ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA ELEKTROTECHNICKÁ

KATEDRA POČÍTAČŮ

Petr Mareš

Zabezpečení operačních systémů v informačních systémech pracujících s utajovanými informacemi

Bakalářská práce

Školitel: Ing. Tomáš Vaněk, Ph.D.
Studijní program: Softwarové inženýrství a technologie
Datum: 13. 8. 2020

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne……

……
podpis Petr Mareš

Anotace

Bakalářská práce se zabývá oblastí ochrany citlivých a utajovaných elektronických dat. V práci popisuji bezpečnostní opatření pro komunikační a informační zařízení/systémy, především pro počítače zpracovávající neveřejné a utajované informace. V bakalářské práci popisuji různé metody jejich zabezpečení. Součástí bakalářské práce bylo vytvoření programu na kontrolu bezpečnostních nastavení u off-line počítačů.

Klíčová slova

Kybernetická bezpečnost, ochrana utajovaných informací, bezpečnostní nastavení, kontrola bezpečnostního nastavení, program

Annotation

This bachelor thesis focuses on the topic of sensitive and classified electronic data. In this thesis I explain Security measures for communication and information systems. Mostly for computers working with non-public and classified information. In this bachelor thesis I describe different methods of providing Security. Included in the bachelor thesis is the creation of a program which checks the Security options of offline computers.

Keywords

Cyber security, protection of classified information, security settings, control of security settings, program

Obsah

1 Úvod

Se vzrůstajícím pokrokem informačních technologií a potřebou lidí sdílet dokumenty, informace a data vzrůstá i nutnost digitální informace chránit. V prostředí elektronické komunikace – digitálním prostředí – dochází k vytváření, čtení, zápisu, úpravám a samozřejmě výměně informací. Tyto informace obsahují údaje, jejichž ztráta by mohla někoho poškodit.

V práci se zabývám zabezpečením operačních systémů a související legislativou, tj. krizovým zákonem, zákonem o kybernetické bezpečnosti a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti. Pozornost věnuji zejména zabezpečení utajovaných informací, jež vyžaduje zákon.

Je velmi důležité rozlišovat krizový zákon, zákon o kybernetické bezpečnosti a zákon o ochraně utajovaných informací a bezpečnostní způsobilosti. Tyto zákony mají jeden společný úkol, a to chránit informace.

Každý z uvedených zákonů však nahlíží na ochranu informací z jiného pohledu. Obecně lze tyto informační struktury rozlišit na neutajované a utajované. V této práci se na rozdílné i společné aspekty těchto zákonů snažím poukázat v kapitole Legislativa.

Výsledkem předložené práce je vytvoření analyticko-bezpečnostního programu, který podle požadavků zákona 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti klade důraz na požadavky na systémy zpracovávající utajované informace. Program dokáže analyzovat bezpečnostní nastavení v počítači s operačním systémem Windows 10 a vytvořit o něm celkový report, který pomůže zefektivnit zaměstnancům certifikačního oddělení práci.

2 Legislativa

2.1 Krizový zákon

Tato kapitola popisuje zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále jen krizový zákon). Krizový zákon zajišťuje krizové situace nesouvisející s obranou státu před vnějším napadením. Krizový zákon upravuje a definuje odvětví, ve kterých se nacházejí prvky kritické infrastruktury. Dále stanovuje pravomoci a působnost státních orgánů, institucí, fyzických a právnických osob při krizové situaci. Definuje stav nebezpečí a proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb.

Odvětvová kritéria pro určení prvku KI uvedená v písm. A. – F., odvětví VI. přílohy nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb., se použijí přiměřeně pro oblast kybernetické bezpečnosti (KB), pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

Do krizového zákona tedy spadá mimo jiné kritická infrastruktura (KI), kritická informační infrastruktura (KII) a významné informační systémy (VIS).

2.1.1 Popis kritické infrastruktury (KI)

Kritická infrastruktura jsou fyzické, kybernetické a organizační (obslužné) systémy, které jsou nutné pro zajištění ochrany životů a zdraví lidí a majetku, minimálního chodu ekonomiky a správy státu. [1] Je to například energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, komunikační a informační systémy, potravinářství a zemědělství, zdravotnictví a chemický průmysl. Kritická infrastruktura není utajovaná – není k tomu důvod. Je však velmi dobře zabezpečená před útoky z vnějšku, protože v případě krizové situace – tedy narušení či omezení funkcionality jednotlivých prvků či systému prvků kritické infrastruktury – by mohlo dojít k narušení chodu a bezpečnosti státu, zabezpečení základních životních potřeb a zdraví obyvatel či ekonomiky státu.

2.1.2 Kritická informační infrastruktura (KII)

Kritickou informační infrastrukturou se dle § 2 písm. g) a písm. i) zákona č. 240/2000 Sb., krizového zákona, rozumí prvek nebo systém prvků kritické infrastruktury, v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti dle § 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

V praxi se jedná o takové informační nebo komunikační systémy, příp. ICS/SCADA systémy, které naplní kritéria pro určení prvků KII. [2]

2.1.3 Významný informační systém (VIS)

Významným informačním systémem je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací (narušení důvěrnosti, dostupnosti a integrity) může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. [2]

Každý významný informační systém musí mít svého správce a provozovatele. VIS jsou například Centralizovaný informační systém STK (CIS STK), jehož správcem je Ministerstvo dopravy, Štábní informační systém AČR (ŠIS), jehož správcem je Ministerstvo obrany (MO). Celkový přehled těchto VIS je v příloze č. 1 k vyhlášce č. 317/2014 Sb.

Správce významného informačního systému

Správcem významného informačního systému je takový orgán nebo osoba, která určuje účel zpracování informací a podmínky provozování informačního systému.

Provozovatel významného informačního systému

Provozovatelem významného informačního systému je takový orgán nebo osoba, která zajišťuje funkčnost technických a programových prostředků tvořících informační systém, správce je určil a o této skutečnosti informoval.

Aby zařízení, konkrétně počítač, bylo možné považovat za zabezpečený pro kritickou infrastrukturu nebo ochranu utajovaných informací, musí být naplněna litera zákona. Přesněji se jedná o zákon číslo 412/2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti, a číslo 181/2014, o kybernetické bezpečnosti.

2.2 Zákon o kybernetické bezpečnosti

Tato kapitola popisuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen zákon o kybernetické bezpečnosti). Ústředním správním úřadem pro oblast kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB). Jeho část označovaná jako GOVCERT *hraje klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB).*

Každá země, která má své kritické systémy připojeny do veřejné internetové sítě, musí být schopna efektivně a účinně čelit bezpečnostním výzvám – hrozbám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při předcházení incidentům. [3]

Tento zákon zapracovává příslušné předpisy Evropské unie (Čl. 5 odst. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148.) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. [4]

Základními vlastnostmi bezpečnosti informací jsou integrita, zajištění důvěrnosti, dostupnost informací a dat. V zákoně č. 181/2014 se nejedná o důvěrnost podle zákona č. 412/2005, ale o neutajovanou informaci, jež má povahu citlivého charakteru. Nejedná se pouze o data, ale i služby, jako jsou on-line tržiště, internetové vyhledávače nebo cloud computing. NÚKIB poskytuje bezpečnost informačního a komunikačního systému kritické informační infrastruktury, významného informačního

systému a systému základních služeb. Ze zákona o kybernetické bezpečnosti vyplývá několik obecných bezpečnostních opatření pro on-line zařízení.

2.2.1 Bezpečnostní opatření podle zákona o kybernetické bezpečnosti

(1) Bezpečnostními opatřeními jsou

a) organizační opatření,

b) technická opatření.

(2) Organizačními opatřeními jsou

a) systém řízení bezpečnosti informací,

b) řízení rizik,

c) bezpečnostní politika,

d) organizační bezpečnost,

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv,

g) bezpečnost lidských zdrojů,

h) řízení provozu a komunikací,

i) řízení přístupu osob,

j) akvizice, vývoj a údržba,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

l) řízení kontinuity činností,

m) kontrola a audit.

(3) Technickými opatřeními jsou

a) fyzická bezpečnost,

b) nástroj pro ochranu integrity komunikačních sítí,

c) nástroj pro ověřování identity uživatelů,

d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací,

l) bezpečnost průmyslových a řídicích systémů. [4]

2.3 Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, klade požadavky na systémy zpracovávající utajované informace. Systémy zpracovávající utajované informace musí být zabezpečeny před útoky zevnitř a vně. Tyto systémy nejsou připojeny do klasické internetové sítě s výjimkou případů, kdy má systém pro tento účel mezi svou vlastní a veřejnou komunikační sítí vhodné bezpečnostní rozhraní podle § 9a Vyhlášky č. 523/2005 Sb.

Odpovědnost za ochranu utajovaných informací

Pokud se jedná o zařízení zpracovávající utajované informace, je zákonem číslo 412/2005 určeno, že za informační bezpečnost odpovídá (má zmocnění) Národní úřad pro kybernetickou a informační bezpečnost, který problematiku řeší ve spolupráci s Národním bezpečnostním úřadem.

2.3.1 Vysvětlení pojmu utajovaná informace

Utajovaná informace (UI) je informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči, označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací (§ 139). [5]

2.3.2 Popis činnosti Národního bezpečnostního úřadu

Národní bezpečnostní úřad je orgánem moci výkonné a je ústředním správním úřadem pro oblasti ochrany utajovaných informací a bezpečnostní způsobilosti. Kvůli tomu je zařazen jak mezi správní úřady, tak i ústřední úřady.
Úřad vydává osvědčení o bezpečnostní způsobilosti nejen podnikateli, ale i fyzické osobě. Tím garantuje, že proti jeho držiteli nebyly zjištěny skutečnosti, jež by bránily, aby měl přístup k utajovaným informacím. Díky těmto skutečnostem může stát nakládat či sdílet informace se subjekty, které pomohou jak při ochraně státu, tak při mezinárodní spolupráci. Mezi tyto případy patří například vojenské, politické a ekonomické záměry, které slouží k ochraně života, zdraví a majetku státu a občanů.

2.3.2.1 *Struktura Národního bezpečnostního úřadu*

- Sekce bezpečnostního řízení,
- Kancelář 1. náměstka ředitele,
- Odbor průmyslové bezpečnosti,
- Odbor evidenčního šetření a podpory,
- 1.– 4. odbor personální bezpečnosti,
- Sekce kancelář ředitele Úřadu,
- Odbor personální,
- Odbor bezpečnostní,
- Odbor administrativní a fyzické bezpečnosti,
- Oddělení mezinárodní spolupráce,
- Archiv Národního bezpečnostního úřadu,
- Sekce provozně právní,
- Odbor provozně ekonomický,
- Odbor právní a legislativní,
- Odbor komunikačních a informačních systémů,
- Oddělení kontroly.

Pro potřeby zajištění bezpečnosti utajovaných informací nebo certifikace informačních a komunikačních systémů jsou důležité pouze jeho vybrané části, a to:

- Odbor průmyslové bezpečnosti,
- Odbor personální bezpečnosti,
- Odbor administrativní a fyzické bezpečnosti.

Ty zajišťují podklady průmyslové, personální, administrativní a fyzické bezpečnosti pro certifikační oddělení. Požadavky těchto oddělení musí být splněny, jinak není možné dále pokračovat v certifikaci komunikačního nebo informačního systému.

Odbor průmyslové bezpečnosti

Odbor průmyslové bezpečnosti zajišťuje a v rozsahu stanoveném zákonem provádí bezpečnostní řízení o žádosti podnikatele a bezpečnostní řízení o zrušení platnosti osvědčení podnikatele. Rozhoduje o přerušení a zastavení bezpečnostního řízení o vydání či nevydání osvědčení podnikatele nebo o vydání souhlasu s jednorázovým přístupem k utajované informaci. Dále vydává a ruší osvědčení pro podnikatele. Aktualizuje a vede o podnikatelích bezpečnostní svazky.

