ochranných opatrení je bezpečnostný audit. Audit je systematický, nezávislý a zdokumentovaný proces získavania dôkazov auditu a ich objektívneho vyhodnocovania s cieľom určiť rozsah, v akom sa plnia kritériá auditu. Bezpečnostný audit je audit zameraný na posúdenie informačnej bezpečnosti. Kritériami auditu je súbor politík, postupov alebo požiadaviek, ktoré sa použijú ako odkazy voči, ktorým sa porovnávajú dôkazy auditu [1].

Dôkaz auditu sú záznamy, konštatovania skutočností alebo iné informácie týkajúce sa kritérií auditu, ktoré sú verifikovateľné. Výsledky hodnotenia zozbieraných dôkazov auditu voči kritériám auditu sú zistenia auditu. Zistenia z auditu môžu byť pozitívne alebo negatívne. Zhoda je splnenie požiadavky a nezhoda je nesplnenie požiadavky. Činnosť vedúca k odstráneniu príčiny nezhody sa nazýva nápravné opatrenie [1].

Audit vykonáva audítor. Audítor vykonáva audit podľa plánu. Plán auditu obsahuje opis činností a opatrení auditu. Plány pre súbor jedného alebo viacerých auditov plánovaných na konkrétny časový úsek a zameraných na konkrétny cieľ sa nazýva program auditu [1].

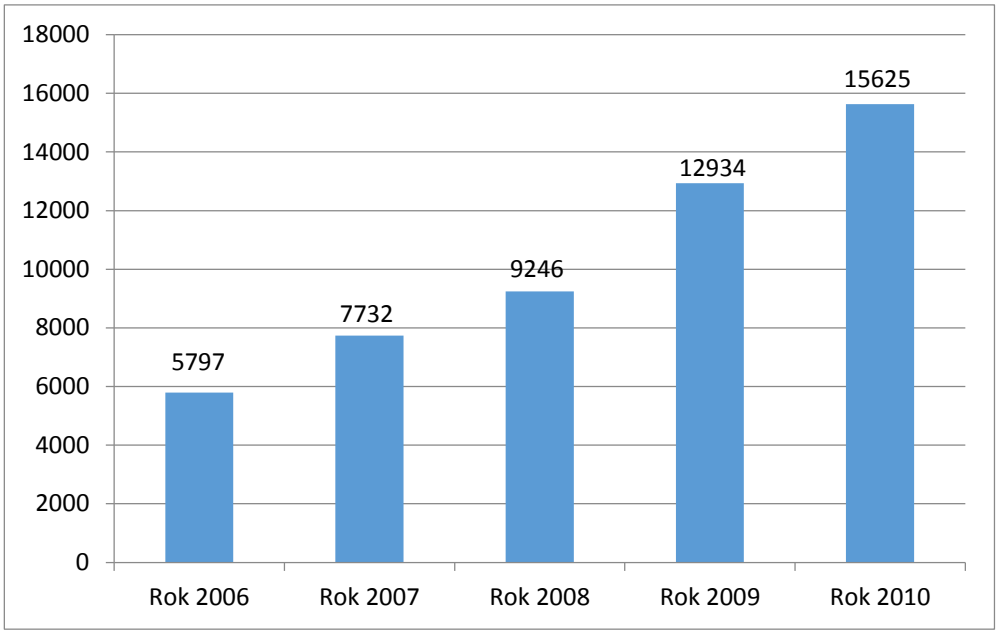
## 1.2 Model informačnej bezpečnosti

Pre riešenie problematiky informačnej bezpečnosti bolo vytvorených niekoľko štandardov. Tieto štandardy stanovujú kritéria na jednotlivé prvky systému, ktorých splnenie zabezpečí požadovanú úroveň informačnej bezpečnosti. Medzi najznámejšie štandardy patrí sústava štandardov radu ISO/IEC 270xx, COBIT® spoločnosti ISACA, NIST Special Publication 800-53 [18] z Amerického národného inštitútu pre štandardy a technológie a iné. Pri riešení

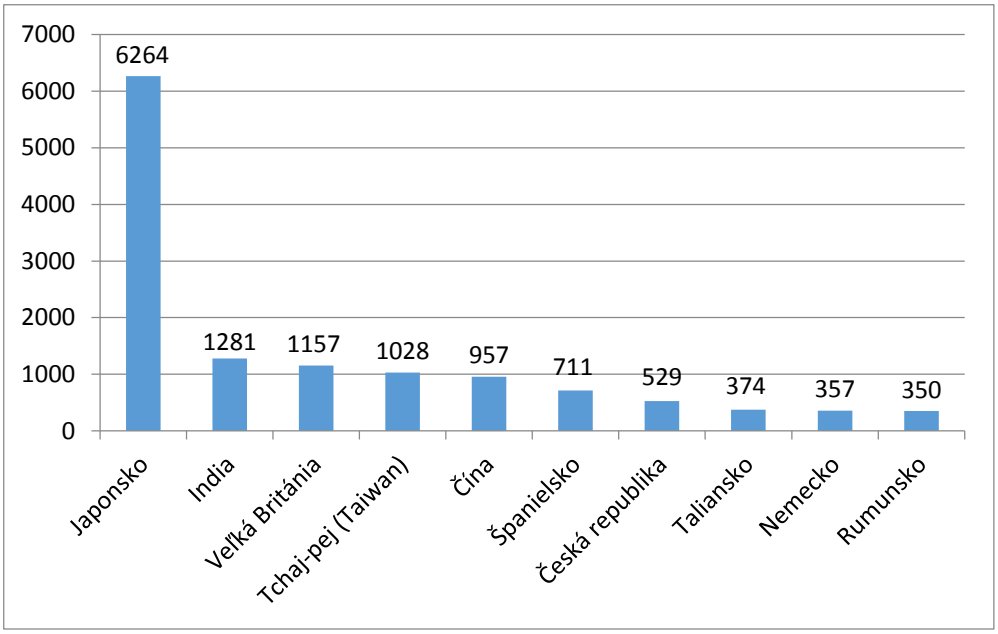
modelu informačnej bezpečnosti je prostredie ISO/IEC 27001 využívané z nasledovných dôvodov:

- Normy radu ISO/IEC 270xx sú vo svete dobre zavedené a sú doporučené ako predpoklad zhody s legislatívou. Napr. smernice OECD pre informačnú bezpečnosť.
- Mnohé organizácie sú certifikované podľa štandardu ISO/IEC 27001. Implementovanie štandardov SCAP pre bezpečnostný audit operačných systémov prináša pre tieto spoločnosti vyššiu pridanú hodnotu vykonaného auditu.
- Štandard ISO/IEC 27001 je konzistentný s ďalšími manažérskymi systémami ako ISO 9001, ISO 14001, ISO 18001 a pod., pričom všetky tieto štandardy využívajú jednotnú auditnú metodiku podľa ISO 19011 Návod na auditovanie systému manažérstva, čo výrazne uľahčuje proces auditovania manažérskeho systému.

Pre ilustráciu rozšírenia aplikácii štandardu ISO/IEC 27001 vo svete možno uviesť nasledovné prehľady vydaných certifikátov, ktoré boli prevzaté z publikovaných informácii [13] z obdobia rokov 2006 až 2010. Napriek tomu, že aktuálnejšie údaje o vydaných certifikátoch podľa ISO/IEC 27001 nie sú k dispozícii, možno z uvedených grafov usúdiť niekoľko skutočností. Nárast certifikácii vo svete neustále významne rastie a tento rast je ďaleko významnejší vo Východnej Ázii ako v ostatných krajinách sveta (viac ako 50% v roku 2010). Vysoký podiel Veľkej Británie na vydaných certifikátoch v Európe je následok postavenia noriem radu ISO 270xx na základe národných noriem pre informačnú bezpečnosť vo Veľkej Británii. Na druhej strane napr. v USA certifikácia podľa ISO/IEC 27001 nie je rozšírená (329 certifikácii v roku 2010), pretože vláda Spojených štátov zvolila vlastný legislatívny prístup k riešeniu informačnej bezpečnosti, ktorý nie je konzistentný s ISO/IEC 27001.




Obr. 1.1: Počet výdaných certifikátov podľa ISO 27001 [13]




Obr. 1.2: Počet výdaných certifikátov podľa ISO 27001 v roku 2010 [13]

## 1.3 Životný cyklus informačnej bezpečnosti

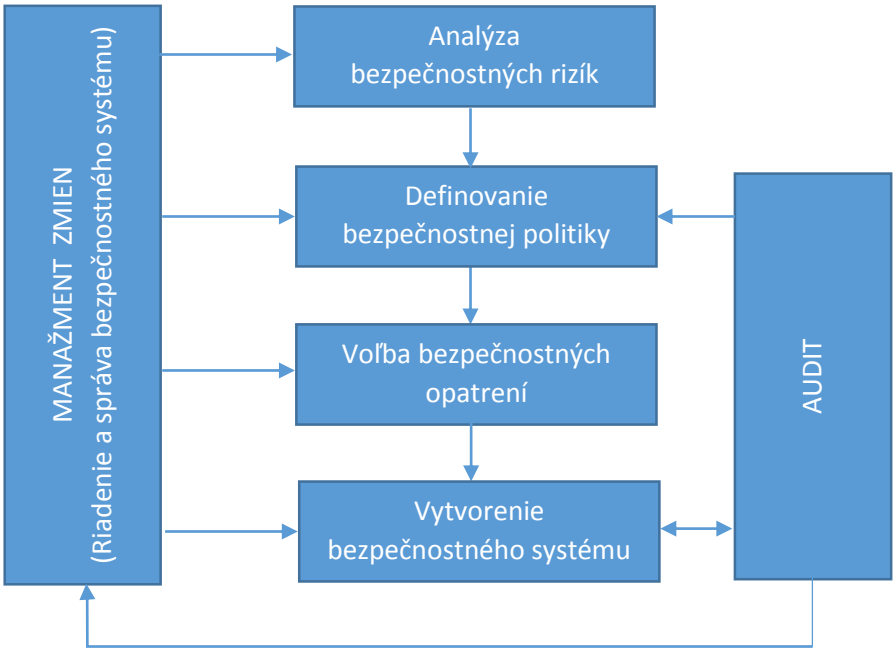
Zaistenie bezpečnosti je potrebné chápať ako vzájomnú interakciu rôznych procesov, ktoré sa cyklicky opakujú, ako je znázornené na obrázku 1.3. Tomuto javu hovoríme životný cyklus informačnej bezpečnosti. Všeobecne sem patria procesy analýzy rizík, procesy súvisiace so stanovením cieľov, stratégií a politík informačnej bezpečnosti, procesy implementácie opatrení znižovania rizika, procesy prevádzky a údržby systému, procesy jeho pravidelného preskúmania, monitorovania, auditu a v neposlednom rade procesy zlepšovania a zavádzania zmien informačnej bezpečnosti.

Medzi najvýznamnejšie procesy životného cyklu informačnej bezpečnosti zaraďujeme proces analýzy rizika a proces monitorovania resp. proces bezpečnostného auditu. Analýzou rizika sa identifikujú požadované opatrenia, aby sa zabránilo výskytu incidentov a ochránili sa tak aktíva spoločnosti. Bezpečnostným auditom sa preveruje, či bezpečnostné opatrenia sú náležite implementované a tým je zabezpečená požadovaná úroveň bezpečnosti. Opakovanie procesu analýzy rizika má menšiu periodicitu, napr. raz za dva roky, ako opakovanie bezpečnostného auditu spravidla raz za rok, prípadne aj častejšie. V prípade, že je potrebné preverovať aktíva veľmi často, napr. denne, potom hovoríme o monitorovaní informačnej bezpečnosti.