Ve stručnosti tedy kontrolou právnických osob zjišťují, zda nejsou v konfliktu se zákonem a mohou přistupovat k utajovaným informacím.

Odbor personální bezpečnosti

Odbor personální bezpečnosti má podobnou agendu jako Odbor průmyslové bezpečnosti, ale řeší fyzické osoby.

Odbor administrativní a fyzické bezpečnosti

Tento odbor vytváří a prosazuje jednotnou koncepci ochrany utajovaných informací za oblast administrativní a fyzické bezpečnosti, spolupracuje s orgány státu a organizacemi v oblasti ochrany utajovaných informací. Pro odbor právní a legislativní, odbor průmyslové bezpečnosti a oddělení státního dozoru zabezpečuje jednotný metodický výklad v oblasti administrativní bezpečnosti, podílí se na přípravě a na výkonu státního dozoru v oblasti fyzické bezpečnosti. Vytváří celostátní metodiku certifikace technických prostředků v oblasti fyzické bezpečnosti, provádí metodickou činnost při zpracování a hodnocení projektů fyzické bezpečnosti. Zajišťuje proces certifikace technických prostředků pro zajištění fyzické bezpečnosti, určuje způsob jejich použití a dobu platnosti certifikátů a provádí aktualizaci seznamu certifikovaných technických prostředků, posuzuje projekty fyzické bezpečnosti a v rámci kontrolní činnosti provádí její ověřování.

2.3.3 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) je ústředním správním orgánem. Stará se o kybernetickou bezpečnost, ochranu utajovaných informací v rámci komunikačních a informačních systémů, kryptografickou ochranu a systém Galileo. Navrhuje v oblasti kybernetické a informační bezpečnosti standardy bezpečnosti, standardy pro informační systémy a stanovuje standardy nutné pro bezpečný chod státu.

<u>NÚKIB je gestorem v oblastech zajišťující:</u>

- Kybernetickou bezpečnost,
- GOVCERT,
- Ochranu utajovaných informací v ICT, kde důležitými součástmi jsou:
    - Odbor bezpečnosti informačních a komunikačních technologií
        - Oddělení certifikací informačních a komunikačních systémů (OCIKS),
        - Oddělení certifikace kryptografických prostředků a pracovišť (OCKPP),
        - Oddělení šifrové služby (OŠS),
        - Oddělení kryptologie a vývoje kryptografických prostředků (OKVKP),
        - Oddělení Tempest,
- Galileo PRS.

Podobně jako u NBÚ pro potřeby zajištění bezpečnosti utajovaných informací nebo certifikace informačních a komunikačních systémů jsou důležité pouze jeho vybrané části, a to: **Oddělení certifikací informačních a komunikačních systémů**, **Oddělení kryptologie a vývoje kryptografických prostředků** a **Oddělení Tempest**.

Oddělení kryptologie a vývoje kryptografických prostředků

Toto oddělení je výzkumné a vytváří prostředky pro bezpečnou komunikaci. Jedná se například o speciální software, hardware nebo další různá zařízení. Jejich prioritou je vytvářet kryptografické prostředky, ale velmi často vytvářejí i specifické podpůrné prostředky pro potřeby státu.

Oddělení Tempest

Jeho funkce je popsána v kapitole „Problematika elektromagnetického vyzařování“.

Oddělení certifikací informačních a komunikačních systémů

Jedná se o stěžejní oddělení pro certifikace speciálních prostředků, určených pro bezpečnou komunikaci. Jejich práce spočívá v analýzách bezpečnostních novinek, sestavování bezpečnostních doporučení a hlavně kontrole komunikačních a informačních systémů v oblasti zákona č. 412/2005.

Bezpečnost informačních a komunikačních systémů se podle zákona č. 412/2005 Sb. dělí na:

(1) komunikační systémy, kde se utajované informace vyskytují pouze v rámci komunikace a neukládají se tam (schvaluje se zde projekt komunikačního systému),

(2) informační systémy (zde probíhá práce s utajovanými informacemi – takové systémy musí být certifikovány).

Ve své práci se zaměřím na obě tyto skupiny, ale v souladu se zadáním zůstane prioritní především oblast informační bezpečnosti.

2.3.4 Ochrana informací

Je důležité rozlišovat, které informace je důležité chránit, a které ne. Stupeň utajení vždy určuje autor (zpracovatel) informace. *Původcem utajované informace je orgán státu, právnická osoba nebo podnikající fyzická osoba, u nichž utajovaná informace vznikla, nebo Úřad průmyslového vlastnictví podle § 70 odst. 4.* [5] Tato skutečnost platí i u součástí informačních systémů. Například: pokud je ukraden monitor, není to takový problém, jako když je ukraden HDD s utajovanými informacemi.

Jednou z doporučujících norem, z nichž se přitom vychází, je řada norem ISO/IEC 27 000. Zde jsou uvedeny doplňující informace, které lze použít při zabezpečení počítače a celkově všech systémů zpracovávajících utajované informace. Jedná se například o tempery, pečeti a další zařízení schopná rozpoznat kompromitaci.

Celkově požadavky potřebné pro splnění certifikačních kritérií vycházejí z doporučení vytvořených v rámci NATO, EU, Německa, Francie, Velké Británie, evropských norem a zkušeností pracovníků certifikačního oddělení.

Aby člověk mohl pracovat (nakládat) s utajovanými informacemi, musí splňovat požadavky vyhlášky č. 523/2005 Sb. (vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor) a musí znát tzv. „need to know“.

2.3.5 Stupně utajení

Utajovaná informace se klasifikuje stupněm utajení:

a) přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,

b) tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,

c) důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,

d) vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky. (5)

Pro každý stupeň utajení jsou zákonem a prováděcími vyhláškami stanoveny požadavky na bezpečnost a zabezpečení informačního systému. Ty se postupně navyšují. Například od stupně utajení DŮVĚRNÉ a více se provádí měření skupinou Tempest (elektromagnetické záření) a od stupně TAJNÉ a PŘÍSNĚ TAJNÉ je nutné řešit i odposlech (mikrofony, snímače pohybu apod.). Definice ze zákona (§ 45)*: Ochranou utajovaných informací stupně utajení Přísně tajné, Tajné nebo Důvěrné před jejich únikem kompromitujícím vyzařováním je zabezpečení elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu.*

Pokud jsou splněny všechny podmínky stanovené zákonem, lze konstatovat, že počítač splňuje podmínky udělení certifikátu pro příslušný stupeň utajení.

2.4 Problematika elektromagnetického vyzařování

Oddělení Tempest plní v rámci zákona č. 412/2005 Sb. úkoly Národního centra pro kompromitující vyzařování. V rámci této kompetence vydává metodické pokyny v oblasti kompromitujícího vyzařování (KV), provádí certifikaci stínicích komor, provádí zónová měření, měření KV v laboratoři NÚKIB a provádí kontrolu instalace informačních systémů v místě dislokace.
Celkově oddělení Tempest měří elektromagnetické vyzařování elektronických zařízení, aby se předešlo úniku informací formou nežádoucího vyzařování.

Zde je možno uvést pouze velmi obecné informace, neboť veškeré standardy z této oblasti jsou utajované. V současné době se v této oblasti preferuje tzv. „zónový koncept“, jehož princip spočívá ve využití útlumu přirozenými překážkami (vzduch, zdi, okna atd.), aby se dosáhlo utlumení elektromagnetického pole (tzn. KV) na akceptovatelnou úroveň. Z fyzikální podstaty se jedná o poměr úbytku elektromagnetického záření vůči vzdálenosti. Tomuto měření se říká zónové měření a jeho objekty jsou místnosti a budovy, kde je IS dislokován. Tímto postupem je dané místo dislokace (budova, místnost) ohodnocena jako tzv. „Zóna“. Poté se provádí měření KV konkrétního IS, který je v dané „Zóně“ instalován.

Certifikační oddělení požádá oddělení Tempest o změření úrovní elektromagnetického záření – KV daného IS. Oddělení Tempest toto měření provede podle postupů definovaných v bezpečnostních standardech a předá zprávu o provedeném měření pracovníkovi oddělení certifikací, který provádí certifikaci daného IS. Výsledkem měření je ohodnocení daného IS a zařazení do tzv. „třídy“ zařízení. Výsledek tohoto měření se přiloží ke všem potřebným dokumentům a pracovník oddělení certifikací rozhodne o splnění podmínek vlastní certifikace. Hodnocení KV se tedy provádí v rámci procesu certifikace IS, a to pouze pro IS zpracovávající UI stupně utajení Důvěrné a vyšší. Veškerá technická dokumentace k této problematice je utajená. Normy a standardy jsou původem dokumenty NATO, později převzaté z existující legislativy členských státu EU a mezinárodních norem. Existují i kompatibilní české bezpečnostní standardy NBÚ, které jsou taktéž utajované.

2.4.1 Nové problémy, výzvy

K novým problémům a výzvám patří:

- Komponenty IS zpracovávající UI nesmí obsahovat bezdrátové technologie. Taková zařízení (např. tiskárny) se dnes těžko dají koupit, v budoucnu se možná taková ani nebudou vyrábět.
- Nastupuje 5G technologie, bude problematická instalace těchto BLACK (neutajované) a RED (utajované) komponent v jednom místě.
- Některé (nové) systémy (SW) vyžadují při své práci on-line připojení k internetu. Pokud by se měly zpracovávat UI na takových systémech (např. CAD), nebude to možné. Zde nepomůže ani datová dioda.

- Tempest (problematika neúmyslného úniku informací) by měl v budoucnu zahrnovat i problematiku úmyslné modifikace komponent IS a problematiku odposlechových prostředků.
- V ČR je NÚKIB národní autorita v Tempestu a NÚKIB akreditoval několik pracovišť Tempest (MO ČR, BIS, VZ atd.). To znamená, že NÚKIB tato pracoviště metodicky řídí, kontroluje a ony měří a hodnotí. To je, domnívám se, dobrá koncepce do budoucna.
- Výsledky interních projektů skupiny Tempest používají téměř všechny členské země NATO a EU.

3 Analýza rizik

Každý projekt, výzkum a systém má ve svých začátcích i při svém působení a chodu svá rizika. Ta je vždy vhodné eliminovat, aby nedocházelo k nežádoucím problémům, ztrátám a v případě informační bezpečnosti k tak zvaným bezpečnostním incidentům.

Bezpečnostní incident v informatice je událost, která nastala při porušení pravidel potřebných k ochraně informační technologie nebo informačního systému nebo při níž došlo přímo k narušení jejich bezpečnosti. Za následky bezpečnostního incidentu lze považovat například omezení nebo ochromení činnosti organizace a samozřejmě únik informací.

Typy těchto incidentů lze hodnotit podle různých kritérií např.:

- podle jejich charakteru, tedy jestli byl tento incident úmyslný, způsobený nevědomostí nebo nedbalostí;
- podle způsobu jejich provedení, tedy aktivní nebo pasivní. Aktivní může mít za následky nedostupnost, narušení integrity a další. Obecně tedy mívá přímý dopad na systém. Pasivní je například odposlech, který též řeší již zmíněná skupina Tempest. Rozdělit se dále dá na incidenty podle cíle nebo způsobených škod.

Při rizikové analýze (RA) je důležité si umět identifikovat rizika, dokázat ohodnotit jejich nebezpečí a míru.