Pri projektovaní bezpečnosti systému účinne pomôže PDCA model (Plan – Do – Check – Act) [13], ako je zobrazené na obrázku 1.4. PDCA model môžeme aplikovať na jednotlivé fázy jeho životného cyklu nasledovne:

- Fáza prípravy
- Fáza implementácie
- Fáza overenia (auditu)

- Fáza používania a zlepšovania



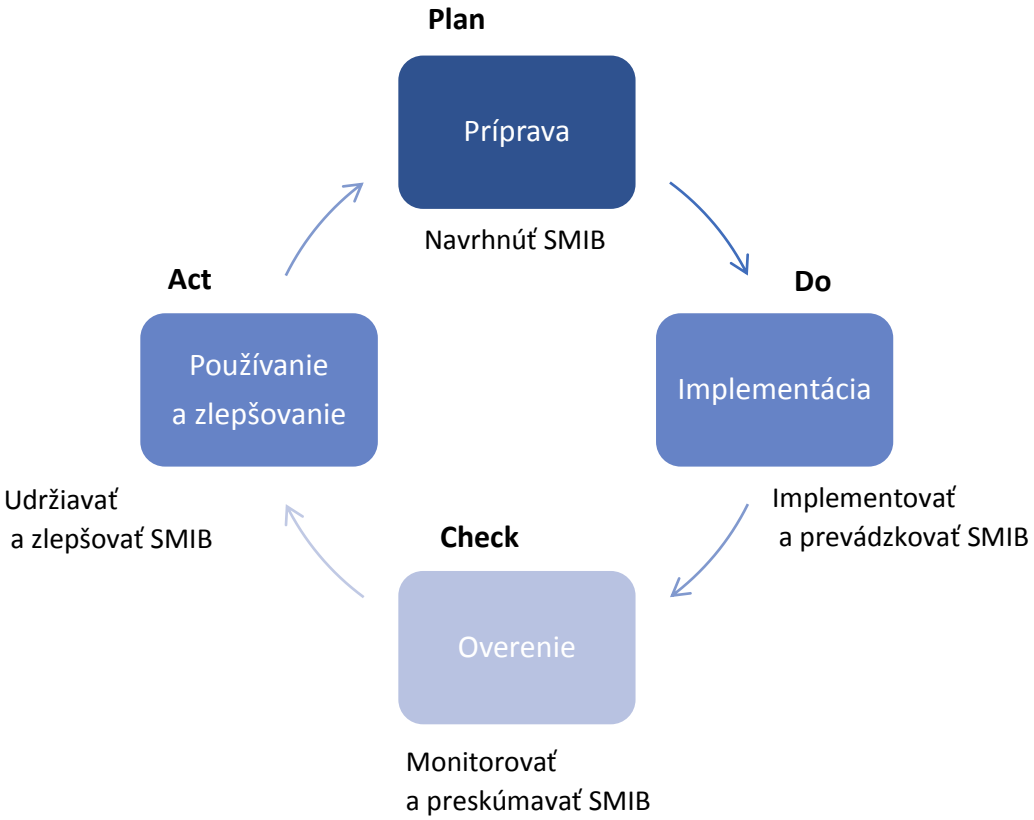

Obr. 1.3: Životný cyklus bezpečnosti [15]

### 1.3.1 Fáza prípravy

Fáza prípravy je najdôležitejšou fázou životného cyklu informačnej bezpečnosti. Od vrcholového vedenia závisí, aký bude prístup spoločnosti k zabezpečeniu informačnej bezpečnosti. V tejto fáze životného cyklu vrcholový manažment formuluje záväzok vybudovať efektívny systém informačnej bezpečnosti. V projekte musia byť zadefinované vonkajšie (legislatívne) aj vnútorné obmedzenia. Sú identifikované všetky aktíva a vyčíslená ich hodnota pre spoločnosť. Veľkú pozornosť treba venovať identifikácii hrozieb, ako zdroju incidentov a identifikácii zraniteľností, ako slabých miest aktív.

Na základe týchto vstupov je vykonaná analýza rizík. Analýza rizika nemá byť prácou jednotlivca (napr. konzultačná firma), ale je to tímová práca kompetentných pracovníkov z rôznych oddelení (manažér SMIB, metodík analýzy rizík, investície/logistika a pod.) Keď je známy bezpečnostný zámer a vykonaná analýza rizík, môže sa pristúpiť k formulovaniu celopodnikovej bezpečnostnej politiky. Túto politiku formuluje vrcholové vedenie za účasti predstaviteľa manažmentu pre bezpečnosť informácii – manažér systému manažérstva informačnej bezpečnosti (SMIB). Následne je bezpečnostná politika rozpracovaná na dielčie politiky pre jednotlivé časti/subsystémy. V súlade s bezpečnostnou politikou musí byť stanovená akceptovateľná a neakceptovateľná úroveň rizika.

Poslednou časťou fázy prípravy je výber vhodných bezpečnostných opatrení zameraných na ošetrenie/zníženie miery rizika všetkých aktív tak, aby boli v súlade s cieľmi riadenia a prijatými kritériami formulovanými v bezpečnostnej politike. Táto časť môže byť časovo veľmi náročná, pretože je potrebné vypracovať všetku dokumentáciu požadovanú




Obr. 1.4: Model PDCA aplikovaný na procesy SMIB [13]

normou ISO 27001, ako aj dokumentáciu požadovanú analýzou rizík (procedúry, pracovné inštrukcie, auditné nástroje a pod.).

### 1.3.2 Fáza implementácia

Vo fáze implementácie sú zavedené všetky navrhnuté opatrenia vrátane administratívnych a fyzických. Je vykonaná verifikácia opatrení. Všetky nedostatky sú zaznamenané a následne riešené prípadnou úpravou alebo zmenou bezpečnostného opatrenia. V rámci implementácie veľkú pozornosť je potrebné venovať zaškoleniu pracovníkov na SMIB ako detailné oboznámenie sa s relevantnou dokumentáciou, podpísanie vyhlásenia o dodržiavaní dobrých bezpečnostných praktík a ochrane utajovaných skutočností, vyškolenie audítorov a pod. Výsledkom tejto fázy je rozhodnutie o uvoľnení bezpečnostného systému do prevádzky.

### 1.3.3 Fáza overovania

Funkčnosť zavedeného bezpečnostného systému je priebežne overovaná v zmysle stanovenej politiky. Je to jednak priebežné monitorovanie funkcii bezpečnostného systému a jednak vykonávanie bezpečnostných auditov. Audit môže byť zameraný aj na bezpečnostnú politiku alebo aj na analýzu rizika. Zistenia z bezpečnostného auditu sú podnetom pre nápravné opatrenia v prípade zistenia nezhody (manažment zmeny) a pre hodnotenie efektívnosti systému bezpečnosti.

### 1.3.4 Fáza používania a zlepšovania

Počas rutinnej prevádzky je bezpečnostný systém vystavený hrozbám, ktoré boli posudzované v analýze rizika ale aj hrozbám, ktoré neboli uvažované alebo prijaté opatrenia boli nedostatočné. Vzniknutý stav – udalosť informačnej bezpečnosti, v horšom prípade incident informačnej bezpečnosti je potrebné včas identifikovať a prijať účinné nápravné opatrenia. Nástrojom na odstránenie hrozby je manažment zmeny, ktorý môže byť uplatnený na všetky prvky bezpečnostného systému. Proaktívne zlepšovanie bezpečnostného systému je realizované na základe jeho priebežného monitorovania ale aj vykonávania bezpečnostných auditov.

## 1.4 Proces manažérstva rizika informačnej bezpečnosti

Riešenie bezpečnosti systému je založené na procese manažérstva rizika a najmä na jeho najdôležitejšej časti, ktorou je analýza rizika. Návod na manažérstvo rizika bezpečnosti informácii dáva štandard ISO/IEC 27005 [2].

Jednotlivé etapy procesu manažérstva rizika môžeme rozdeliť na nasledovné časti:

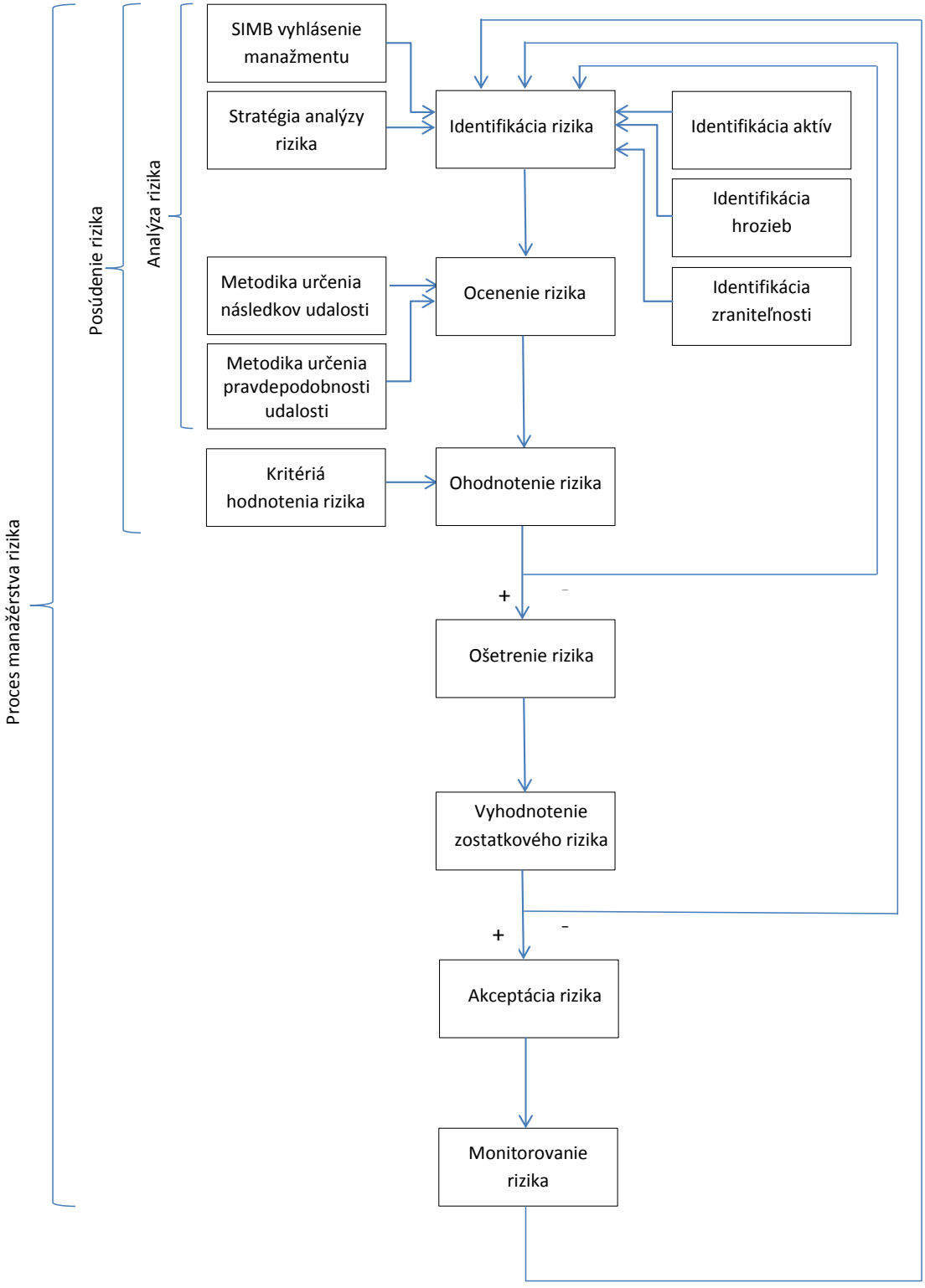
- Identifikácia rizika
- Ocenenie rizika
- Ohodnotenie rizika
- Ošetrenie rizika
- Ohodnotenie zostatkového rizika
- Akceptovanie rizika
- Monitorovanie rizika

Vzájomný vzťah medzi jednotlivými etapami procesu manažérstva rizika[1] je znázornený na obrázku 3.2.