3.1 Přesné přístupy RA

Přesné přístupy RA jsou definované například podle normy ISO/IEC 13335:

- ***Základní přístup*** *– žádná analýza rizik se neprovádí, pouze je vybrána a implementována základní sada opatření z nějakého katalogu.*
- ***Neformální přístup*** *– jedná se o pragmatický přístup k analýze rizik, kdy se provádí rychlá, tzv. orientační analýza, založená na zkušenostech expertů a vyhodnocení možných scénářů.*
- ***Formální přístup*** *– jde o detailní analýzu rizik, tj. provádí se hodnocení aktiv, hrozeb a zranitelnosti, nejčastěji za použití matematického aparátu.*
- ***Kombinovaný přístup*** *– na základě provedené orientační analýzy, kdy byla pro organizaci identifikována kritická aktiva nebo procesy, se provede detailní analýza rizik.* [6]

Pro svou práci jsem jako nejvhodnější zvolil pracovní alternativu „Neformální přístup“, a to zejména z kapacitních důvodů. Z vlastní praxe mohu konstatovat, že analýza rizik vycházející z „Formálního přístupu“, resp. „Kombinovaného přístupu“, vyžaduje vysoce profesionální specializované pracoviště s patřičným personálně-kapacitním obsazením.

Pokud se jedná o zabezpečené informační systémy definované zákonem 412/2005, je možný (při dodržení všech bezpečnostních pravidel) pouze jeden druh útoku. Jedná se o útok zevnitř, kdy útočník je v té dané místnosti.

Pokud se jedná o systém s přístupem do veřejné sítě, bývá to zpravidla kombinace útoků zevnitř a zvenčí. V následujícím textu budou popsány základní typy rizik, jaké mohou mít následky a jak je možné tato rizika minimalizovat.

4 Popis operačních systémů

V této části se primárně zaměříme na desktopové operační systémy a operační systémy mobilních zařízení. Tyto operační systémy jsou nejčastěji používané pro již zmíněné bezpečnostní komunikační a informační systémy. Tento výběr není náhodný, jedná se o nejčastěji používané systémy jak v běžném životě, tak i v oblasti informační bezpečnosti. Je tedy vhodné znát alespoň jejich základní popis. Jejich popis jsem strukturoval na vznik, vlastnosti, uživatelskou obsluhu, prostředí administrátora a útočníka, tedy na důležité faktory rizik z pohledu bezpečnosti.

4.1 Mobilní operační systémy

4.1.1 Popis operačního systému iOS

Systém iOS je operační systém firmy Apple pro mobilní zařízení na bázi UNIX systému. Původně byl vytvořen pouze pro mobilní telefon – smartphone iPhone. V rámci vývoje byl tento operační systém postupně upravován do takové podoby, že mohl být použit i pro další zařízení, například iPod Touch nebo iPad.

Od tohoto operačního systému je odvozeno několik dalších systémů téhož výrobce:

- iPad OS je určen pro novější iPady;
- WatchOS je určen pro nositelnou elektroniku;
- tvOS je určen pro televizní zařízení.

V současné době se jedná o druhý nejpoužívanější mobilní operační systém.

Z pohledu běžného uživatele – technického laika – je tento systém optimální. Takovýto uživatel si zde nedokáže změnit nastavení systému, a tím si potenciálně poškodit funkčnost operačního systému. Lidově řečeno je tento systém relativně velmi odolný vůči nepředvídatelnému uživatelskému chování.

Z pohledu administrátora je tento systém příjemný pro jednoduchost ovládání a možnosti zabezpečení. Lze v něm jednoduše nastavit základní požadavky pro zabezpečení jak vzdáleně, tak i pomocí navádění uživatele.

Z pohledu útočníka se jedná o systém, který je nejvíce zabezpečen, protože do operačního systému nelze volně přistupovat. Veškeré aktualizace systému a bezpečností opravy dostává uživatel ve stejnou chvíli jako ostatní uživatelé z celého světa. A to i v případech, kdy uživatel vědomě nedovolí aktualizovat své zařízení. V takovém případě si totiž zařízení automaticky stáhne nejnovější dostupné aktualizace. Z tohoto pohledu lze tedy toto zařízení v dané chvíli považovat za nejlepším možným způsobem zabezpečené. Jedním z faktorů bezpečnosti zařízení značky Apple je skutečnost, že výrobce deklaruje delší podporu svých zařízení. Jedná se především o bezpečnostní aktualizace po dobu až 6 let. Vytvoření zavirované aplikace a její vložení do telefonu je velmi složité. Obchod pro stahování aplikací na tomto systému se v současné době nazývá App Store. Pokud chce útočník vytvořit aplikaci a distribuovat ji přes App Store, musíte se nejprve zaregistrovat u firmy Apple jako vývojář. Přitom platí, že obelstít Apple není vůbec jednoduché. Při nahrávání aplikace do AppStoru automatizovaný systém Applu kontroluje velmi hluboce kvalitu tohoto programu, čímž zaručuje uživateli, že si stáhne do svého telefonu bezpečnou aplikaci. Toto pravidlo platí pro naprostou většinu situací.

Je však známo i několik případů, kdy zavirovaná aplikace byla dostupná na AppStore. Konkrétně se jednalo o aplikaci, jež měla pomocí čtečky otisku prstu měřit srdeční tep. Je až s podivem, že tato

aplikace prošla kontrolou Applu, neboť výrobce s jistotou věděl, že jejich snímače něco takového neumožňovaly.

Z pohledu útočníka lze tedy velmi špatně útočit na zařízení jako takové. Jako výhodnější se jeví atak na neznalost uživatele.

Samozřejmě, že existuje i možnost, jak si i tento operační systém přizpůsobit svým potřebám, pokud uživatel není spokojený s nabízenými (omezenými) možnostmi. Jedná se o softwarovou úpravu mobilního telefonu iPhone – jailbreak. Po jailbreaku lze do iPhonu instalovat neoficiální aplikace (nevydávané v App Store), které mají přístup do systému iOS. Tento proces modifikuje operační systém podle toho, kdo daný jailbreak vytvořil. Díky tomu lze do zařízení nejen nahrávat neoficiální aplikace, ale také přistupovat k dříve nedostupným datům atd. Jailbreak má kromě zmiňovaných výhod také mnoho nevýhod. Jednou z nich je například nedokonalé odladění modifikovaného systému pro daný hardware, jako je třeba větší spotřeba baterie, zamrzání systému apod.

4.1.2 Popis operačního systému Android

Operační systém Android vznikl jako startup, tedy jako snaha vytvořit jednotný operační systém pro mobilní telefony. Jeho Linuxové jádro je přizpůsobeno pro chod na skoro jakémkoli moderním hardwaru. Veškeré jeho zdrojové kódy jsou opensource. Zařízení s OS Android jsou velmi náchylná k útokům. Protože tento OS je vedený jako open source, lze přistupovat ke zdrojovým kódům tohoto systému a systematicky vytvářet aplikace nebo viry k jeho napadení. Když se totiž přijde na zranitelnost, chvíli trvá, než je vytvořena záplata na čistý operační systém. Většina výrobců mobilních zařízení přidává k čistému operačnímu systému i svoji grafickou, bezpečnostní nadstavbu. Po vydaných oficiální záplatách a aktualizacích systému je však zapotřebí od těchto výrobců implementovat tato vylepšení do jimi upraveného systému. Tento způsob je velmi zdlouhavý, protože výrobci musí každý update přizpůsobit pro svá specifická zařízení. Po tuto dobu jsou tedy všechna jejich zařízení náchylná na zmíněnou známou chybu. Vlastně je velmi mnoho možností, jak napadnout zařízení s OS Android.

Tento systém je pro neznalého uživatele poměrně hodně nebezpečný, protože dovoluje nahrávat škodlivé aplikace odkudkoli. Škodlivými aplikacemi se rozumí aplikace, jež dokáží vytvářet, číst, odesílat a mazat data uživatele bez jeho vědomí. Dokonce i sám uživatel může změnit nastavení systému tak, že změní nastavení operačního systému, který pak nedokáže správně fungovat. Jedním z mnoha příkladů je i neúmyslné spuštění režimu Vývojář, jenž se aktivuje jednoduše pomocí několika kliknutí na systémovou informaci v nastavení systému. Tímto nastavením lze povolovat a zakazovat nastavení, která by měl provádět pouze zkušený uživatel.

Dalším bezpečnostním problémem, který se již řeší, je tzv. root zařízení. Jedná se o přepnutí do privilegovaného režimu, kdy se útočníci nebo nezkušení uživatelé snaží obejít vlastnosti operačního systému nastavené výrobcem. Tomuto se snaží částečně zabránit již nový OS Android verze 10. Ten má v sobě integrované softwarové vylepšení, převzaté od společnosti Samsung a jejího produktu Knox.

Knox je vícevrstvá architektura zaručující důvěryhodnost systému i HW součástí mobilního zařízení. Bohužel, toto řešení lze uplatnit pouze u vlajkových lodí společností, vyrábějících mobilní telefony. Tyto vlajkové lodě jsou většinou výrazně nad finančními možnostmi běžných uživatelů. Ti následně preferují zařízení cenově dostupná, ale také s nižším zabezpečením – zejména s velmi krátkou podporou bezpečnostních aktualizací od výrobců. Pokud se budeme pohybovat cenově kolem 3 000,- Kč, tak tato zařízení nemají podporu ani na jeden rok.

4.2 Desktopové operační systémy

4.2.1 Popis operačního systému Windows 10

Operační systém Windows 10 je operační systém určený hlavně pro stolní nebo přenosné počítače. Vychází z řady operačních systémů Windows NT (NewTechnology). Řada těchto operačních systémů se oproti svému předchůdci, řadě Windows MS-DOS, vyznačuje především podporou novější řady procesorů Intel, nového chráněného režimu a podporou preemptivního multitaskingu, kdy správně napsaná aplikace dokáže používat najednou procesor s více aplikacemi. Existují však zařízení, jež nelze považovat za klasické počítače, ale běží na nich Windows 10. Ta ale není možné považovat v tuto chvíli za kvalitně zabezpečitelná podle zákona, protože jejich specifické úpravy nelze jednoduše definovat a nenacházejí se na místech, kde se zpracovávají utajované informace. Jedná se například o průmyslové stroje.

Pokud se jedná o počítače s přístupem do internetové sítě, je to s jejich bezpečností složitější. Jedna z prvních věcí, která se u nich musí zabezpečit, je přístup do internetové sítě. Počítače, které nemají přístup do internetové sítě, lze v současné době velmi kvalitně zabezpečit, například podle pravidel NÚKIB. Tato pravidla nastavují vnitřní politiku počítače tak, aby v případě nutnosti chránila informace uložené uvnitř (třeba proti útočníkovi uvnitř organizace). Skutečnost, že operační systém Windows 10 je nejrozšířenějším operačním systémem pro počítače na světě, s sebou nese výhody jak pro administrátora, tak i pro případného útočníka. Existuje spousta webů s návody a popisem toho, co a jak nastavit a zabezpečit, případně záplatovat. To je velká výhoda pro administrátora a nevýhoda pro útočníka. Má to však i druhou stranu mince, protože existuje i mnoho návodů s podrobným popisem, jak a kam zaútočit. Rozhodnout se v takovém případě, co je pro útočníka výhodnější – tedy zda útočit na systém a jeho implementaci, nebo se soustředit na uživatele – je těžké. Osobně bych v takovém případě upřednostnil kombinaci obojího.

4.2.2 Popis operačního systému Linux

Linux je jádro operačního systému původně vyvíjeného jedním nadšencem do informačních technologií pro zpestření výuky. Tento nadšenec se pro svou tvorbu inspiroval operačním systémem UNIX. Po jeho prvním zveřejnění na internetu, v roce 1991, se strhl velký zájem o jeho vylepšení a využívání. Dnes tento systém žije svým vlastním životem, kdy je vyhledáván především komunitou nadšenců, expertů a jiných (často specifických) uživatelů. Tento systém je typem open-source, jeho zdrojové kódy jsou tudíž veřejné. Existuje celá řada tzv. distribucí, jež toto jádro využívají, přičemž některé jsou vyvíjeny komunitně a distribuovány zdarma, zatímco jiné jsou vyvíjeny firmami na komerční bázi. Tento systém je, bohužel, v dnešní době výrazně opomíjený. Z pohledu bezpečnosti existují dvě serverové distribuce s bezpečnostní certifikací dle EAL4. Jsou to RHEL a SUSE – obě v provedení Enterprise Server. Za nimi stojí finančně silné společnosti, které mají do tohoto papírového „krmení medvěda“ alias procesu certifikace ochotu investovat své zdroje. Pro určitá použití je však nevýhodou RHEL, který má kratší dobu podpory nových verzí OS. Například pro raketové systémy nebo další armádní systémy. Ty přitom musí fungovat alespoň 20 let. Pokud je uživatel v situaci, kdy kvůli novému HW musí neustále měnit SW, tj. neustále nasazovat nové verze OS, je často problém se udržet na certifikovaných verzích OS, jež jsou naopak staršího data. V takovém případě je snadnější si zvolit OS typu SUSE, protože díky méně častému vydávání novějších verzí OS a jejich delší podpoře je interní certifikační audit méně náročný.

Všeobecně je totiž známo, že bezpečnostní audit je jak personálně, tak i finančně náročná, dokonce snad nejnáročnější záležitost každého technického projektu, takže jakákoliv snaha jej minimalizovat je zároveň alfou i omegou realizovatelnosti projektu.

5 Podmínky zabezpečení

5.1 Přístupové údaje a jejich uchovávání

Aby bylo možné eliminovat možnosti vniknutí do systému neoprávněnému uživateli a snížit tím rizika na přijatelnou úroveň, je nutné zabránit nepovoleným osobám v přístupu k nim, do nich. V rámci přístupu k údajům a uchovávání informací je tato kapitola rozdělena na dvě části:

- způsob zaznamenávání přístupů,
- uchovávání informací přístupů.

Zaznamenávat přístup v rámci informační bezpečnosti lze mnoha způsoby. Přistupovat k zařízením lze například pomocí čipové karty nebo biometrických snímačů. Ty bývají využívány zpravidla v rámci evidence přístupů do budovy nebo objektu, PIN například do alarmu objektu. Hesla se nejčastěji používají k přístupu do počítače – do BIOSu nebo operačního systému. Uvedené způsoby zaznamenávání přístupů lze nahradit také speciálním hardwarem, například TOKEN.

Uchovat informace v zařízeních u těchto způsobů přístupů lze níže uvedenými způsoby:

Otevřená podoba na fyzickém nezabezpečeném hardwaru

- není bezpečná,
- například starší počítače, neobsahující TPM čip, ukládaly otisk jako obyčejný komprimovaný soubor s vlastní koncovkou. Tento soubor šlo velmi jednoduše okopírovat. Otisk prstu (i na levném mobilním telefonu), lze sice považovat za obecně bezpečný, ale takto hodnotit lze jen jeho ukládání. Jeho snímač však brát za důvěryhodný nelze. Jednoduše řečeno – oblast na snímání otisku je velmi malá, než aby dokázala kvalitně sejmout papilární linie. Odemknout takto zabezpečený mobil pak lze i za použití nekvalitní kopie otisku prstu. Můžeme tedy konstatovat, že staré a low-end zařízení není vhodné používat pro práci s citlivými daty.

Otevřená podoba na vzdáleném nezabezpečeném úložišti

- není bezpečná,
- takto mohou být řešeny například přístupové terminály ve velkých korporacích, kde je před bezpečností preferována především evidence.

Otevřená podoba na fyzickém zabezpečeném hardwaru

- bezpečná,
- například hesla v počítači mohou být takto uchována, protože je v tomto případě pokryt nedůležitější bezpečnostní faktor – hardware

Otevřená podoba na vzdáleném zabezpečeném úložišti

- nebezpečná, pokud není zaručená bezpečnost přenosu.

Zašifrovaná podoba na fyzicky i vzdáleném nezabezpečeném hardwaru

- nevhodná,
- je zde pokryt jen jeden faktor bezpečnosti, a to zašifrování požadovaného dokumentu,
- mnoho uživatelů si například zašifruje svá hesla nebo soubor hesel, jež následně přesunou do Cloudového úložiště, aby k nim mohli kdykoliv a odkudkoliv přistupovat. Před bezpečností je tak prioritně preferován přístup.

Zašifrovaná podoba na fyzicky zabezpečeném hardwaru

- doporučená,
- u moderních mobilních telefonů s operačním systémem Android se používá zabezpečení na softwarové i lehce hardwarové bázi Trusted Execution Environment (TEE). To znamená, že na izolované části hardwaru běží malý, ale efektivní Trusty OS a jeho ovladače pro komunikaci se zbytkem zařízení. Zde jsou uložena například data o otiscích prstů, certifikáty a další. Google –

výrobce operačního systému Android – dal podmínku všem výrobcům, kteří chtějí používat jeho systém s biometrickými údaji, že veškerá analýza údajů o otiscích prstů musí být provedena uvnitř TEE.

To znamená, že:

- veškerá data spojená s otiskem prstu musí být uložena v TEE nebo důvěryhodné paměti, což je paměť, kterou hlavní procesor neuvidí;
- data otisku prstu musí být šifrována samostatně;
- při odebírání uživatelského účtu musí být veškeré informace z telefonu odstraněny;
- žádná aplikace nebo proces nesmí vidět profily otisku prstů;
- otisky prstů a data nesmí být zálohována v žádném jiném úložišti;
- ověření otisku prstu je povoleno pouze procesu, který o něj požádal. [7]

Například firma Samsung u svých telefonů používá k těmto účelům speciální hardwarový kontejner Knox.

Firma Apple u svých zařízení používá podobnou technologii, tato technologie se nazývá Secure Enclave. Otisk prstu se ale nikam neukládá, je převeden na druh matematického znázornění. To je nadále šifrováno a chráněno klíčem, který je dostupný pouze pro Secure Enclave. [8] Windows 10 používá pro bezpečné přihlášení TPM čip s podobnými vlastnostmi a použitím jako již dvě zmíněné technologie.

5.2 Vícefaktorová autentizace

Vícefaktorová autentizace je v rámci bezpečnosti vysoce doporučovanou metodou ochrany. Čím více faktorů přihlášení totiž existuje, tím menší má útočník možnost přihlášení. Vícefaktorovou autentizaci lze v současné době rozdělit na tři základní faktory:

První faktor se soustředí na znalost uživatele. Jedná se vlastně o vše, co si uživatel dokáže zapamatovat, tj. PIN, heslo, znak a další.

Druhý faktor se soustředí na něco v držení uživatele, tj. například klíč, token, čipovou kartu a další.

Třetí faktor se soustředí na nějakou jedinečnost uživatele. Většinou se jedná o biometrická zařízení.

5.3 Zabezpečení mobilních zařízení

Mobilní zařízení nemají sama o sobě možnost vynucení bezpečnostních politik, tak jako to má například Windows 10. Proto se používají níže zmíněná řešení.

5.3.1 Zabezpečení mobilních zařízení pomocí MDM

Mobile device managament (MDM) je nadstavba pro většinu OS mobilních zařízení, která ulehčuje jejich konfiguraci a zabezpečení. Jedná se většinou o aplikaci do mobilního telefonu, server a dashboard. Aplikace může být již nainstalovaná v mobilním zařízení, nebo ji lze dodatečně nainstalovat. Server slouží pro zprostředkování komunikace mezi mobilním zařízením a správcovským dashboardem.

Dashboard slouží jako souhrnná nástěnka pro vzdálenou konfiguraci mobilních zařízení. Zde se nastavují restrikce, pravidla a další vlastnosti, jež uživatel může a nemusí dělat na svém mobilním zařízení. Server a dashboard může být zprostředkováván vzdáleně u poskytovatele tohoto MDM nebo v bezpečnějším režimu on-premise (vše má u sebe a pod kontrolou).

Řešení MDM je velmi pohodlné pro administrátora, který musí spravovat větší množství mobilních zařízení. MDM řešení lze propojit i s různými analytickými nástroji, jako je například SandBlast od CheckPointu. Díky tomu dokáže administrátor vyhodnotit závadnou aplikaci a pomocí MDM ji na všech mobilních zařízeních zakázat. MDM dokáže například řešit autorizovaný a neautorizovaný přístup do sítě, připojení či vymazání zařízení nebo přidělení práv uživateli.

V současné chvíli neexistuje v České republice řešení, jež by dokázalo plnohodnotně zabezpečit mobilní telefon. Neexistuje ani šablona, oficiální seznam doporučení, na které by bylo vhodné se odvolávat. Velmi doporučovaným řešením je tedy zabezpečení právě pomocí MDM a kombinací dalších nástrojů.

5.3.2 Zabezpečení mobilního zařízení pomocí EMM

Enterprise Mobility Management (EMM) je výraz pro označení technologií pro zabezpečení a správu mobilních zařízení zaměstnanců podniků, firem či pracovišť (chytré telefony, tablety apod.), kteří ve své práci mohou kdykoliv a odkudkoliv přistupovat k podnikovým či firemním datům. Tato zařízení je však třeba hromadně spravovat a zabezpečit proti úniku citlivých informací.

Díky Enterprise Mobility Management technologiím mohou být všechna mobilní zařízení (včetně soukromých v režimu BYOD) spravována z jedné administrátorské konzole a firemní data zůstávají pod kontrolou. Oproti MDM, které spravuje pravidla a nastavení v zařízení, EMM zabezpečuje mj. i přístup do jejich systémů. [9]

5.3.2.1 *Bring Your Own Device*

Zaměstnanci používají pro práci svá vlastní zařízení (BYOD – Bring Your Own Device, přines si své vlastní zařízení). To zvyšuje nároky na bezpečnost citlivých firemních informací, k nimž se zaměstnanci ze svých zařízení připojují. Díky použití některé z EMM technologie je snadné i zařízení v BYOD režimu vzdáleně spravovat.

Administrátor má přehled pouze o firemní části zařízení, do části soukromé nemá přístup. V případě ztráty zařízení či odchodu zaměstnance z firmy vzdáleně smaže pouze firemní data. [10]

5.4 Doporučená nastavení mobilního zařízení / MDM / EMM

Samozřejmě existuje neoficiální soubor nepsaných pravidel, co a jak by se mělo u desktop a mobilních zařízení nastavit.

Jako příklad je možné uvést:

zakázaná wifi

- Přístupový bod lze jednoduše podvrhnout, čímž je myšleno vytvoření stejně pojmenovaného přístupového bodu, jaký už dané zařízení zná, a sledovat pomocí něj komunikaci zařízení, resp. číst přenesená data.

zakázané bluetooth

- Starší verze bluetooth (BT), které neobsahují téměř žádné bezpečnostní prvky, lze jednoduše napadnout, například se na ně připojit.
- Novější verze bluetooth již obsahují bezpečnostní prvky, jako jsou eliptické křivky. Na Mikulášské kryptobesídce v roce 2019 měl izraelský kryptograf, prof. Eli Biham, skvělou přednášku právě na toto téma. Útok, na nějž přišel prof. Eli Biham se svým studentem Liorem Neumannem, patří mezi pokročilé útoky na implementaci, který implementátoři nečekali. Tajný klíč se v uvažované verzi bluetooth ustanovuje pomocí ECDH, tedy kryptografie na bázi eliptické křivky. Obě párovaná zařízení používají tutéž bezpečnou křivku. Pod pojmem bezpečná křivka zde rozumíme to, že určitá matematická úloha (v tomto případě problém hledání diskrétního logaritmu) je na této křivce současnými znalostmi a technologiemi neřešitelná v rozumném čase. Útočník je schopen pozměnit zprávy, jež si zařízení posílají, a to tak, že počítají na jiné křivce (než by se normálně použila), na níž je tato úloha snadno řešitelná. Díky tomu útočník získá klíč.