Dôsledné vykonanie analýzy rizika je veľmi náročný proces, ktorý si vyžaduje kvalifikovaných analytikov a je aj časovo veľmi náročný. Preto boli vyvinuté automatizované nástroje na analýzu rizika, ako napr. MELISA, LAVA, CRAMM a jeho novšia verzia RAMSES (Risk Analysis and Management System for Enhanced Security). RAMSES je metodika, ktorá podporuje nielen vykonanie analýzy rizika ale aj posúdenie rizika a ponúka na výber rôzne protiopatrenia . Je to veľmi sofistikovaný nástroj na podporu informačnej bezpečnosti vhodný aj pre malé organizácie rôzneho typu [24]. Pre samostatnú identifikáciu zraniteľností je možné využiť rôzne sofistikované metódy, ako napríklad metódu Attack surface (Oblasť útoku) [16] alebo metódu založenú na protokole SCAP, viď kapitola 1.6.1.

**a) Identifikácia rizík**
Účelom identifikácie rizík je identifikovať potenciálne straty ak by nastala určitá udalosť. Vykonanie tohto procesu je podmienené zhromaždením značného množstva informácii týkajúcich sa všetkých aktív v organizácii, ktoré môžu byť predmetom útoku. Aktíva treba roztriediť z hľadiska ich hodnoty, ktorú majú pre organizáciu. Ďalej je

[1] Keďže sa riziko v systéme nevyskytuje izolovane, pre lepšie vyjadrenie podstaty bude v ďalšom texte použitý plurál tohto slova t.j. riziká.




Obr. 1.5: Proces manažérstva rizika informačnej bezpečnosti

potrebné definovať hrozby, ktorým môžu byť vystavené aktíva a aké to bude mať následky pre organizáciu, ak sa takáto udalosť stane. Identifikácia zraniteľnosti má odhaliť slabé miesta systému. Pri tejto činnosti sa zohľadňuje aj aktuálny stav riadiacich a kontrolných opatrení. Na identifikáciu rizík ale aj na celú analýzu rizika ma rozhodujúci vplyv postoj manažmentu k tvorbe tejto analýzy. Stratégia analýzy rizika určuje, či tento postoj bude formálny alebo viac detailný. Pri formálnej analýze sa identifikácia hrozieb a zraniteľností robí dotazníkovou metódou. Detailná stratégia analýzy rizík vyžaduje použiť sofistikovanejšie nástroje, ako napr. RAMSES.

**b) Ocenenie rizík**

Ocenenie rizík zahŕňa určenie závažnosti a pravdepodobnosti následkov hrozby pre organizáciu. Pre určenie závažnosti môžu byť využité kvalitatívne alebo kvantitatívne metódy. Kvalitatívna metóda je jednoduchšia, ale je viac subjektívna. Pravdepodobnosť následkov hrozby má podobnú metodológiu. Závažnosť miery rizika sa ohodnocuje napr. veľmi závažná, závažná a mierna a pravdepodobnosť následkov hrozby bude mať klasifikáciu malá, možná a vysoká. Údaje pre tento účel sa môžu získať napr. dotazníkovou metódou.

**c) Ohodnotenie rizík**

Ohodnotenie rizík sa vykoná pomocou matice rizík v našom prípade matice 3x3.

| | **Pravdepodobnosť (P)** | | |
|---|---|---|---|
| **Závažnosť (Z)** | Malá | Možná | Vysoká |
| Veľmi závažná | 3 | 6 | 9 |
| Závažná | 2 | 4 | 6 |
| Mierna | 1 | 2 | 3 |

Tabuľka 1.1: Tabuľka ohodnotenia rizík

Miera rizika MR = Z x P

Vyhodnotenie:

1. Ak miera rizika je $\geq 4$, červená oblasť tabuľky, potom riziko je neakceptovateľné;
2. Ak miera rizika je $= 3$, žltá oblasť tabuľky, potom miera rizika je prijateľná;
3. Ak miera rizika je $< 3$, zelená oblasť tabuľky, potom riziko je akceptovateľné;

Pre mieru rizika $= 3$ je zavedené monitorovanie vybraných atribútov bezpečnostného systému.

**d) Ošetrenie rizík**

Ošetrenie rizík zahŕňa štyri typy opatrení:

1. Aplikovanie vhodných preventívnych činností, ktorými sa zníži miera rizika. Napr. zálohovanie, nasadenie IDS (Intrusion detection system) a pod.
2. Vedomé akceptovanie rizík za predpokladu, že spĺňajú akceptačné kritériá, t.j. miera rizika $\leq 3$.
3. Vyhnutie sa rizikám, napr. zmena systému komunikácie.
4. Prenesenie rizika na tretiu stranu, napr. na poisťovateľa.

Ošetrenie rizika musí byť implementované a implementácia verifikovaná. Doporučuje sa vypracovať katalógový zoznam opatrení. Pre zníženie určitého rizika môžu byť vybrané aj dve, prípadne viac opatrení podľa katalógu.

**e) Ohodnotenie zostatkových rizík**
Prijatým bezpečnostným opatrením alebo opatreniami by sa miera rizika mala znížiť na akceptovateľnú úroveň. Zodpovedný tým za proces manažérstva rizika preskúma aké je zostatkové riziko po implementovaní opatrení. Pri preskúmaní zostatkového rizika zároveň posúdi, či sa zavedením bezpečnostného opatrenia nezaviedla aj ďalšia hrozba alebo sa nezvýšila miera rizika inej hrozby.

**f) Akceptovanie rizík**
Ak všetky zostatkové riziká sú akceptovateľné, potom predstaviteľ manažmentu pre informačnú bezpečnosť organizácie vypracuje tzv. Vyhlásenie o aplikovateľnosti, ktoré obsahuje ciele riadenia a opatrenia na minimalizovanie miery rizika a to minimálne v rozsahu podľa Prílohy A štandardu ISO/IEC 27001.

**g) Monitorovanie rizík**
Organizácia musí zabezpečiť neustále monitorovanie rizík, či sa v dôsledku nejakých zmien v systéme bezpečnosti nezmenila závažnosť alebo pravdepodobnosť výskytu hrozby, následkom čoho by bolo riziko preklasifikované do neakceptovateľnej úrovne. Ďalej je potrebné zaviesť monitorovanie jednotlivých prvkov systému manažérstva rizika bezpečnostného systému, najmä zmien aktív, hrozieb a zraniteľností aktív alebo opatrení.

## 1.5 Bezpečnostný audit

Podľa štandardu ISO/IEC 27001 organizácia musí v plánovaných intervaloch vykonávať interné audity s cieľom určiť, či ciele riadenia, opatrenia, procesy a postupy jej systému manažérstva informačnej bezpečnosti [5]:

**a)** Vyhovujú požiadavkám tejto medzinárodnej normy a relevantnej legislatívy alebo predpisov;

**b)** Vyhovujú identifikovaným požiadavkám informačnej bezpečnosti;

**c)** Sú efektívne implementované a udržiavané;

**d)** Pôsobia podľa očakávania.

Návod ako vykonávať audit systému manažérstva bezpečnosti informácii dáva štandard ISO/IEC 27007 [3]. Tento štandard je aplikovateľný pre vykonávanie interných, ale aj externých auditov. Štandard ISO/IEC 27007 v podstate rozširuje požiadavky normy ISO 19011 na vykonávanie auditov manažérskych systémov o špecifiká informačnej bezpečnosti.

Metodika vykonávania bezpečnostných auditov je založená na zhromažďovaní dôkazov auditu t.j. informácii, ktoré sú verifikovateľné a teda sú spoľahlivé pre prijímanie rozhodnutí. Článok 6.4.6.1 štandardu ISO/IEC 27007 uvádza nasledovné požiadavky na zhromažďovanie a overovanie informácii:

Zhromažďovanie informácii a dôkazov o tom, že procesy a opatrenia sú implementované a sú efektívne, tvorí dôležitú časť auditu SMIB. Možné metódy ako zhromažďovať príslušné informácie počas auditu zahrňujú [3]:

**a)** Preskúmanie informačných aktív a procesov a opatrení SMIB, ktoré sú pre ne zavedené

**b)** Použitie automatizovaných nástrojov pre vykonávanie auditu

Z uvedeného vyplýva, že použitie automatizovaných nástrojov pre vykonanie bezpečnostného auditu môže byť účinným prostriedkom pre vyhodnotenie efektívnosti prijatých bezpečnostných opatrení.

### 1.5.1 Manažérstvo bezpečnostného auditu

Bezpečnostný audit je vykonávaný kompetentným audítorom, t.j. audítor musí preukázať dostatočné znalosti a zručnosti na dosiahnutie plánovaných výsledkov. Pre audítora platí všeobecná zásadaeho nezávislosti od auditovaných činností. Problematika posúdenia kvalifikácie audítora je nad rámec bakalárskej práce, a preto sa ňou nebudem zaoberať. Podrobnejšie informácie o požiadavkách na kompetentnosť a hodnotenie audítora možno nájsť v štandardoch ISO/IEC 27007 a EN ISO 19011.

Vykonanie bezpečnostných auditov systému môžeme rozdeliť na dve fázy. Na fázu plánovania – program auditu a fázu realizácie.

Program auditu definuje dielčie bezpečnostné audity, ktoré majú byť vykonané v nasledujúcom období spravidla v nasledujúcom roku. Obsahuje základnú metodológiu auditu a zabezpečenie zdrojov. Rozsah programu auditu závisí od veľkosti organizácie, resp. množstva a kritickosti systémov, zamerania organizácie, hodnoty aktív atď. Jednotlivé fázy procesu manažérstva programu auditu sú uvedené na obrázku 1.6 a na obrázku 1.7 sú znázornené fázy realizácie bezpečnostného auditu.

#### Určenie cieľov programu auditu

Ciele programu auditu majú korešpondovať s cieľmi a politikou systému manažérstva informačnej bezpečnosti. Ciele programu zohľadňujú aktuálny stav hrozieb a súvisiacich rizík bezpečnosti informácii, ktorým je vystavená organizácia. Podľa zamerania auditu ďalej sa zohľadňujú aj legislatívne požiadavky a požiadavky ISO/IEC 27001.