  Je tedy možný útok „man in the middle“. [11] Nejnovější informace o takovém útoku lze dohledat v publikaci „Breaking the Bluetooth Pairing– The Fixed Coordinate Invalid Curve Attack“. [12] Při kombinaci více faktorů, jako je například NFC, lze aktivovat různé periferie mobilního telefonu, například bluetooth. Jednoduchým příkladem jsou dnes moderní přenosné reproduktory. Jejich připojení není nijak složité, stačí mít zapnuté NFC, které aktivuje bluetooth a spáruje se s daným reproduktorem. Komunikace přes bluetooth může být v některých případech považována za bezpečnou, například pokud se jedná o veřejně známé informace. I zde platí pravidlo, že je vždy lepší útokům předcházet a preventivně mít BT vypnuté. Nikdy nevíte, kdo a kdy objeví novou zranitelnost. Další známé útoky: BlueBorne, Bluetooth Low Energy Jamming, Bleedingit.

zakázané NFC

- Zranitelnost mobilního telefonu pomocí NFC je vysoká. Od té doby, co je NFC využíváno především pro mobilní platby, výrobci změnili svoji strategii a NFC je u nových zařízení po prvním spuštění již zapnuté, což si mnoho uživatelů neuvědomuje. Stačí pak jednoduchý dotyk „nakaženého“ terminálu, kdy cílové zařízení pouze zobrazí nenápadnou výzvu o instalaci aplikace (útočníkovi), která je podobná například běžné aktualizaci. Prakticky je tento útok popsán v publikaci „Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones“ [13].

zakázané polohové služby

- Lze jimi sledovat polohu telefonu. Pokud jste významná osoba, je to nebezpečné.

zákaz instalace aplikací z neznámého zdroje (přímo vlastnost v Androidu)

- Umožňuje do telefonu propašovat neznámou aplikaci nejisté funkčnosti.

zákaz instalace firmware updatů

- Mohou způsobit nekompatibilitu použitých bezpečnostních nastavení, nemusela by fungovat podpora MDM.

zákaz USB debugging

- Ladění pomocí USB -> umožní zařízení komunikovat s počítačem oboustranně a využívat pokročilé techniky.

zákaz screen captures

- Zavirovaná aplikace by mohla kopírovat aktivitu na display.

zákaz synchronizace

- Není vhodné ukládat, sdílet svá data do vzdáleného úložiště, které není pod přímou osobní ochranou.

zákaz prediktivního zadávání textu na klávesnici

- Prediktivní zadávání si pamatuje, učí se napsané věci -> je nevhodné při zadávání hesel a přístupových údajů.

nezálohovat data

- Záloha dat je nepřípustná, kdokoliv by je mohl odcizit – zálohování je ze své podstaty nebezpečné, je to totéž jako napsat si poznámku na papír a tu vložit do kartotéky. Většina organizací volí možnost nezálohování dat na mobilních zařízeních. Jejich bezpečné zálohování by bylo velmi náročné na investice a lidské zdroje.

black list aplikací

- Seznam známých škodlivých aplikací, jako je například aplikace Baterka, používající bluetooth.

white list aplikací

- Seznam povolených aplikací, například firemních aplikací nebo služeb.

při ztrátě vzdáleně smazat zařízení

- Je to první doporučená akce při ztrátě telefonu, aby nedošlo ke kompromitaci jakéhokoliv materiálu uvnitř telefonu.

pokud to lze, využívat dvoufaktorové ověřování

- Je vhodné vynutit minimálně PIN a druhý faktor alespoň přihlášení pomocí biometrických údajů.

povolená jen soukromá vpn

- Přistupovat k internetu a datům pouze přes kvalitní firemní infrastrukturu.

Databáze uživatelů umístěná ve vlastní infrastruktuře, ven pouštět jen anonymizované informace

- Zamezí se případnému přístupu k informacím od poskytovatele bezpečnostního řešení.

5.5 Fakta o obejití zabezpečení operačního systému v mobilních telefonech

Pro bezpečnostní služby na celém světě je důležitá možnost nabourat se do mobilních zařízení podezřelých osob. Je známá kauza, kdy americká FBI zabavila muži podezřelému z terorismu jeho mobilní telefon iPhone 5c. V telefonu bylo nastaveno, že po 5 špatných přihlášeních se telefon celý smaže. Zbývaly už jen dva poslední pokusy. FBI tedy požádala Apple o zpřístupnění zadních vrátek do systému. Apple tuto žádost odmítl s tím, že se sice jedná o muže podezřelého z terorismu, ale pokud by vyšetřovatelům zpřístupnila zadní vrátka, umožnilo by to FBI zároveň kontrolovat kohokoli. Po tomto oznámení se ozvala izraelská firma, že by si s problémem dokázala poradit a zadní vrátka odemknout, což se následně také podařilo.

Poznámka:
Izraelské firmy jsou v hackerském oboru na světově špičce. Této problematice se věnují především dvě firmy: izraelská Cellebrite a americká Grayshift. Firma Cellebrite nabízí nástroj s názvem UFED – Universal Forensic Extraction Device Premium. Na svých webových stránkách deklaruje, že se dokáže nabourat do těchto typů zařízení:

- *veškerá mobilní Apple zařízení,*
- *veškeré modely a především vlajkové lodě značky Samsung,*

- *populární modely značek Motorola, LG, Huawei, Sony, Oppo, Nokia, ZTE, VIVO a Xiaomi.*

Osobně jsem měl možnost s nimi na jedné konferenci hovořit. Bylo mi řečeno, že jim stačí donést jakýkoliv mobilní telefon a nejpozději do měsíce jsou schopni jej úplně nabourat a dešifrovat.

5.6 Zabezpečení OS Windows 10 podle zákona 412/2005 Sb.

V této kapitole je uveden výčet požadavků, jež musí počítače s operačním systémem Windows 10 splňovat, aby byly v souladu se zákonem. V některých specifických případech lze od některých požadavků ustoupit, to však vyžaduje zabezpečení oblasti a souhlas pracovníka certifikačního oddělení.

5.6.1 Instalace a aktualizace operačního systému

Počítač musí mít nově nainstalovaný čistý operační systém nebo předinstalovaný a nikdy nespuštěný od výrobce na disku v souborovém systému NTFS. Jsou zakázány všechny volitelné podsystémy. Operační systém musí být aktivovaný a legální. Systém nesmí být obnovitelný do výchozího stavu. Je povolená aktualizace systému nebo jeho komponent pouze v režimu off-line. To znamená, že pověřená osoba přinese na vyměnitelném médiu aktualizaci, kterou následně nainstaluje do počítače.

5.6.2 Instalace a nastavení antivirového programu

Je nutná instalace antivirového programu, pokud se nepoužije Windows Defender. Antivirový program musí mít zapnutou rezidentní ochranu včetně testování zásuvných paměťových médií, jako jsou například diskety, CD, DVD a USB. Antivirus je nutné aktualizovat, ideálně pomocí stažení aktualizací na zařízení s přístupem do veřejné sítě, jež se na bezpečném médiu přenesou do počítače.

5.6.3 Zakázání periferií

Samozřejmostí je zákaz veškeré možné drátové i bezdrátové komunikace, jako je například WiFi, Bluetooth, Infraport, LAN (ve specifických případech lze LAN port povolit) a další. Tento zákaz lze řešit manuálně pomocí přepínače v BIOSu nebo v operačním systému.

5.6.4 Nastavení aplikací

Pro zpřehlednění operačního systému je vhodnější odinstalovat nepotřebné aplikace, jež bývají součástí operačního systému. Jsou to například 3Dbuilder, Bingfinance a další. Součástí systému je i aplikace OneDrive. Té je nutné zakázat a jejím komponentům bránit, aby byly použity jako úložiště souborů. Je zakázáno používat technologii ReadyBoost, využívající paměťová média.

V systému je nutné zakázat možnosti automatického přehrávání. Samozřejmostí je i zákaz systémových služeb pro automatickou konfiguraci těchto síťových periferií. V případě nastavení uživatelských práv pro skupiny k systémovým souborům a adresářům se ve větší míře důvěřuje výchozímu nastavení operačního systému + drobným specifickým úpravám.

5.6.5 Nastavení pravidel skupin a profilů uživatelů

Pro nastavení uživatelských práv pro skupiny je nutné mít správně vytvořené profily. Výchozí – pevně zabudované účty Administrator a Guest – jsou zablokované.
Nově musí být vytvořeny účty:

- Správce počítače – ten je členem skupiny Administrators,
- Bezpečnostní správce počítače – ten je členem skupiny Users a Event Log Readers,
- Uživatel – ten je členem skupiny Users.

Jedním z mála povolených externích zařízení jsou tiskárny. I těm je však nutné přiřadit určitá pravidla. Mohou k nim přistupovat uživatelé skupiny Administrators a Users. Mohou též instalovat ovladače tiskáren.

5.6.6 Nastavení pravidel přihlašování

Tato pravidla a zásady by byly k ničemu, pokud by s nimi mohl pracovat kdokoli. Proto je nezbytné nastavit hesla k jednotlivým profilům; přesněji: správné zásady hesel. To je například složitost nebo minimální délka hesla, ta je stanovena na 9 znaků. Stáří hesla je minimálně 1 den a limit maximálně 90 dní. Je zakázáno používat ukládání pomocí reverzibilního šifrování. Stejné heslo se může použít až po použití 24 dalších různých hesel. Doba uzamčení účtu po opakovaně špatně zadaném hesle je nastavena na 0 minut; to znamená, že je účet uzamčen, dokud není administrátorem znovu odemčen. Počet špatně zadaných hesel je stanoven na 3 chybné pokusy. Vlastnost v systému nazvaná „Vynulovat čítač uzamčení účtu“ nastavuje interval u počtu možných špatných pokusů o přihlášení. Pokud máme například nastavené maximálně 3 špatné pokusy na přihlášení, pokud zadáme 1. nebo 2. heslo špatně a počkáme si tento interval, pak máme opět 3 pokusy. Pokud ovšem zadáme i potřetí heslo špatně, účet se podle předchozí zásady uzamkne. Záměrně zde používám pouze slovo „heslo“. Není totiž dovoleno používat PIN kód a obrázkové heslo. Je povolené pouze klasické přihlašování.

5.6.7 Nastavení auditu

Aby auditor mohl kontrolovat dodržování zmíněných pravidel, musí být stanoveny zásady auditu. Auditují se úspěšné a neúspěšné pokusy a operace při auditování správy účtů, systémových událostí, události přihlášení, události přihlášení k účtu a změn zásad. Jak jsem již na začátku naznačoval, výchozímu nastavení uživatelských práv se ve větší míře důvěřuje, ale jsou nutné drobné specifické úpravy, jako je například povolení pouze skupině Administrators obnovení souborů a adresářů. Odepřít místní přihlášení může pouze skupina Guests. Naopak skupiny Users a Administrators mohou povolit místní přihlášení. Vypnout operační systém může pouze Administrators a Users. Uživatelé těchto skupin musí být přihlášeni, aby mohli systém vypnout. S tím souvisejí další nastavení, jako například neprovádět žádnou akci při stisknutí tlačítka napájení.

Zálohovat soubory a adresáře může (pouze z bezpečnostních důvodů!) skupina Administrators. Na první pohled banální, ale ve výsledku důležité úpravy, jako je například změna časového pásma nebo systémového času, mohou provádět pouze Local Services a Administrators. I taková drobná změna, jako je změna času, může při auditu zakrýt stopy při nepovolené činnosti na počítači. Pokud není možnost auditu, systém se vypne. Velikost souboru protokolu je doporučená na 50 048 kB. U verzí Windows 8–10 se musí nastavit limit pro interaktivní přihlašování při nečinnosti počítače na 900 s. Totéž platí i pro limit šetřiče obrazovky.