#### Vytvorenie programu auditu

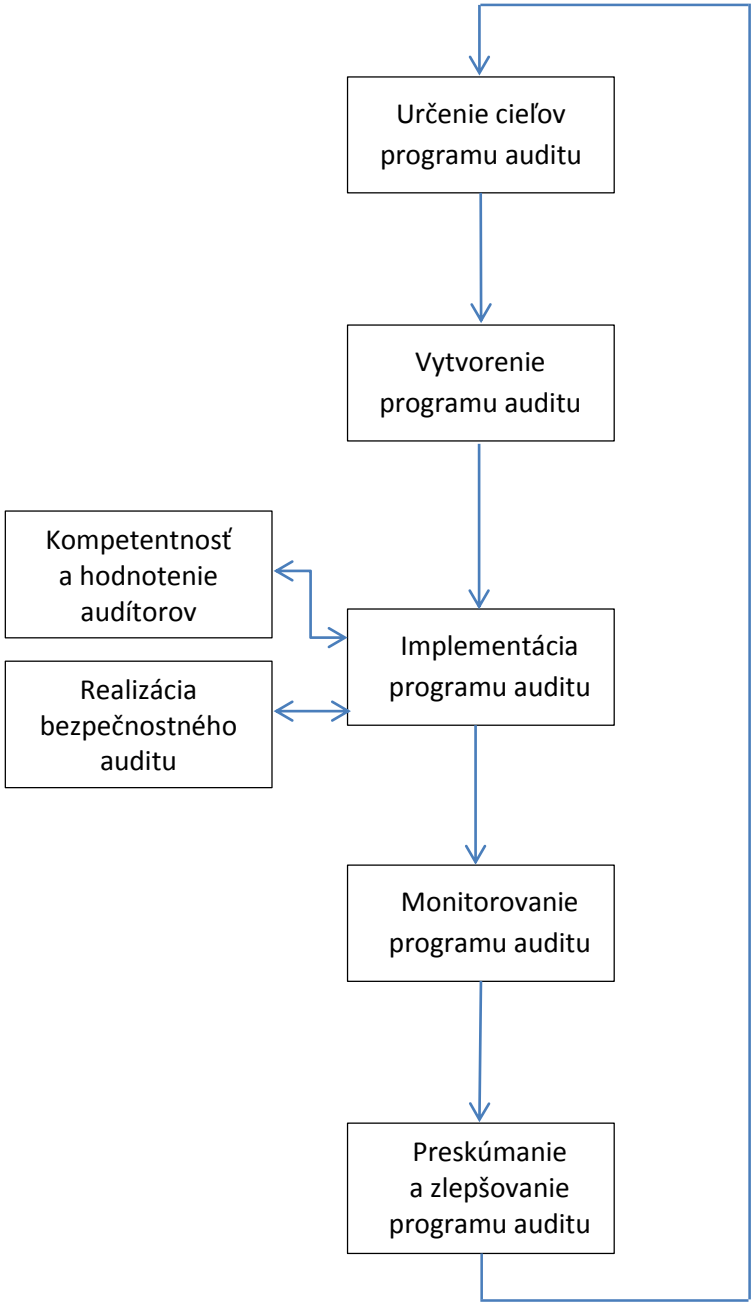
Program auditu tvorí manažér poverený vedením zodpovednosti za systém manažérstva informačnej bezpečnosti (SMIB). V dielčích bezpečnostných auditoch zohľadňuje ciele auditu, navrhuje zameranie bezpečnostného auditu a jeho kritériá, zostavuje auditný tým, navrhuje vedúceho audítora, plánuje časový harmonogram bezpečnostných auditov a identifikuje hodnotí riziká, ktoré môžu nastať pri realizáciii bezpečnostných auditov. Program auditu preskúma a schváli vrcholový manažment.

#### Implementácia programu auditu

Po schválení programu auditu manažér pre SMIB informuje vedúcich audítorov o ich menovaní za vykonanie bezpečnostných auditov. Pre efektívne implementovanie programu auditu je potrebné vyjasniť s vedúcim audítorom najmä nasledovné skutočnosti [1].

**a)** Cieľ bezpečnostného auditu;

**b)** Kritériá bezpečnostného auditu a akékoľvek referenčné dokumenty;




Obr. 1.6: Manažérstvo programu auditu

**c)** Predmet bezpečnostného auditu, vrátane organizačných a funkčných jednotiek (informačných systémov), ktoré sa majú auditovať;

**d)** Metódy a postupy bezpečnostného auditu;

**e)** Zloženie audítorského týmu;

**f)** Skutočnosti týkajúce sa dôvernosti a bezpečnosti informácii;

**g)** Výsledky z predchádzajúceho bezpečnostného auditu a následné vykonané činnosti

Kritériá bezpečnostného auditu môžu byť napr.:

**a)** Legislatívne a zmluvné požiadavky prijaté organizáciou;

**b)** Zhodnosť s politikami a cieľmi organizácie;

**c)** Výsledky preskúmania vedenia SMIB a nápravných opatrení;

**d)** Efektívnosť prijatých opatrení pre zníženie rizika;

**e)** Metodika posúdenia rízík bezpečnosti informácii

**f)** Vyhlásenie o aplikovateľnosti

Metódy a postupy bezpečnostného auditu musia byť vypracované a schválené pred začatím auditu v zmysle zásad správnej dokumentačnej praxe. Použitie automatizovaných nástrojov na vykonanie bezpečnostného auditu musí byť vykonané bez akýchkoľvek zmien v systéme a bez akýkoľvek zásahov do systému. V prípade, že tento prístup nie je možný, v systémovej dokumentácii musí byť stanovený pre tento účel detailný postup (napr. vytvorenie záložnej kópie aktíva a jej následné zmazanie po skončení auditu). Vyvinuté vlastné automatizované nástroje na vykonanie bezpečnostného auditu majú byť pred prvým použitím validované. Majú byť prijaté opatrenia na ochranu nástrojov auditu tak, aby nemohli byť zneužité.

#### Monitorovanie programu auditu

Monitorovanie programu auditu podáva informácie o priebehu plnenia programu auditu, informácie o odchýlkach a hodnotenie audítorov. Výsledok monitorovania môže byť podnetom na zmenu v programe auditu.

#### Preskúmanie a zlepšovanie programu auditu

Manažér pre SMIB vykonáva minimálne aspoň raz ročne preskúmanie programu auditu. Zdrojom pre preskúmanie sú správy z bezpečnostných auditov a výsledky monitorovania programu auditu. Výstupom je správa pre preskúmanie SMIB vrcholovým manažmentom, v ktorej sú navrhnuté možnosti pre zlepšovanie programu auditu a náväzných bezpečnostných auditov v organizácii (napr. návrh nových metód pre automatizované vykonávanie bezpečnostných auditov).

### 1.5.2 Začatie bezpečnostného auditu

Začatím bezpečnostného auditu sa rozumie úvodný kontakt vedúceho audítorského týmu s predstaviteľom auditovanej organizačnej jednotky za účelom dohodnutia podrobností o realizácii bezpečnostného auditu (prítomnosť zainteresovaných osôb na audite, spresnenie času auditu, miesta a pod.).


Obr. 1.7: Realizácia bezpečnostného auditu

### 1.5.3 Príprava na činnosti bezpečnostného auditu

Zahŕňa prípravu relevantných dokumentov k auditu ako program auditu, pracovne inštrukcie platné pre predmet bezpečnostného auditu, inštrukcie pre automatizované nástroje auditu, auditný checklist, formuláre na záznam súvisiacich skutočností a pod. Na základe podkladov vedúci audítor pripraví realizačný plán bezpečnostného auditu, v ktorom sú podrobne popísané jednotlivé kroky bezpečnostného auditu, určené zodpovednosti pre auditný tým a časový harmonogram vykonania jednotlivých činností bezpečnostného auditu. Realizačný plán bezpečnostného auditu schvaľuje manažér pre SMIB. Získavanie informácii vzorkovaním má byť založené na použití štatistických metód, prípadne na základe expertného posúdenia.

### 1.5.4 Realizácia činností bezpečnostného auditu

Vlastný bezpečnostný audit je zameraný na zhromažďovanie dôkazov auditu s cieľom zistiť, či sú splnené kritériá auditu. Zistenia z bezpečnostného auditu môžu dokazovať zhodu alebo nezhodu s kritériami bezpečnostného auditu. Všetky dôkazy auditu sa musia zaznamenať. K tomu sa môže využiť checklist, pripravený formulár alebo údaje sú zaznamenávané elektronicky. Metódy auditovania závisia od zamerania auditu, t.j. aký prvok SMIB sa audituje (druh informačného aktíva, proces SMIB, bezpečnostné opatrenie SMIB). Metóda auditovania je určená v realizačnom pláne bezpečnostného auditu a môže to byť napríklad:

- Ústny pohovor s následnou kontrolou;
- Preskúmanie dokumentácie a záznamov SMIB;
- Pozorovanie javov;
- Kontrola súborov určených pre tento účel (auditný log);
- Testy od dodávateľov aplikácii;
- Využitie vlastných testovacích skriptov.
- Využitie sofistikovaných nástrojov pre testovanie bezpečnosti operačných systémov a aplikácii (OpenSCAP, Nessus a i.)

Ak sa počas auditu zistí nejaké významné riziko, musí sa to bez meškania oznámiť vrcholovému manažmentu. Akúkoľvek požiadavku na zmenu plánu bezpečnostného auditu, ktorá sa objaví počas priebehu bezpečnostného auditu musí manažér SMIB preskúmať a schváliť. Po ukončení činností zisťovania dôkazov auditu nasleduje vyhodnotenie zistení bezpečnostného auditu. U zistených nezhôd audítor klasifikuje ich závažnosť a identifikujú sa príležitosti na zlepšenie. Výsledky z bezpečnostného auditu vedúci audítor prezentuje na záverečnom rokovaní všetkých zainteresovaných strán na audite.

### 1.5.5 Príprava a distribúcia správy z bezpečnostného auditu

Vedúci audítor zistenia z auditu spracuje do správy o vykonaní bezpečnostného auditu na predpísanom formulári. Vedúci audítor vyhodnotí všetky plánované aktivity podľa realizačného plánu bezpečnostného auditu. Doplní aj všetky neplánované skutočnosti ak boli prítomné. Správu z bezpečnostného auditu podpisuje vedúci auditu a aj audítori ak bol zostavený auditný tým. Vedúci audítor auditné checklisty zaradí do príloh správy. Správa z bezpečnostného auditu je zaslaná auditovanej organizačnej jednotke a manažérovi pre SMIB. Správa je uchovávaná aj v elektronickej forme.

### 1.5.6 Vykonanie následného bezpečnostného auditu

Ak výsledkom zistení boli skutočnosti, ktoré indikujú na výskyt udalosti informačnej bezpečnosti, potom je potrebné prijať nápravné opatrenia resp. preventívne opatrenia. Opatrenia môžu mať zameranie napr. na opakované posúdenie rizika a prijatie účinnejších bezpečnostných opatrení, v jednoduchších prípadoch môže byť zavedené monitorovanie určitých atribútov systému. V prípade zistenia závažnej nezhody manažér SMIB neodkladne informuje o nezhode vrcholové vedenie za účelom prijatia okamžitých nápravných opatrení. Verifikácia efektívnosti prijatých opatrení je súčasťou následného, niekedy mimoriadneho bezpečnostného auditu.

## 1.6 U.S. Government prístup k zabezpečeniu bezpečnosti informácií

Vláda Spojených štátov prijala zákon, aby každá federálna organizácia vytvorila, dokumentovala a zaviedla program na zabezpečenie informačnej bezpečnosti tzv. FISMA (Federal Information Security Management Act) [20]. Naplnenie požiadaviek stanovených v tomto nariadení je náročné na aplikáciu v danej inštitúcii, náročné na čas implementovania ako aj náchylné na možné omyly, kedže nie sú využívané štandardizované nástroje.