5.6.8 Nastavení pro zjednodušení obsluhy

Aby nedošlo k nejasnostem, musí se ošetřit každá možná eventualita, jež by mohla uživateli znepříjemnit přihlašování. Například nadpis pro uživatele snažícího se přihlásit musí obsahovat slovo „Upozornění“. Uživatel následně zbystří, že má dávat pozor. Po tomto upozornění se uživateli pokoušejícímu se přihlásit musí zobrazit text: „Přihlašujete se do informačního systému nakládajícího s utajovanými informacemi podle zákona č. 412 / 2005 Sb. Nejste-li autorizováni pro práci v tomto systému, ihned se odhlaste, jinak se vystavujete možným sankcím podle tohoto zákona.“ Účel tohoto textu je všeříkající. Aby nedošlo k rychlému zablokování účtu, například při náhodném zavadění o klávesy a tlačítka enter, doporučuje se do režimu přihlášení vejít pomocí kláves CTRL + ALT + DELETE. Náhodné zmáčknutí těchto tří kláves najednou je velmi nepravděpodobné. Je nutné nezobrazovat naposledy použité uživatelské jméno, aby nedošlo k „ulehčení“ pro případného útočníka. Je nezbytné toto zakázat při již spuštěném systému, ale i po restartování systému. Uživatel je vždy 14 dní před exspirací hesla upozorněn, aby si změnil heslo. Nesmí nastat situace, kdy je standardní uživatel vyzván ke zvýšení oprávnění. Je povolen režim schvalování správce pro integrovaný účet správce. Je důležité zablokovat účty Microsoft, je zakázáno je vytvářet a přihlašovat se k nim. Ty by v případě bezpečnostního incidentu, jako je například připojení počítače do veřejné sítě, všechno odeslaly ven a došlo by ke kompromitaci. Je vhodné též přejmenovat účet Guest a učet správce. Jde o jasnější identifikaci přihlášených uživatelů při případném auditu. Stav účtu správce je nastavený na Povoleno

pouze při existenci jednoho administrátorského účtu. Musí zde být ale nastaveno silné heslo a musí být používán pouze v nouzových případech.

Zakazuje se zpracování místních objektů Zásad skupiny a protokolování výsledné sady zásad. Je nutné zakázat veškerá oznámení na zamykací obrazovce a vstupní body pro Rychlé přepínání. Proto je také požadováno automaticky zálohovat a řídit chování protokolu událostí při jeho naplnění. Správcům je zakázáno přepisovat zásady Omezení pro instalaci zařízení. Pokud by nastala situace, kdy nastavení zásad znemožní instalaci zařízení, je příhodné na tento problém upozornit uživatele. Povolená zařízení, jež se budou připojovat k počítači, je nutné si ujasnit hned na začátku nebo pod dozorem bezpečnostního správce. Je nutné tato zařízení identifikovat například pomocí identifikátorů, jimiž se hlásí do systému. Tyto identifikátory je potřeba povolit v systému, protože systém může pracovat se zařízením jemu známým a povoleným. Spouštění, čtení, výmaz, zápis nebo přístup k těmto zařízením mu může být ale i odebrán. Například je zakázáno používat webovou kameru i při přihlašování a prezentace na zamykací obrazovce. Šetřič obrazovky je povolený, nesmí ale provádět změny v systému jakéhokoli charakteru a opět musí být chráněn heslem. Jeho časový limit musí být nastaven rovněž na 900 vteřin. Pokud uživatel odstraní soubor, tak se tento soubor nepřesune do koše, ale úplně se vymaže.

5.7 Zabezpečení OS Windows 10 s přístupem do veřejné sítě

Zabezpečit počítače a celkově všechna zařízení, která je možno připojit do veřejné internetové sítě, je velmi složité. Nelze je totiž plně fyzicky zabezpečit před útoky přes síť. Vždy existuje možnost, jak propašovat skrze síťové připojení škodlivý kód. Útočník většinou nemá omezené zdroje, zato majitelé zařízení připojených do sítě ano. Lze tomu alespoň částečně předcházet. Bohužel neexistuje oficiální dokument – norma pro zabezpečení počítačů přistupujících do veřejných sítí. Každá země, stát, organizace vlastní většinou pouze seznam doporučení. Zde uvádím odkaz na vzorové doporučení od britské vlády pro nastavení Windows 10 na koncových stanicích: https://www.gov.uk/government/publications/end-user-devices-security-guidance-windows-10/end-user-devices-security-guidance-windows-10

5.7.1 Obecná bezpečnostní doporučení

Základem je správné nastavení síťových prvků, jako je router, modem, firewall, diody apod. Pokud se jedná o počítač, je důležité si na začátku procedury zabezpečení ujasnit, jaké aplikace potřebuji na svém počítači.

Já osobně bych situaci řešil následovně:

- aplikace nutné pro zajištění základních služeb zařízení a zajištění připojení,

- aplikace umožňující uživateli provádět základní pracovní činnosti.

Reprezentativní příklad takovýchto aplikací je: MS Office, Adobe Reader, Mozilla Firefox, Notepad ++, Total Commander, VLC.

Lze rovněž doporučit několik pravidel, jež by měl uživatel dodržovat, aby jeho počítač nepodlehl útočníkovi. Jedná se především o veškeré aktualizace od výrobce operačního systému, dále použití kvalitního antiviru, neklikat na podezřelé reklamy, e-maily, webové stránky, nestahovat podezřelý software, používat kvalitní hesla. Není od věci použít i doporučená nastavení podle zákona 412/2005 a snažit se vždy ochránit svoji identitu, tedy mazat historii surfování na internetu a připojovat se pouze přes ověřené připojení do veřejné sítě (například se připojovat přes VPN).

5.7.2 Bezpečnostní prvky používané s Windows 10

Je doporučeno používat UEFI (2.3.2.c a novější), které podporuje SecureBoot. UEFI samo o sobě je nové rozhraní oproti klasickému BIOSu, jež například podporuje Secure Boot a GPT. Má také mnohé výhody, ovšem i nevýhody. Jednou z nevýhod je skutečnost, že výrobce ukončil podporu pro starší typy procesorů, které mohly vykazovat velkou zranitelnost. Jejich podpora se stejně nevyplatila. Díky tomuto postupu nebylo nutné s nimi držet zpětnou kompatibilitu a výrobce mohl využít nových vlastností novějších procesorů.

5.7.3 Bezpečnostní součásti Windows 10

SecureBoot je bezpečná metoda startování počítače. Díky ní však vznikl problém s instalací jiných operačních systémů, než jsou Windows 8 a novější. SecureBoot je podporována pouze u 64bitových systémů. Pokud se dodržuje správné zacházení s operačním systémem, dokáže toto zabezpečení předcházet Rootkit a Bootkit útokům, jež většinou přicházejí z vnější internetové sítě.

TPM neboli Trusted Platform Module je součást počítače, díky níž je možné používat bezpečnostní prvky, jako jsou bezpečné ukládání klíčů, dvoufaktorová autentizace nebo šifrování disku. Doporučená verze pro používání TPM je verze 2.0.

Správně nastavený Windows Firewall na straně koncového zařízení je též doporučovaná vlastnost. Jednoduše: zakázat vše a pak postupně povolovat vlastnosti nutné pro chod systému nebo potřeby uživatele.

Osobně doporučuji použít také Virtual Based Security (VBS), jež řeší zabezpečení na základě virtualizačních metod – izoluje od operačního systému procesy v počítači a tím ochraňuje klíčové procesy OS.

Windows Defender Credential Guard je softwarová i hardwarová vlastnost Windows 10, využívající VBS pro izolaci Local Security Authority (LSA). Díky tomu data uložená v izolované LSA nejsou přístupná zbytku operačního systému, a tak odolávají Pass the Hash nebo Pass The Ticket útokům. Hash chrání heslo a WDCG chrání hashe.

Při použití Windows Defender Application Control je počítač odolnější proti malware – využívá VBS a konfigurovatelnou kontrolu integrity kódu na úrovni uživatele (tzv. „User Mode Code Integrity“, UMCI) a kernelu (tzv. „Kernel Mode Code Integrity“, KMCI). Znemožňuje spustit jakýkoliv proces, který neodpovídá nastaveným parametrům, již na úrovni OS. Podobnou vlastnost, jaká byla uvedena u MDM, existuje i u Windows 10. Jmenuje se AppLocker, používá se whitelisting aplikací.

Microsoft aplikace, kterou bych doporučil každému, kdo nechce přijít o svá data, je Microsoft BitLocker. Používá se k šifrování disku a zajišťuje ochranu citlivých informací. Jeho další vlastnost umožňuje i kontrolu integrity celého systému. BitLocker se doporučuje používat především na počítačích, které mají TPM čip. Tam je jeho účinnost největší.

Další bezpečnostní vlastností, již má Windows 10, je Exploit Guard. Jedná se o sadu nových možností ochrany koncového zařízení Windows 10 před napadením, která současně umožňuje snížit možnosti útočníka na úrovni jednotlivých aplikací. Její součástí je například Attack Surface Reduction (ASR). Ochrání počítač před malwarem na bázi Office dokumentů, jejich skriptů a kombinací těchto dvou věcí v e-mailu.

V korporacích se tato nastavení řeší hromadně s využitím MDM. Stejně jako u zabezpečení podle zákona 412 bych pro přihlášení do systému doporučil použití jak klasického uživatelského jména, tak i složitého hesla. Je to univerzální řešení pro každého, kdo se potřebuje jednoduše přihlásit a zároveň udržet úroveň bezpečnosti. Je-li třeba využívat i přihlášení pomocí biometrických zařízení, určitě bych doporučil toto přihlášení používat pouze u profilů typu Host, přičemž bych u nich omezil veškerá práva a možnosti na minimum. Pokud ale uživatel chce mít počítač zabezpečený ještě lépe,

než je doporučeno, je možnost přihlašovat se pomocí dvou nebo vícefaktorového ověření, například v kombinaci s čipovou kartou.

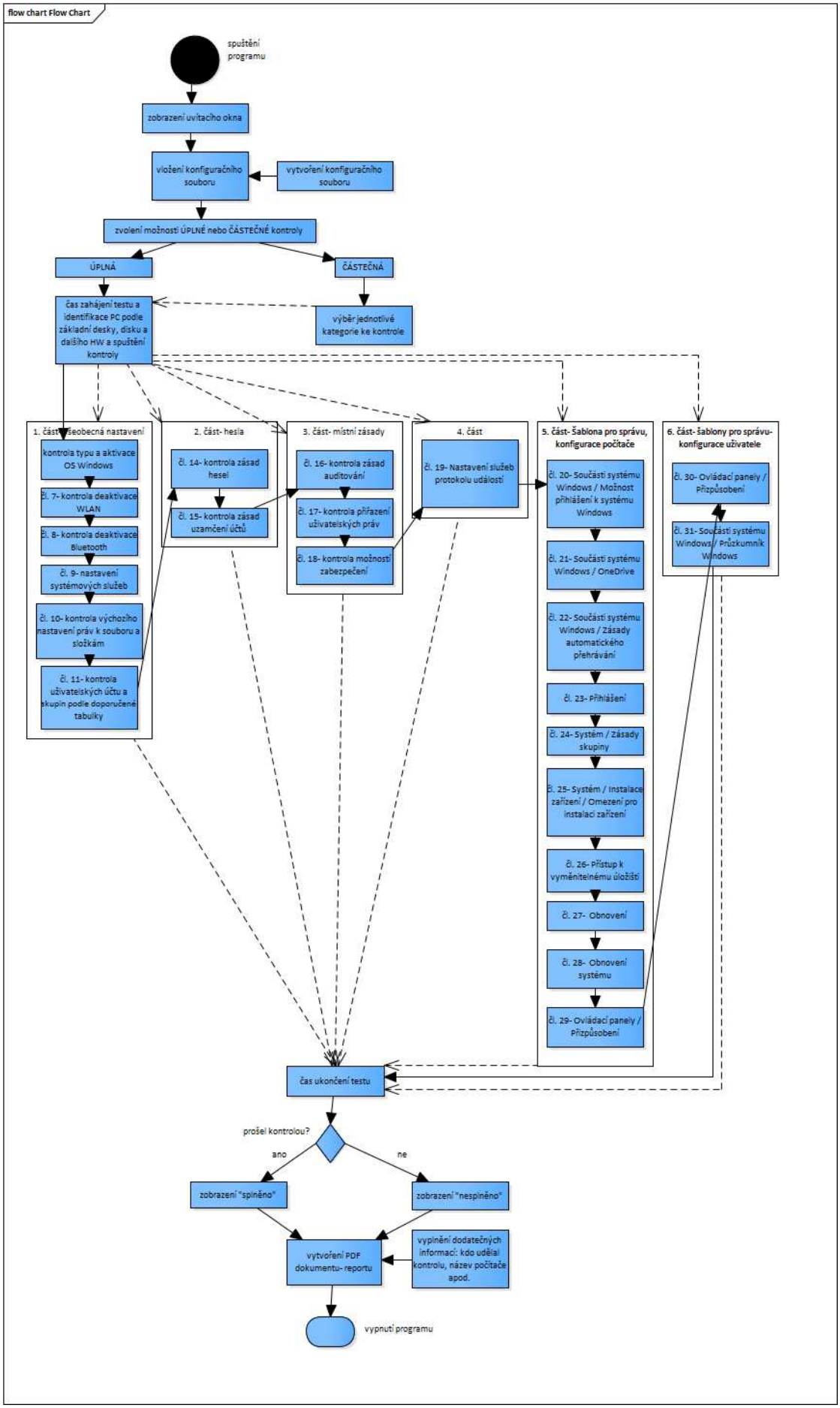
6 Potřebnost řešení

Řešení tohoto problému je velmi přínosné. Bude to velmi efektivní nástroj, který zvýší efektivitu práce a ušetří čas pracovníkům certifikačního oddělení na NÚKIB. V současné době kontrola bezpečnostních politik probíhá manuálně. Tento program dokáže rychleji překontrolovat dané politiky a na závěr vytvořit základní report o proběhlé kontrole.