NIST (National Institute of Standards and Technology) navrhol program, ktorý by úľahčil splnenie požiadaviek FISMA vytvorením špecifických štandardov SCAP (Security Content Automation Protocol). Tento súbor štandardov je určený pre vládne organizácie, ale môže ho použiť akákoľvek iná organizácia.

### 1.6.1 Security Content Automation Protocol (SCAP)

SCAP bol vydaný ako balík špecifikácii v štandardizovanom formáte XML v roku 2009, pričom technické špecifikácie boli publikované v NIST Special Publication 800-126 [23]. Súbor štandardov je navrhnutý tak, aby organizoval a meral charakteristiky informačnej bezpečnosti ako aj referenčné dáta, napríklad identifikátory softvérových záplat a následne vyhodnotil systémovú bezpečnosť, prípadne identifikoval znaky jej narušenia.

SCAP môže byť použitý na automatické monitorovanie bezpečnosti systémov s využitím štandardizovaného checklistu bezpečnosti konfigurácie. Checklist je možné prispôsobiť na podmienky preverovaného systému. Nastavenie v checkliste je porovnávané s aktuálnou systémovou konfiguráciou s cieľom potvrdiť zhodu s checklistom a teda identifikovať odchýlky. Táto činnosť by mala byť vykonaná pred uvedením do prevádzky systému v rámci jeho validácie. Porovnávanie aktuálneho stavu s checklistom môže byť vykonávané ako súčasť bezpečnostného auditu alebo priebežného monitorovania bezpečnosti systému.

#### Komponenty SCAP

Protokol SCAP v prvej verzi obsahoval 6 kompotentov: XCCDF, OVAL®, CCE, CPE™, CVE® a CVSS. V druhej finálnej verzi, vydanej v roku 2010, ktorá nesie označenie 1.1, bol definovaný framework OCIL. Posledná finálna verzia označená 1.2, ktorá bola vydaná v septembri 2011, obsahuje dohromady 11 komponentov [25]:

- **XCCDF: The Extensible Configuration Checklist Description Format**
  Je špecifikácia jazyka pre tvorbu checklistov a benchmarkov. Obsah XCCDF dokumentu v jazyku XML (Extensible Markup Language) popisuje kolekciu pravidiel pre bezpečnú konfiguráciu systému, ako aj dátový model a formát pre ukladanie výsledkov, pričom zachováva prenositeľnosť medzi platformami [26].

- **OVAL®: Open Vulnerability and Assessment Language**
  Jazyk štandardizuje tri hlavné kroky v procese posudzovania [11]:

  1. reprezentácia informácii o konfigurácii systému pre testovanie
  2. popis špecifických stavov systému
  3. podávanie správ s výsledkami

- **OCIL: Open Checklist Interactive Language**
  Umožňuje zostaviť súbor otázok, ktoré budú následne predložené užívateľovi, aby na základe jeho odpovedí mohli byť vymenované opatrenia [27]:

  1. definícia otázky
  2. definícia možných odpovedí, z ktorých je možné vyberať
  3. definícia opatrení vyplývajúcich z odpovedí užívateľa
  4. vymenovanie sady opatrení

- **Asset Identification**
  Táto špecifikácia opisuje účel identifikácie aktív, ich datový model a metódy na ich identifikáciu. Uvádza tiež príručku a množstvo prípadov použitia identifikácie aktív [28].

- **ARF: Asset Reporting Format**
  Popisuje dátový model prenosového formátu informácií o aktívach, čím uľahčuje vyhodnotenie a koleráciu [29].

- **CCE™: Common Configuration Enumeration**
  Poskytuje jedinečnú identikáciu problému konfigurácie systému s cieľom uľahčiť a urýchliť proces kolerácie medzi rôznymi zdrojmi a nástrojmi [30].

- **CPE™: Common Platform Enumeration**
  Je štandardizovaná metóda, ktorá identifikuje a popisuje abstraktné triedy výrobkov, aplikácii, operačných systémov a hardvérových zariadení. Nástroje IT manažmentu môžu zhromažďovať informácie o nainštalovaných produktoch, pričom indentifikovanie pomocou ich CPE názvov pomáha úplne alebo čiastočne automatizovať rozhodnutia týkajúcich sa týchto aktív. Napríklad, zistením prítomnosti abstraktnej triedy softvéru môže viesť ku kontrole známych zraniteľností v softvéri alebo ku kontrole konfigurácie daného softvéru voči bezpečnostnej politike organizácie. Tento príklad ukazuje použitie CPE názvu ako štandardizovaného zdroja informácií pre presadzovanie a overovanie zásad pre IT manažment [31].

- **CVE®: Common Vulnerabilities and Exposures**
  Pomáha k dosiahnutiu interoperability bezpečnostných nástrojov a zdieľaniu informácií medzi nimi [14]:

  – zahŕňa a rozlišuje všetky známe zraniteľnosti
  – každej zraniteľnosti priraďuje štandardný a jedinečný názov
  – existuje nezávisle na množstve rôznych perspektív
  – je verejne dostupný a voľne šíriteľný bez obmedzení

- **CVSS: Common Vulnerability Scoring System**
  Je metrika na ohodnotenie závažnosti zraniteľností na posúdenie miery rizík. CVSS sa skladá z troch základných metrík [32]:

  1. základná – hodnotí prirodzené kvality zraniteľností
  2. dočasná – charakteristiky zraniteľností, ktoré sa menia v priebehu času

3. enviromentálna – charakteristiky zraniteľností, ktoré závisia na užívateľskom prostredí

- **CCSS: Common Configuration Scoring System**
  Tento systém metrík je odvodený od CVSS. Obsahuje súbor metrík na ohodnotenie závažnosti vzniknutých zraniteľností v dôsledku nevhodnej konfiguráci softvéru. CCSS bol vyvinutý, aby poskytol pomoc organizáciam pri rozhodnutí, ako by mali byť riešené problémy s konfiguráciou v oblasti bezpečnosti. Taktiež poskytuje údaje, ktoré môžu byť použité v kvantitatívnom posúdení celkovej bezpečnosti sytému. [21].

- **TMSAD: Trust Model for Security Automation Data**
  Tento model dôvery je zložený z odporúčaní, ako využiť existujúce špecifikácie. Vzhľadom k tomu, že informácie v oblasti zabezpečenia sa primárne vymieňajú za použitia XML, zameranie tohto modelu je na spracovanie XML dokumentov [33].

#### National Vulnerability Database (NVD)

Vznikla ako projekt vlády Spojených štátov v roku 2005 a ako produkt NIST Information Technology Laboratory (ITL), Computer Security Division (CSD). Slúži ako repozitár pre dáta o softvérových zraniteľnostiach a pre nastavenia konfigurácie s využitím otvorených štandardov poskytovať spoľahlivé a interoperabilné informácie o zraniteľnostiach, vplyve metriky, technických metódach posudzovania a o identifikácii údajov o produktoch. Pre zlepšenie interoperability dát NVD zverejňuje údaje založené na štandarde SCAP.

NVD poskytuje informácie o charakteristike a závažnosti stoviek nových zraniteľností a ich variantov objavených každý mesiac. Poskytované informácie môžu byť využívané vo verejnom aj v súkromnom sektore. Verejnosť tak môže reagovať a priorizovať zraniteľnosti s vyššou prioritou za účelom ochrany dôležitých systémov.

NIST poskytuje priebežnú analýzu novoobjavených chýb zabezpečenia CVE a prideľuje základnú metriku CVSS pre každú zraniteľnosť. Priebežná analýza a vyhodnocovanie pomáha používateľom NVD pochopiť potenciálnu závažnosť každej zraniteľnosti a pomáha používateľom stanoviť priority činností riadenia bezpečnosti. NIST spolupracuje s inými národnými organizáciami ako Japan Vulnerability Network (JVN) a Spanish National Institute of Communication Technologies (INTECO) s cieľom rozšíriť medzinárodný dosah a zlepšiť kvalitu publikovaných informácií [12].

## 1.7 Center for Internet Security (CIS)

Je nezisková organizácia, ktorá od roku 2000 pomáha organizáciam posúdiť a zlepšiť ich kyberbezpečnosť. Kladie si za cieľ zvýšiť pripravenosť a reakciu verejného a súkromného sektora na bezpečnostné hrozby. CIS slúži ako kľúčový zdroj informácii v oblasti počítačovej bezpečnosti, publikuje bezpečnostné odporúčania a benchmarky na preverenie bezpečnosti konfigurácií systémov, ďalej poskytuje automatizované nástroje pre posudzovanie bezpečnosti, metriky a certifikáciu bezpečnostných softvérových produktov [19].

### 1.7.1 CIS Benchmarky

Poskytujú odporúčané kritéria konfigurácie, zameranú na zabezpečenie systému, ktoré môžu byť využité pre širokú škálu technológií, vrátane serverov a personálnych operačných sys-

témov, webových prehliadačov, mobilných zariadení. Popisujú tiež špecifické postupy, ako uplatňovať tieto odporúčania a audítorské postupy [19].

# Kapitola 2

# Prehľad existujúcich nástrojov

Táto kapitola obsahuje stručné charakteristiky najznámejších nástrojov určených na automatizované testovanie operačných systémov a ich konfigurácií vzhľadom k špecializovanému štandardu SCAP a jeho komponentom, prípadne odporúčaniam a kritériam CIS.

## 2.1 OpenSCAP

OpenSCAP vznikol ako open source projekt, súčasťou ktorého je konzolový nástroj oscap a jeho grafická alternatíva SCAP Workbench. Knižnica OpenSCAP implementuje štandardy SCAP a jeho komponenty. Pri spracovaní checklistov uplatňuje predovšetkým jazyk XCCDF v kombinácii s inými špecifikáciami ako CPE, CCE a OVAL. OpenSCAP je certifikovaný NIST [34].

## 2.2 CIS Configuration Assessment Tool (CIS-CAT)

Je nástroj od CIS napísaný v jazyku Java určený pre analýzu a posúdenie stavu bezpečnosti configurácie systémov a ich aplikácii. Používa vlastné benchmarky a checklisty popísané vo formáte XCCDF, voči ktorým preveruje configuráciu cieľového systému. Výsledky reprezentuje skóre na škále od 0 do 100.

Nástroj umožňuje preverovať systém len lokálne, sieťové skenovanie nie je podporované. IS-CAT môže byť ovládaný konzolovým rozhraním, rovnako ako cez grafické rozhranie. Podporuje systémy Microsoft Windows od verzie XP, Sun Solaris, IBM AIX, HP-UX a Linux platformy, pričom vyžaduje Java Runtime Environment (JRE) vo verzi v1.6.0 alebo vyššej [7].

## 2.3 Nessus®, SecurityCenter™, SecurityCenter™ CV

Produkty spoločnosti Tenable Network Security patria k svetovo najrozšírenejším v oblasti detekcie, skenovania a auditovania systémov. Poskytujú množstvo funkcii na riadenie a kolaboráciu. Umožňujú užívateľom, prípadne celým skupinám, navzájom zdieľať plánovanie, politiky a výsledky testov [10].

## 2.4 Qualys SCAP Auditor

Riešenie od spoločnosti Qualys vo významnej miere podporuje štandardy SCAP, pričom uplatňuje všetky jeho komponenty. Rovnako je možné vytvoriť a použiť vlastné politiky definované v jazykoch OVAL alebo XCCDF. Pre výstup výsledkov je možné vybrať z viacerých formátov, podporovaný je okrem CVS a XML aj formát ARF [8].

## 2.5 Ďalšie nástroje poskytujúce automatické testovanie OS

Existujú aj ďalšie nemenej významné podobné nástroje od rôznych spoločností, ktoré poskytujú automatické testovanie bezpečnosti operačných systémov voči štandardu SCAP, ktoré poskytujú rovnaké alebo podobné funkcie:

- Lynis a Lynis Enterprise od spoločnosti CISOFY
- Secutor Prime spoločnosti ThreatGuard™
- OpenVAS publikovaný pod licenciou GNU GPL
- SAINT 8 Security Suite od spoločnosti SAINT®
- McAfee Policy Auditor od McAfee patriaca Intel®
- Tripwire Enterprise od Tripwire
- BMC Server Automation a BMC Client Management od firmy BMC

# Kapitola 3

# Nástroj pre bezpečnostný audit

Na zabezpečení operačných systémov, ako vrstvy medzi aplikačnou vrstvou a vrstvou hardware, viď obrázok 3.1, závisí bezpečnosť ostatných služieb, systémov a aplikácii. Predvolené nastavenie, s ktorým sú operačné systémy nasadené, nespĺňa z bezpečnostného hľadiska všetky požiadavky zákazníkov a organizácii, hoci výrobcovia systémov hľadajú rovnováhu medzi bezpečnosťou a používateľskou prívetivosťou, pričom sa snažia nastaviť bezpečnostnú politiku najstriktnejšie, ako je len možné. Táto úloha nie je jednoduchá, pretože bezpečnostné požiadavky sa líšia z počítača na počítač, z organizácie na organizáciu, z personálneho počítača na server, ktorý môže tvoriť architektúru cloudu.

Niektoré požiadavky sú od systému nezávislé, ako napríklad požiadavky na používateľké účty, ako sú minimálna dĺžka hesla, doba platnosti hesla, ale aj iné. Požiadavky sa líšia vzhľadom na rôznorodosť operačných systémov, a to aj napriek tomu, že sa niektoré hlavne Unix-like systémy snažia dodržiavať aplikačné rozhranie z rodiny POSIX štandardov a niektoré bezpečnostné požiadavky sú definované aj priamo v POSIX štandardoch. Napriek tomu, že niektoré požiadavky sú na platforme nezávislé, je potrebné brať do úvahy aj možné rozdiely v ich implementácii [17].

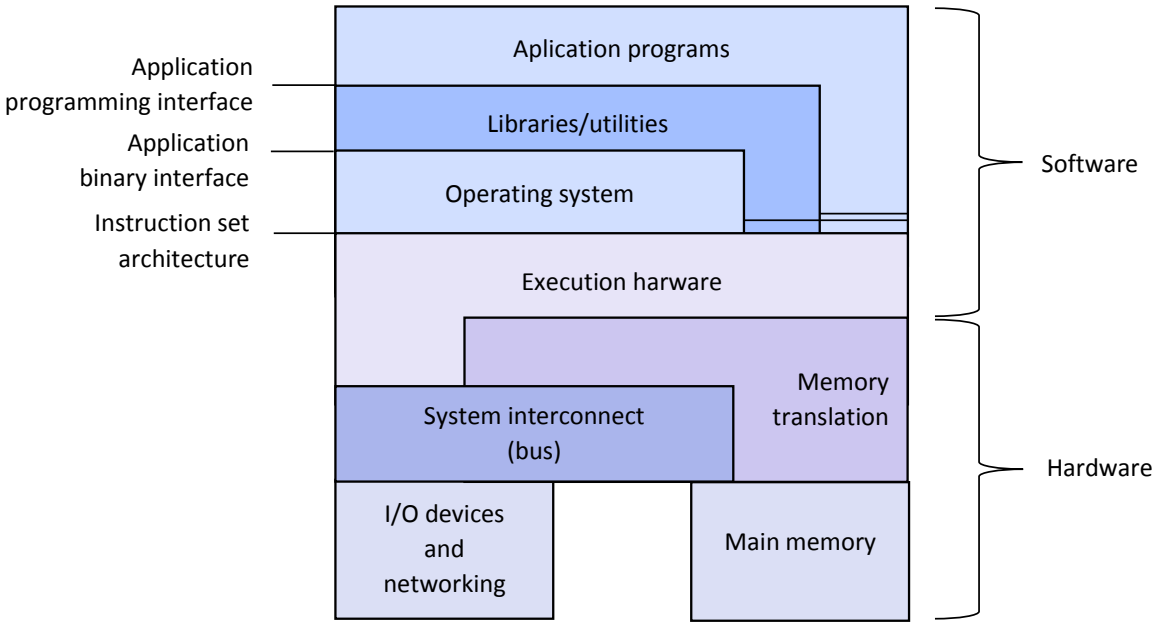
## 3.1 Špecifikácia požiadavkov

Ako bolo uvedené v kapitole 1.2 pri návrhu a implementácii nástroja určeného pre bezpečnostný audit bolo treba zohľadniť prostredie systému manažérstva bezpečnosti informácii podľa modelu ISO/IEC 27001. Preto vznikla požiadavka implementovať multiplatformový nástroj pre bezpečnostný audit, ktorý by bol použiteľný na preukázanie zhody konfiguračných vlastností operačných systémov s požiadavkami štandardu ISO/IEC 27001, rovnako aj s využitím odporúčaní CIS a štandardov z balíka SCAP. Auditný nástroj má slúžiť na overenie opatrení prijatých na zníženie rizika podľa Prílohy A ISO/IEC 27001. Podrobnejšie informácie o opatreniach a cieľoch riadenia boli získané zo štandardu ISO/IEC 27002 [6]. Nástroj má byť implentovaný v skriptovacom jazyku bash, čo je jednou z požiadaviek.

Z Prílohy A štandardu ISO/IEC 27001 boli vybraté nasledovné kategórie informačnej bezpečnosti súvisiace s bezpečnosťou operačných systémov:

- Riadenie prístupu do systému a k aplikáciám
- Ochrana proti malware
- Monitorovanie OS

- Audit OS
- Správa bezpečnosti siete



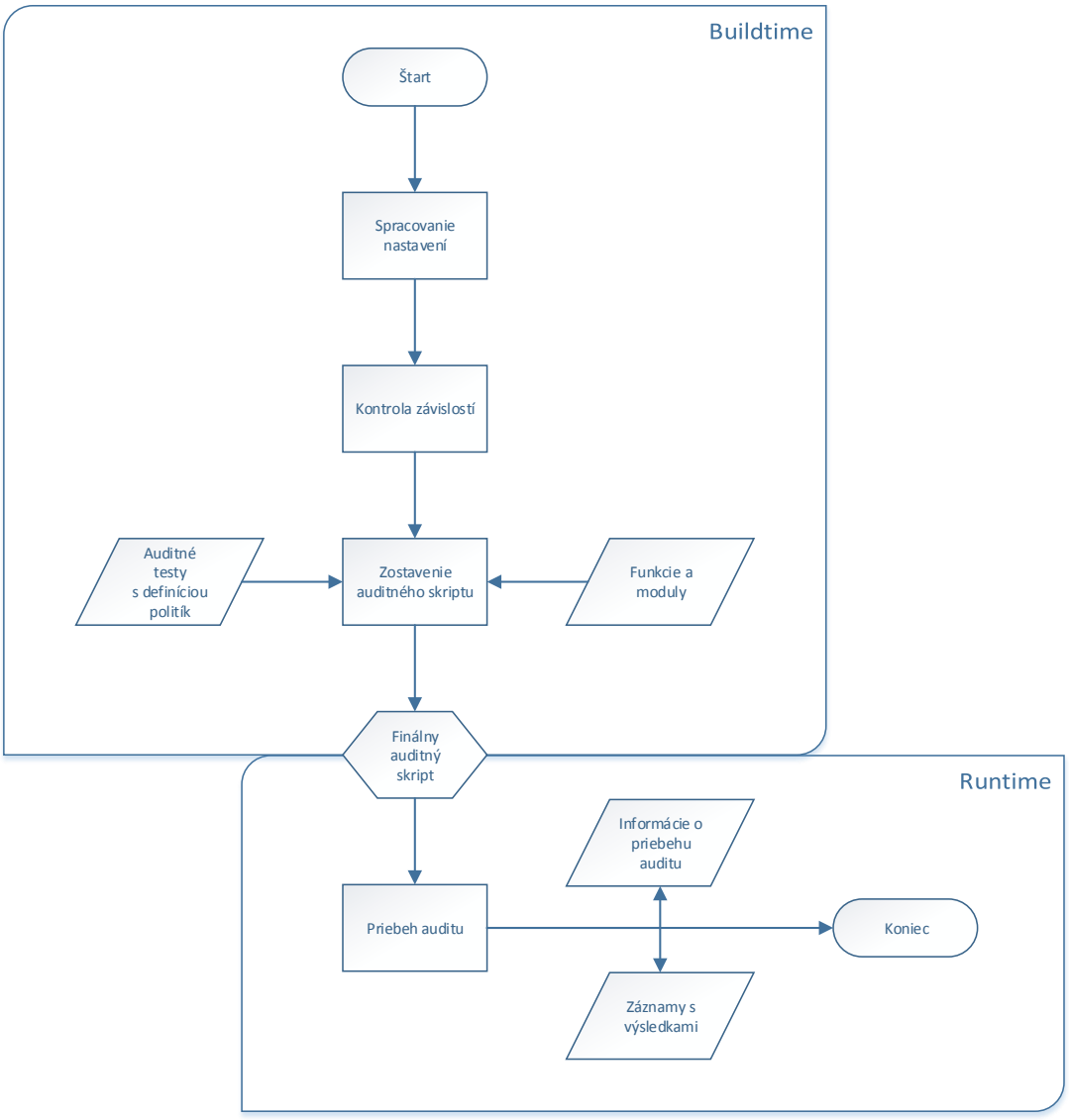

Obr. 3.1: Štruktúra software a hardware počítača [22]

## 3.2 Analýza a návrh nástroja

Pri analýze a návrhu je potrebné vychádzať z požiadavkov kladených na projekt, ktoré je možné rozdeliť na viac častí. Ďalším cieľom tejto etapy vývoja je vytvorenie architektúry nástroja, definovanie vstupov a výstupov. Pre popis hlavného návrhu systému je využívaný statický návrh vytvorený modelovacím jazykom UML. Tento vzniknutý diagram tried vizualizuje návrh tried, ich popis a definíciu rozhraní.

### 3.2.1 Architektúra nástroja

Grafické zobrazenie činnosti nástroja zobrazuje diagram na obrázku 3.2. Ako je možné vidieť, celý proces možno rozdeliť na proces zostavovania auditného skriptu (buildtime) a následne na proces behu skriptu (runtime). Prvý proces reprezentuje činnosť navrhovaného auditného nástroja, ktorého úlohou je zostaviť auditný skript z definíc bezpečnostných politík pre špecifickú verziu operačného systému, špecifikovanú ako parameter príkazového riadka. Druhý proces zobrazuje už samotný beh zostaveného auditného skriptu. Vstupom celého procesu sú nastavenia špecifikované ako parametre pri spustení nástroja. Jedná sa predovšetkým o už spomínaný typ a verziu operačného systému, ďalej o špecifikovanie auditných politík, ale aj o ďalšie voľby upravujúce správanie behu nástroja.