Program KOBENOS umožní automatický sběr a vyhodnocení informací o konkrétním zabezpečení off-line stanice v souladu s požadavky zákona 412/2005 Sb.

7 Postup při tvorbě programu

Při tvorbě tohoto programu jsem nejprve získal potřebný dokument od certifikačního oddělení s doporučeným bezpečnostním nastavením systému pro Windows 10. Poté jsem zvažoval, jak má vlastně celý program fungovat. Jednoduše jsem si v programu Enterprise Architect navrhl průchod programu.



Graf 1: Průchod programu

Následně jsem si musel ujasnit, jaký programovací jazyk zvolím. Zvolil jsem C# (.NET Core), protože ten nepotřebuje ke svému běhu na Windows 10 žádné dodatečné instalace externích programů nebo knihoven. Pro celý program jsem použil vývojové prostředí Microsoft Visual Studio Community Edition 2019. Začal jsem tedy nejdříve tvořit grafickou část programu. Načrtnul jsem si tak základní rozhraní programu. Pak jsem se soustředil na konkrétní testy. Od započetí testů jsem postupoval od prvního k poslednímu. Použil jsem Windows Management Instrumentation (dále jen WMI). WMI je sada umožňující operačnímu systému poskytovat různá oznámení a informace. Toto rozhraní mi umožnilo přistupovat především k informacím o hardwaru a systému. V tomto rozhraní jsem se na všechny potřebné údaje dotazoval podobným jazykem, jako je dotazování v SQL. V tomto případě je dotazování pojmenováno WMI Query Language (dále jen WQL). Pro lepší orientaci ve WMI jsem použil nástroj zvaný WMI Explorer 2.0. [14] Bohužel i toto rozhraní má své meze. Nenalezl jsem možnost, jak nalézt některé další údaje.

Proto jsem se rozhodl použít další systémový nástroj. Použil jsem tedy PowerShell. PowerShell je výkonný nástroj na zjišťování informací v operačním systému. Stačí jen znát správné příkazy. Potřeboval jsem zjistit informace z registrů. Umět najít a pak přímo číst některé informace z registrů přímo do konzole je pro mě velmi složité, proto jsem si nechal v některých případech vypsat vše potřebné z registrů do souboru a ten pak kontroloval.

Program je nutné spouštět vždy jako administrátor. WMI i PowerShell potřebují k vykonání příkazů toto privilegium.

8 Popis programu a použitých bezpečnostních politik

Program je přeložený pro Windows 10 64-bit verzi. Je nutné ho spouštět jako administrátor, aby WMI i PowerShell dostaly administrátorská práva. Grafika je tvořena ve Windows Presentation Foundation (WPF). Pro WQL používám cestu root\CIMV2. Potom použiji příslušný WQL dotaz pro získání požadované odpovědi.

Příkaz pro PowerShell1 je: `secedit /export /cfg temp.ini; Get-Content -Path .\\temp.ini;`

Příkaz pro PowerShell2 je: `$adsi = [ADSI]\"WinNT://$env:COMPUTERNAME\"; $adsi.Children | where {$_.SchemaClassName -eq 'user'} | where {$_.Name -eq '" + accountName + "'} | Foreach-Object {$_.Groups() | Foreach-Object {$_.GetType().InvokeMember(\"Name\", 'GetProperty', $null, $_, $null)} }`

Uživatelská práva, zásady hesel a zásady auditu jsou vypsaná v souboru z PowerShellu1. Uživatelé a skupiny jsou tam označeni pomocí kódového označení. To je možné si prohlédnout na webu Microsoftu. [15]

Příkaz PowerShell2 dokáže zjistit, v jaké skupině se nachází daný uživatel.

Konfigurační soubor se skládá z těchto částí:

Záhlaví skupiny testů:

```
<suite name="Název testu">
…….
</suite>
```

Dotazování na WMI:

```
<wmi name="název daného testu">
        <scope>adresa ve WMI</scope>
        <query>WQL dotaz</query>
        <eval>
                <first property="název požadovaného sloupce" value="předpokládaná
hodnota v buňce "/>
        </eval>
</wmi>
```

Dotazování na PowerShell1 (PS1):

```
<security name="název daného testu">
        <eval>
                <first property="název třídy" value="požadovaná hodnota/>"
        </eval>
</security>
```

Dotazování na PowerShell2 (PS2):

```
<securityaccount name="název daného testu">
        <accountName>jméno uživatele</accountname>
        <eval>
                <exactCount count="předpokládaný počet skupin"/>
                <hasString value="název skupiny"/>
        </eval>
</securityaccount>
```

Dotazování na registry (REG):

```
<registry name="název testu">
        <key>cesta v registrech</key>
        <value>název hodnoty</value>
        <eval>
                <first value="předpokládaná hodnota"/>
        </eval>
</registry>
```

Program je sestavený z několika komponent. Většina kódu je napsaná v jazyce C# a využívá grafiky WPF. Aby program mohl vyčíst informace o systému, bylo potřeba použít vlastností a knihoven z .NET, .NET Core a WMI. Při spuštění programu se zobrazí uvítací obrazovka s požadavkem na vložení konfiguračního souboru. Konfiguračním souborem se rozumí .xml soubor, v němž jsou napsány veškeré dotazy na hodnoty v systému. Dotazy jsou označeny identifikátory, o jaký typ dotazu se jedná. V konfiguračním souboru lze dohledat dotazy na WMI (WQL), registry a GroupPolicy.

Program má dvě možnosti spuštění testů, a to automatický (spustit vše), nebo manuální režim (spustit vybrané). Nejprve popíši manuální režim (krok za krokem), protože automatický režim dělá veškeré tyto kroky stejně, pouze automaticky projde všechny jeho komponenty. Pokud uživatel vloží konfigurační soubor a zvolí manuální testování, program projde konfigurační soubor.

9 Riziková místa programu

V současné době funguje program na Windows 10 Enterprise (verze 1809, build 17763.503). Rizikovým místem tohoto programu je případný upgrade na novější verze operačního systému Windows od firmy Microsoft. V každé verzi a buildu se, bohužel, nachází drobné odlišnosti, jež mohou některé funkcionality mého programu ovlivnit.

10 Použití

Tento program lze použít pro jakoukoliv organizaci, která má zájem o klasifikovaný systém. To velmi ulehčí práci certifikačnímu oddělení Národního úřadu pro kybernetickou a informační bezpečnost.

11 Dokumentace pro obsluhu programu

11.1 Popis konfiguračního souboru

Vzorový konfigurační soubor má název config.xml a nachází se v hlavním adresáři programu. Obsahuje veškeré proměnné pro testování bezpečnostního nastavení. Konfigurační soubor obsahuje tři typy testování. Jedná se o testování přes WMI, registry a PowerShell. Techniky testování nelze měnit. Je tedy vhodné, aby případné změny prováděla osoba, která má s nimi zkušenosti. Cesty k testovacím scénářům jsou pěvně zadány a nedoporučuji je měnit. Navrhované změny je vhodné provádět pouze u názvu požadovaného sloupce, hodnot, názvu tříd, jmen uživatelů a počtu skupin.

Hodnoty nastavené v konfiguračním souboru jsou zobrazeny v následující kapitole. Originál této tabulky je v příloze (soubor hodnoty_config.xlsx).

11.2 Nastavené hodnoty v konfiguračním souboru

typ testu	Název testu	název proměnné	doporučená hodnota	význam hodnoty
obecná nastavení				
WMI	Kontrola aktivace Windows	value	1	1= aktivovaný
WMI	Kontrola spec. typu OS Windows	value	OK	OK= v pořádku
WMI	Kontrola bootování	Caption	.*\\Device\\Harddisk0.*	výchozí cesta pro bootování
Článek 9 - Nastavení systémových služeb				
WMI	Kontrola deaktivace WLAN- State	State	Stopped	služba je zastavená
WMI	Kontrola deaktivace WLAN- StartMode	StartMode	Disabled	služba je zakázaná
WMI	Kontrola deaktivace WWAN- State	State	Stopped	služba je zastavená
WMI	Kontrola deaktivace WWAN- StartMode	StartMode	Disabled	služba je zakázaná
WMI	Kontrola deaktivace Bluetooth- State	State	Stopped	služba je zastavená
WMI	Kontrola deaktivace Bluetooth- StartMode	StartMode	Disabled	služba je zakázaná
Článek 11 - Kontrola uživatelských účtů a skupin podle doporučené tabulky				
WMI	zablokovaný Administrátor	Status	Degraded	admin je zakázaný
PS2	Správce počítače je člen skupiny Administrators	account name	Správce počítače	Správce počítače= název uživatele
		count	1	1= počet skupin
		value	Administrators	Administrators= název skupiny
PS2	BS je člen kupiny Users a člen skupiny EvenT Log Reader	account name	Bezpečnostní správce	Bezpečnostní správce= název uživatele
		count	2	2= počet skupin
		value	Users, Event Log Reader	Users, Event Log Reader= názvy skupin
PS2	Uživatel je členem skupiny Users	account name	Uživatel	Uživatel= název uživatele
		count	1	1= počet skupin
		value	Users	Users= název skupiny
Článek 14 - Zásady hesla				
PS1	Heslo musí splňovat požadavky na složitost	PasswordComplexity	1	1= nastavení je aktivní
PS1	Maximální stáří hesla	MaximumPasswordAge	90	90= doporučená hodnota ve dnech
PS1	Minimální délka hesla	MinimumPasswordLength	9	6= doporučená hodnota ve dnech
PS1	Vynutit používání historie hesel	PasswordHistorySize	24	24= doporučená hodnota ve dnech
Článek 15 - Zásady uzamčení účtu				
REG	Doba uzamčení účtu	MaxDenials	0	0= doporučená hodnota- zakázáno
REG	Prahová hodnota pro uzamčení účtu	MaxDevicePasswordFailedAttempts	3	3= doporučená hodnota chybných pokusů
REG	Vynulovat čítač uzamčení po	ResetLockoutCount	60	60 = doporučená hodnota v minutách
Článek 16 - Zásady auditu				
PS1	Auditovat použití oprávnění	AuditPrivilageUse	0	0= bez auditování
PS1	Auditovat přístup k adresářové službě	AuditDSAccess	0	0= bez auditování
PS1	Auditovat přístup k objektům	AuditObjectAccess	0	0= bez auditování
PS1	Auditovat sledování procesů	AuditProccessTracking	0	0= bez auditování
PS1	Auditovat správu účtů	AuditAccountManage	3	3 = auditovat úspěšné a neúspěšné pokusy
PS1	Auditovat systémové události	AuditSystemEvents	3	3 = auditovat úspěšné a neúspěšné pokusy
PS1	Auditovat události přihlášení	AuditLogonEvents	3	3 = auditovat úspěšné a neúspěšné pokusy
PS1	Auditovat události přihlášení k účtu	AuditAccountLogon	3	3 = auditovat úspěšné a neúspěšné pokusy
PS1	Auditovat změny zásad	AuditPolicyChange	3	3 = auditovat úspěšné a neúspěšné pokusy
Článek 17 - Přiřazení uživatelských práv				
PS1	Generovat audity zabezpečení	SeAuditPrivilage	*S-1-5-19,*S-1-5-20	*S-1-5-19 = Local Service; *S-1-5-20 = Network Service
PS1	Obnovist soubory a adresáře	SeRestorePrivilage	*S-1-5-32-544	*S-1-5-32-554 = Administrators
PS1	Odepřít místní přihlášení	SeDenyInteractiveLogonRight	Guest	Guest= doporučená hodnota
PS1	Povolit místní přihlášení	SeInteractiveLogonRight	*S-1-5-32-544,*S-1-5-32-545	*S-1-5-32-544= Administrators;*S-1-5-32-545= Users
PS1	Provést úlohy údržby svazku	SeManageVolumePrivilege	*S-1-5-32-544	*S-1-5-32-544= Administrators
PS1	Převzít vlastnictví souborů a dalších objektů	SeTakeOwnershipPrivilege	*S-1-5-32-544	*S-1-5-32-544= Administrators
PS1	Spravovat auditování a protokol zabezpečení	SeSecurityPrivilege	*S-1-5-32-544	*S-1-5-32-544= Administrators
PS1	Vypnout systém	SeShutdownPrivilege	*S-1-5-32-544,*S-1-5-32-545	*S-1-5-32-544= Administrators;*S-1-5-32-545= Users
PS1	Zálohovat soubory a adresáře	SeBackupPrivilege	*S-1-5-32-544	*S-1-5-32-544= Administrators
PS1	Změnit časové pásmo	SeTimeZonePrivilege	*S-1-5-19,*S-1-5-32-544	*S-1-5-19= Local Service;*S-1-5-32-544= Administrators
PS1	Změnit systémový čas	SeSystemtimePrivilege	*S-1-5-19,*S-1-5-32-544	*S-1-5-19= Local Service;*S-1-5-32-544= Administrators