Obr. 3.2: Priebeh zostavenia a následného spustenia zostaveného auditného skriptu

### 3.2.2 Návrh tried

Návrhnuté triedy, ktoré boli implementované zobrazuje obrázok 3.3. Zobrazuje diagram tried, na ktorom možno vidieť ich grafickú reprezentáciu a vzťahy medzi nimi. Uvedené triedy predstavujú návrh jednotlivých častí auditného nástroja:

- **lib** – trieda knižníc
- **share** – trieda na systéme nezávislých knižníc
- **src** – trieda definujúca auditné politiky
- **build** – trieda implementujúca správanie nástroja

- **default_variables** – trieda predvolených nastavení zostavovaného skriptu
- **error_mssgs** – trieda chybových hlásení
- **functions** – trieda funkcii zostavovaného skriptu
- **lib_build** – trieda knižníc auditného nástroja
- **lib_redhat** – trieda implementujúca podporu systému Red Hat Enterprise Linux
- **lib_solaris** – trieda implementujúca podporu systému Solaris
- **lib_variables** – trieda nastavení auditného nástroja
- **help** – trieda nápovedy zostavovaného skriptu
- **info** – trieda informácii o zostavenom skripte
- **usage** – trieda nápovedy auditného nástroja

## 3.3 Popis riešenia

Problému implementácie tried zabezpečujúcich podporu testovania rozdielnych operačných systémov bol vyriešený implementovaním metód zabezpečujúcich spúšťanie špecifických politík len pre systém, pre ktorý sú charakteristické. Podobným prístupom bol riešený aj problém v rozdieloch medzi jednotlivými verziami operačných systémov. Vďaka tomuto riešeniu je možné spúšťať špecifické príkazy nasledujúcim spôsobom:

```
redhat           echo "Všetky verzie Red Hat Enterprise Linux"
solaris          echo "Všetky verzie Solaris"
redhat v4 v5 v6  echo "Red Hat Enterprise Linux vo verzii 4, 5 a 6"
solaris v11      echo "Solaris verzie 11"
```

Kde kľúčový identifikátor:

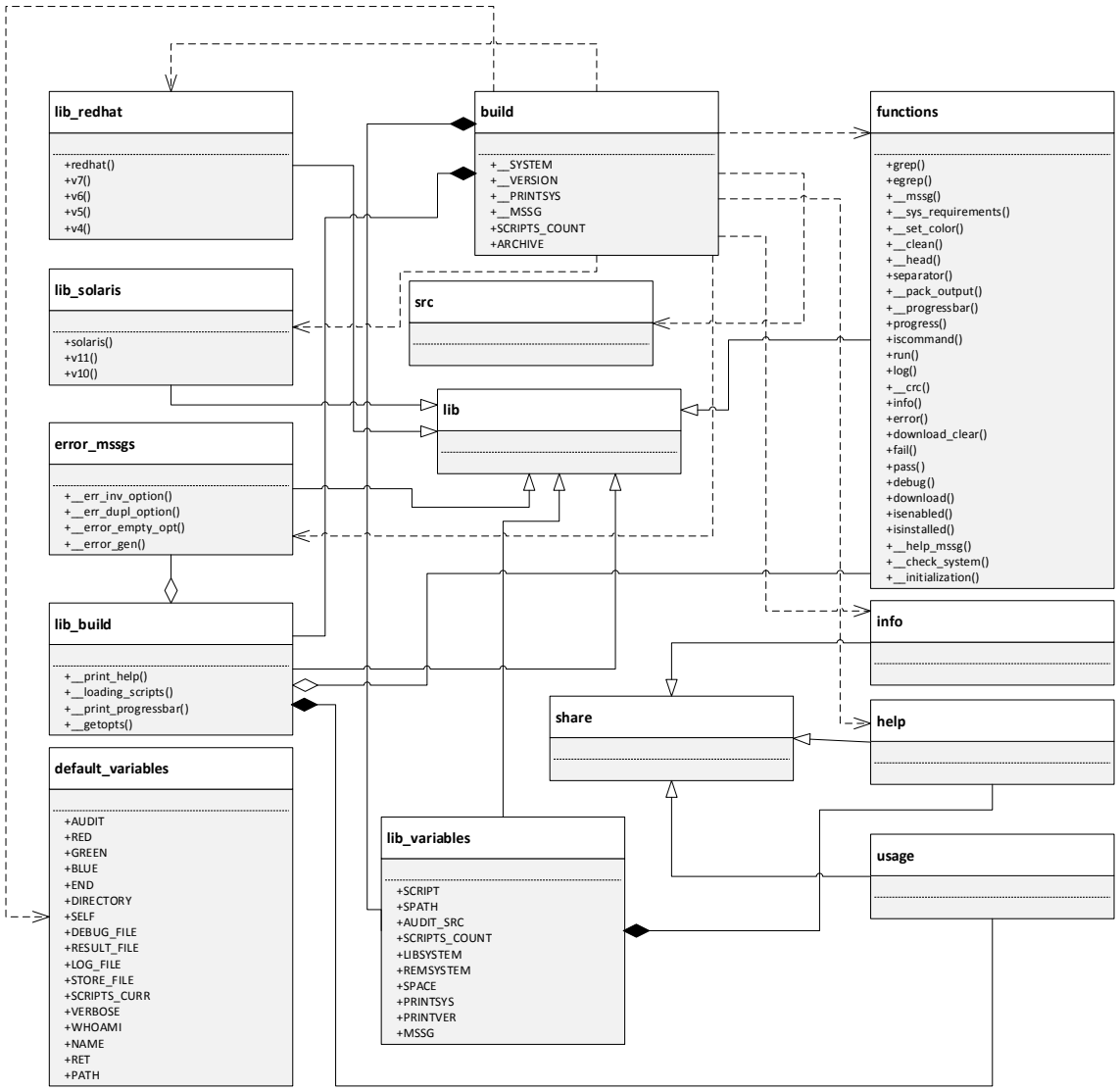
| | |
|---|---|
| `redhat, solaris` | špecifikuje operačný systém |
| `v4, v5, v6, v11` | špecifikuje jeho verziu |

## 3.4 Popis implementácie

Riešenie implementácie vychádza z analýzy a návrhu nástroja popisovanej v predchádzajúcich častiach práce. Implementácia jednotlivých tried a ich metód odpovedá návrhu zobrazenom na diagrame tried 3.3. Trieda *build* implementuje hlavné správanie nástroja, pričom výsledný skript zostaví spracovaním tried *src*, *functions*, *default_variables*, *help, info* a tried implementujúcich podporu systémov *lib_redhat* a *lib_solaris*.

Metódy tried podpory rôznych platforiem a ich verzii implementujú riešenie rozoberané v predchádzajúcej časti 3.3. Toto riešenie implementuje algoritmus 1, ktorý ilustruje implementáciu metódy *redhat()*.

Správanie metódy *redhat()* sa špecifikuje v závislosti na okolnostiach, za ktorých bude zavolaná. Pri prvom spustení metóda *redhat()* redefinuje samú seba podľa nastavenej hodnoty premennej *$SYSTEM*, ktorú nie je potrebné opakovane kontrolovať, vzhľadom na fakt,




Obr. 3.3: UML diagram tried – architektúra nástroja pre bezpečnostný audit

že sa od nastavenia počas behu nástroja nemení. V ďalších volaniach metódy jej správanie reflektuje definíciu správania redefinovanú pri jej prvom spustení. Ak je obsah premennej *$SYSTEM* nastavený na systém zhodný s názvom metódy, definuje správanie špecifické pre jej správanie, v opačnom prípade bude mať správanie prázdnej funkcie.

Ďalšie metódy tejto triedy, typu *v7()*, resp. *v11()*, implementujú rozšírenie chovania metód *redhat()* a *solaris()* o možnosť špecifikovať verziu operačného systému.

### 3.4.1 Základné informácie o implementácii nástroja

Nástroj na bezpečnostný audit bol implementovaný v skriptovacom jazyku bash, pričom sa snaží dodržovať POSIX kompatibilitu kvôli použitiu na rôznych platformách. Nástroj bez auditných politík v adresári `src/` sa skladá z 12 súborov a 1 425 riadkov zdrojového kódu, pričom dosahuje veľkosť 34,7 kB.

**Algoritmus 1:** redhat()

**Input:** $@
**Output:** $*RET*

```
1: if SYSTEM = "redhat" then
2:     RET=2
3:     redhat() {
4:         if $1 = "v7"  ||  $1 = "v6"  ||  $1 = "v5"  ||  $1 = "v4" then
5:             echo $@ | grep -q -E v$VERSION
6:             ret=$?
7:             if $ret -ne 0 then
8:                 return $RET
9:             end if
10:        end if
11:        RET=2
12:        $@
13:        RET=$?
14:        return $RET
15:    }
16:    redhat $@
17: else
18:    redhat() {
19:        :
20:    }
21: end if
```

## 3.5 Testovanie

Funkčnosť implementovaného riešenia bola overená testovaním na virtualizovaných systémoch Red Hat Enterprise Linux 7.2 a Solaris 11.3. Funkčnosť zostavovať auditné skripty pre rôzne systémy rôznych verzii, nezávisle od systému, na ktorom boli zostavené, bola overená na systéme Arch Linux. Pre účely testovania funkčnosti zostavených auditných skriptov, bola použitá sada auditných politík implementujúca vlastné kritériá, ale aj odporúčania CIS.

### 3.5.1 Testovanie na systéme Red Hat Enterprise Linux 7.2

Nástroj úspešne zostavil auditný skript, ktorý následne prebehol v poriadku, pričom boli správne identifikované politiky definované pre daný systém a jeho verziu. Rovnaký priebeh mal aj skript zostavený na inej platforme pre tento systém.

Ukážka z výstupu pre politiku SELinux:

```
----------------------------------------
[SECTION] selinux
----------------------------------------
[OK] Selinux is in "Enforcing" mode.
[OK] RPM package's signature is checked prior to its installation
```

```
[OK] Targeted policy selected (SELINUX)
[FAIL] SETroubleshoot is installed: 'setroubleshoot-3.2.24-1.1.el7.x86_64'
[OK] MCS Translation service is not installed
[OK] No unconfined daemons found on the system (SELINUX)
```

### 3.5.2 Testovanie na systéme Solaris 11.3

Priebeh testovanie na operačnom systéme Solaris mal podobný priebeh ako na systéme Red Hat Enterprise Linux. Rozdiely vznikli kvôli definíciam politík, nakoľko sú dizajnované primárne pre Red Hat Enterprise Linux. Dôvodom je napríklad Trusted Extensions v Solarise, na rozdiel od Red Hat Enterprise Linux s použitím SELinux. Preukázanie funkčnosti implementovaného nástroja to napriek tomu negatívne neovplyvnilo.

## 3.6 Možnosti rozšírenia a pokračovanie vývoja

Nástroj je vďaka zvolenému prístupu v návrhu jednoduché rozšíriť o podporu ďalších operačných systémov, prípadne o ďalšie nové verzie už aktuálne podporovaných. Bolo by vhodné rozšíriť auditné politiky a kritériá kladené na konfigurácie systémov, pričom je možné využiť nie len odporúčania CIS, ale aj databázu NVD s využitím štandardov SCAP. Ďalším významným prínosom by bolo implementovať možnosť oceňovania politík vzhľadom na závažnosť rizík tak, aby bolo možné vyhodnotiť skóre v bodovej reprezentácii.

# Záver

Práca poskytuje ucelený prehľad problematiky informačnej bezpečnosti a zaoberá sa procesom bezpečnostného auditu, v rámci ktorého popisuje bezpečnostné štandardy používané pri automatizovanom testovaní. Ďalej predstavuje už existujúce nástroje poskytujúce automatizované testovanie systémov voči zavedeným bezpečnostným štandardom.

Hlavným cieľom bolo navrhnúť a implementovať nástroj pre automatizované testovanie konfigurácii operačných systémov určených pre bezpečnostný audit OS Linux/Unix/AIX, ktorý by zautomatizoval priebeh auditu a tým uľahčil jeho proces.

V rámci práce bol tento cieľ naplnený tým, že bol navrhnutý a implementovaný multiplatformový nástroj pre bezpečnostný audit, ktorý umožňuje automatizované testovanie konfigurácii operačných systémov pri zachovaní integrity testovaných systémov. Vyvinutý nástroj je možné využiť v kontexte bezpečnostného auditu s použitím štandardov Security Content Automation Protocol (SCAP) a odporúčaní CIS (Center for Internet Security). Nástroj bol implementovaný v skriptovacom jazyku bash a následne otestovaný na systémoch Red Hat Enterprise Linux a Solaris.

Prínosom tejto práce bolo vytvorenie nástroja, ktorý je použiteľný na preukázanie zhody konfiguračných vlastností operačných systémov nie len s využitím odporúčaní CIS a štandardov z balíka SCAP, ale aj s požiadavkami štandardu ISO/IEC 27001.

Implementovaný nástroj bol navrhnutý s ohľadom na budúci vývoj a možné ďalšie rozšírenie. Pri návrhu bola braná do úvahy potreba jednoduchého rozširovania o ďalšie verzie a systémy.

# Literatúra


[1] *ISO 19011:2011, Guidelines for auditing management systems*. Geneva: International Organization for Standardization, 2011.

[2] *ČSN ISO/IEC 27005 (369790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[3] *ČSN ISO/IEC 27007 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[4] *ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[5] *ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[6] *ČSN ISO/IEC 27002 (369798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[7] *CIS Configuration Assessment Tool CIS-CAT: Users Guide*. v3.0.01. East Greensbush: Center for Internet Security, ©2001–2014.

[8] *Qualys PC/SCAP Auditor: Getting Started Guide*. Redwood Shores: Qualys, ©2011–2015.

[9] *Baseline IT Security Policy [S17]*. Version : 5.0. Hong Kong: Government of the Hong Kong Special Administrative Region, The Office of the Government Chief Information Officer, ©2012.

[10] *Nessus User Guide*. Maryland: Tenable Network Security, ©2016.

[11] BAKER, Jonathan; HANSBURY, Matthew; HAYNES Daniel: *The OVAL® Language Specification*. Version 5.10 Revision 1. Bedford: The MITRE Corporation, ©2011.

[12] BOOTH, Harold; RIKE, Doug; WITTE, Greg: *THE NATIONAL VULNERABILITY DATABASE (NVD): OVERVIEW*. Gaithersburg: National Institute of Standards and Technology, 2013.

[13] DISTERER, Georg: ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, ročník 14, č. 2, 2013: s. 92 – 100, ISSN 1615-5270.

[14] E. MANN, David; M. CHRISTEY, Steven: *Towards a Common Enumeration of Vulnerabilities*. Bedford: The MITRE Corporation, 1999.

[15] JANOŠCOVÁ, Renata: *Princípy informačnej bezpečnosti* [online]. Trenčín: VŠM v Trenčíne / City university of Seattle, 2014 [cit. 2016-05-11]. URL http://ics.upjs.sk/~jirasek/ops/Janoscova.pdf

[16] K. MANADHATA, Pratyusa: *An Attack Surface Metric*. Dizertační práce, Carnegie Mellon University, School of Computer Science, Pittsburgh, 2008, vedúci práce M. Wing Jeannette.

[17] LUKAŠÍK, Šimon: *Compliance Audit of Linux Environments*. Diplomová práce, Masarykova univerzita, Fakulta informatiky, Brno, 2013, vedúci práce Kasprzak Jan.

[18] M. BLANK, Rebecca; D. GALLAGHER, Patrick: *NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations*. Revision 4. Gaithersburg: National Institute of Standards and Technology, 2013.

[19] M. GILLIGAN, John; F. PELGRIN, William: *2014 ANNUAL REPORT*. East Greensbush: Center for Internet Security, 2015.

[20] QUINN, Stephen; SCARFONE, Karen; BARRETT, Matthew; a i.: *NIST Special Publication 800-126: Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0*. Gaithersburg: National Institute of Standards and Technology, 2010.

[21] SCARFONE, Karen; MELL, Peter: *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*. Gaithersburg: National Institute of Standards and Technology, 2010.

[22] STALLINGS, William: *Operating systems: internals and design principles*. 7th ed. Boston: Prentice Hall, ©2012, ISBN 013230998X.

[23] WALTERMIRE, David; QUINN, Stephen; SCARFONE, Karen; a i.: *NIST Special Publication 800-126: The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*. Revision 2. Gaithersburg: National Institute of Standards and Technology, 2011.

[24] *TRAMSES: Řízení bezpečnosti informací organizace* [online]. České republika: Risk Analysis Consultants, ©2016 [cit. 2016-05-16]. URL http://www.rac.cz/rac/homepage.nsf/CZ/Ramses

[25] *The Security Content Automation Protocol (SCAP)* [online]. Gaithersburg: National Institute of Standards and Technology, 2009 [cit. 2016-05-12]. URL https://scap.nist.gov/

[26] *XCCDF – The Extensible Configuration Checklist Description Format* [online]. Gaithersburg: National Institute of Standards and Technology, 2009 [cit. 2016-05-12]. URL https://scap.nist.gov/specifications/xccdf/

[27] *The Open Checklist Interactive Language (OCIL)* [online]. Gaithersburg: National Institute of Standards and Technology, 2009 [cit. 2016-05-12].
URL https://scap.nist.gov/specifications/ocil/

[28] *The Asset Identification* [online]. Gaithersburg: National Institute of Standards and Technology, 2010 [cit. 2016-05-12].
URL https://scap.nist.gov/specifications/ai/

[29] *The Asset Reporting Format (ARF)* [online]. Gaithersburg: National Institute of Standards and Technology, 2010 [cit. 2016-05-13].
URL https://scap.nist.gov/specifications/arf/

[30] *Common Configuration Enumeration (CCE) Reference Data* [online]. Gaithersburg: National Institute of Standards and Technology, 2005 [cit. 2016-05-13].
URL https://nvd.nist.gov/cce

[31] *Common Platform Enumeration (CPE)* [online]. Gaithersburg: National Institute of Standards and Technology, 2011 [cit. 2016-05-13].
URL https://scap.nist.gov/specifications/cpe/

[32] *Common Vulnerability Scoring System, V3 Development Update* [online]. Morrisville: FIRST, 2015 [cit. 2016-05-13].
URL https://www.first.org/cvss

[33] *The Trust Model for Security Automation Data (TMSAD)* [online]. Gaithersburg: National Institute of Standards and Technology, 2011 [cit. 2016-05-13].
URL https://scap.nist.gov/specifications/tmsad/

[34] ŠRUBAŘ, Michal: *OpenSCAP User Manual* [online]. 2015 [cit. 2016-05-14].
URL http://static.open-scap.org/openscap-1.0/oscap_user_manual.html

# Prílohy

# Zoznam príloh

**A Obsah CD** **39**

**B Návod na použitie** **40**

# Príloha A

# Obsah CD

Priložené CD obsahuje zdrojové kódy a dáta uložené v nasledujúcej adresárovej štruktúre:

- `tool/` – obsahuje zdrojové kódy auditného nástroja
- `latex/` – zdrojový text v LaTeXu k vysádzaniu technickej správy
- `thesis/` – technická správa vo formáte PDF

# Príloha B

# Návod na použitie

Obsahom tejto prílohy je popis použitia nástroja, ktorý bol vyvíjaný v rámci tejto práce. Nástroj v aktuálnej verzii podporuje systémy Red Hat Enterprise Linux a Solaris. Pre spustenie je potrebné skopírovať adresár `tool/` z priloženého prenosového média na cieľovú testovaciu stanicu alebo iné prepisovateľné médium, nakoľko je potrebné právo zápisu v aktuálnom adresári.

## Ovládanie

Nástroj sa spúšťa z konzoly, pre zobrazenie nápovedy je možné použiť príkaz z umiestnenia skopírovaného adresára:

```
$ ./build --help
```

Pri použití nástroja bez voľby sa zostaví výsledný auditný skript pre všetky podporované systémy a ich verzie a zároveň sa uplatnia všetky politiky umiestnené v adresári `src/`, pričom pri spustení zostaveného výsledného auditného skriptu je potrebné špecifikovať auditovaný operačný systém a jeho verziu. V opačnom prípade sa voľby a preferované politiky špecifikujú nasledujúcim spôsobom:

```
$ ./build [OPTIONS]... [FILE]...

 FILE      jeden alebo zoznam súborov s politikami oddelený medzerou
 OPTIONS   voliteľné prepínače, popis viď nižšie

 OPTIONS:
 --system=NAME[-VERSION]    názov a verzia operačného systému {redhat, solaris}
 --output=FILENAME.sh       názov zostaveného skriptu
 --srcpath=PATH             nastavenia vlastnej cesty k auditným politikám
 -a, --noarchive            vypne nastavenie zbalenia výsledkov
 -c, --clean                zmaže výsledky z predchádzajúceho testovania
 -d, --nodeps               preskočí kontrolu závislostí potrebných pri audite
 -f, --force                ak existuje, prepíše skript zostavený predtým
 -h, --help                 zobrazí nápovedu
 -m, --nocolor              vypne farebný výstup
```

| | |
|---|---|
| `-o, --nobuild` | nakonfiguruje nastavenia, skontroluje závisloti a skončí |
| `-p, --noprogressbar` | vypne zobrazovanie načítavania |
| `-r, --run` | po zostavení skriptu automaticky spustí testovanie |
| `-v, --verbose` | nastaví podrobnejší výpis |

Príklad:

```
$ ./build system=redhat-7.2 -output=audit.sh basic.sh storage.sh -v -f
```

Zostaví auditný skript „audit.sh“ pre operačný systém Red Hat Enterprise Linux verzie 7.2 zo zdrojov politík basic.sh a storage.sh.

Pre zostavený skript je možné si zobraziť nápovedu s dostupnými možnosťami alebo ho rovno spustiť. V našom príklade môžeme zobraziť nápovedu:

```
$ bash audit.sh --help
```

Dostupné sú nasledujúce voliteľné prepínače:

| | |
|---|---|
| `--system=NAME-VERSION` | názov a verzia operačného systému {redhat, solaris}* |
| `--verbose={1, 2, 3}` | nastaví podrobnejší výpis |
| `-a, --noarchive` | vypne nastavenie zbalenia výsledkov* |
| `-c, --clean` | zmaže výsledky z predchádzajúceho testovania |
| `-d, --deps` | skontroluje potrebné závislosti |
| `-h, --help` | zobrazí nápovedu |
| `-m, --nocolor` | vypne farebný výstup* |
| `-p, --noprogressbar` | vypne zobrazovanie načítavania* |

*V prípade ak voľba nebola špecifikovaná pri zostavení skriptu.

Príklad spustenia:

```
$ bash audit.sh -verbose=3 -c -a
```

Pre podrobnejšie informácie je dostupný súbor README v adresári nástroja.