Tabulka 1: Nastavené hodnoty v konfiguračním souboru

Článek 18 - Možnosti zabezpečení				
REG	Audit: Auditovat oprávnění k zálohování a obnovení dat	FullPrivilegeAuditing	0	0= zakázáno
REG	Audit: Auditovat přístup globálních systémových objektů	AuditBaseObjects	0	0= zakázáno
REG	Audit: Není-li možno protokolovat audity zabezpečení, vypnout okamžitě systém	CrashOnAuditFail	0	0= zakázáno
REG	Audit: Vynutit přednost nastavení podkategorie zásad auditování před nastavením kategorie zásad auditování	SCENoApplyLegacyAuditPolicy	0	0= zakázáno
REG	Interaktivní přihlašování: Limit pro nečinnost počítače	InactivityTimeoutSecs	900	
REG	Interaktivní přihlašování: Nadpis zprávy pro uživatele pokoušející se přihlásit	legalnoticecaption	Upozornění	doporučené oznámení
REG	Interaktivní přihlašování: Nevyžadovat stisknutí kláves Ctrl+Alt+Del	DisableCad	0	0= zakázáno
REG	Interaktivní přihlašování: Nezobrazovat naposledy použité uživatelské jméno- kontrola v registrech	dontdisplaylastusername	1	1= povoleno
PS1	Interaktivní přihlašování: Nezobrazovat naposledy použité uživatelské jméno- kontrola přes PowerShell	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName	4,1	4,1= povoleno
REG	Interaktivní přihlašování: Text zprávy pro uživatele pokoušející se přihlásit	legalnoticetext	Jedná se o systém pro zpracování CITLIVÝCH informací.	doporučené oznámení
REG	Interaktivní přihlašování: Vyzvat uživatele ke změně hesla před jeho vypršením	PasswordExpiryWarning	14	14= počet dnů
REG	Konzola pro zotavení: Povolit automatické přihlášení správce	SecurityLevel	0	0= zakázáno
REG	Konzola pro zotavení: Povolit kopírování na disketu a přítup ke všem jednotkám a složkám	SetCommand	0	0= zakázáno
PS1	Nastavení systému: Volitelné podsystémy	MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional	7	7= žádný
REG	Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro správce v Režimu schválení správce- kontrola v registrech	ConsentPromptBehaviorAdmin	4	4= vyzvat k zadání souhlasu
PS1	Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro správce v Režimu schválení správce- kontrola přes PowerShell	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	4,4	4,4 = vyzvat k zadání souhlasu
REG	Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro standardního uživatele- kontrola v registrech	ConsentPromptBehaviorUser	0	0= automaticky zamítnout
PS1	Řízení uživatelských účtů: Chování výzvy ke zvýšení oprávnění pro standardního uživatele- kontrola přes PowerShell	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser	4,0	4,0= automaticky zamítnout
REG	Řízení uživatelských účtů: Povolit aplikacím UIAccess zobrazení výzvy ke zvýšení oprávnění bez použití zabezpečené plochy	EnableUIADesktopToggle	0	0= zakázáno
REG	Řízení uživatelských účtů: Při zobrazení výzvy ke zvýšení oprávnění přepnout na zabezpečenou plochu	PromptOnSecureDesktop	1	1= povoleno
REG	Řízení uživatelských účtů: Režim schválení správce pro integrovaný účet správce	FilterAdministratorToken	1	1= povoleno
REG	Řízení uživatelských účtů: Spustit všechny správce v Režimu schválení správce	EnableLUA	1	1= povoleno
REG	Řízení uživatelských účtů: Virtualizovat chyby zápisu do souboru a registru do umístění jednotlivých uživatelů	EnableVirtualization	1	1= povoleno
REG	Řízení uživatelských účtů: Zjistit instalace aplikací a zobrazit výzvu ke zvýšení oprávnění	EnableInstallerDetection	1	1= povoleno
REG	Řízení uživatelských účtů: Zvýšit oprávnění pouze u aplikací UIAccess, které jsou nainstalovány v zabezpečených umístěních	EnableSecureUIAPaths	1	1= povoleno
REG	Řízení uživatelských účtů: Zvýšit oprávnění pouze u podepsaných a ověřených spustitelných souborů	ValidateAdminCodeSignatures	0	0= zakázáno
REG	Účty: Blokovat účty Microsoft	NoConnectedUser	3	3= zakázáno
REG	Účty: Omezit použití prázdného hesla místního účtu pouze pro přihlášení ke konzole	LimitBlankPasswordUse	1	1= povoleno
REG	Vypnutí: Povolit vypnutí systému bez nutnosti přihlášení	ShutdownWithoutLogon	0	0= zakázáno
REG	Vypnutí: Vymazat stránkovací soubor virtuální paměti	ClearPageFileAtShutdown	0	0= zakázáno
REG	Zařízení: Zabránit uživatelům instalovat ovladače tiskáren	AddPrinterDrivers	1	1= povoleno

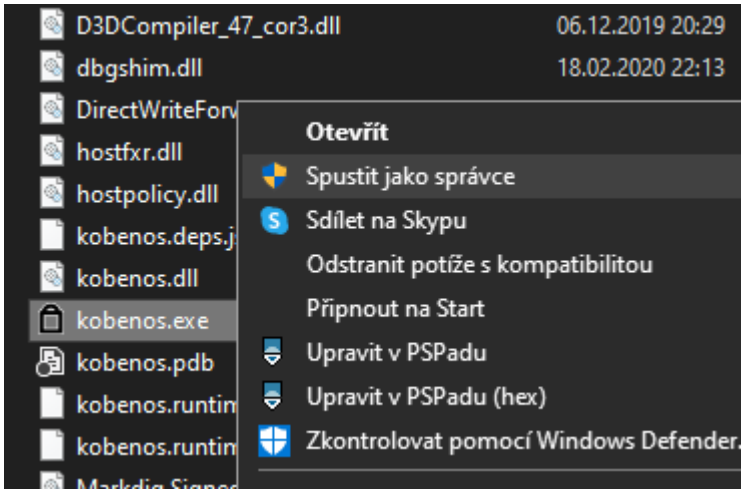
Tabulka 2:Nastavené hodnoty v konfiguračním souboru

Článek 19 - Služba protokolu událostí				
REG	Automaticky zálohovat protokol při naplnění- Aplikace	AutoBackupLogFiles	1	1 = povoleno
REG	Řídit chování služby Protokol událostí, když soubor protokolu dosáhne maximální velikosti- Aplikace	Retention	1	1 = povoleno
REG	Automaticky zálohovat protokol při naplnění- System	AutoBackupLogFiles	1	1 = povoleno
REG	Řídit chování služby Protokol událostí, když soubor protokolu dosáhne maximální velikosti- System	Retention	1	1 = povoleno
REG	Automaticky zálohovat protokol při naplnění- Zabezpečení	AutoBackupLogFiles	1	1 = povoleno
REG	Řídit chování služby Protokol událostí, když soubor protokolu dosáhne maximální velikosti- Zabezpečení	Retention	1	1 = povoleno
Článek 20 - Možnosti přihlášení k systému Windows				
REG	Zobrazit informace o předchozích přihlášeních během přihlášení uživatele	DisplayLastLogonInfo	0	0= zakázáno
REG	Automaticky přihlásit posledního interaktivního uživatele po restartování vyvolaném systémem	DisplayLastLogonInfo	0	0= zakázáno
Článek 21 - One Drive				
REG	Bránit používání OneDrivu jako úložiště souborů	DisableFileSyncNGSC	1	1= povoleno
Článek 22 - Zásady automatického přehrávání				
REG	Vypnout automatické přehrávání	NoDriveTypeAutoRun	181	181= povoleno
Článek 23 - Přihlášení				
REG	Zapnout přihlášení praktickým PIN kodem	AllowDomainPINLogon	0	0= zakázáno
REG	Vypnout přihlášení pomocí obrázkového hesla	BlockDomainPicturePassword	1	1= povoleno
REG	Vypnout oznámení aplikací na zamykací obrazovce	DisableLockScreenAppNotifications	1	1= povoleno
REG	Skrýt vstupní body pro Rychlé přepínání uživatele	HideFastUserSwitching	1	1= povoleno
REG	Vždy použít klasické přihlašování	LogonType	0	0= povoleno
Článek 24 - Zásady skupiny				
REG	Vypnout zpracování místních objektů Zásad skupiny	DisableLGPOProcessing	0	0= zakázáno
REG	Vypnout protokolování výsledné sady zásad	RSoPLogging	1	1= zakázáno
Článek 25 - Omezení instalace zařízení				
REG	Povolit správcům přepsat zásady Omezení pro instalaci zařízení	AllowAdminInstall	0	0= zakázáno
REG	Zobrazit vlastní zprávu v případě, že nastavení zásad znemožní instalaci	DetailText	Instalace nepovoleného zařízení	doporučené oznámení
REG	Zobrazit nadpis vlastní zprávy v případě, že nastavení zásad znemožní instalaci zařízení	SimpleText	Upozornění	doporučené oznámení
REG	Povolit instalaci zařízení s těmito identifikačními čísly zařízení	AllowDeviceIDs	0	0= zakázáno
REG	Zakázat instalaci vyměnitelných zařízení	DenyRemovableDevices	0	0= povoleno
REG	Zakázat instalaci zařízení nepopsaných v jiných nastaveních zásad	DenyUnspecified	0	0= povoleno
Článek 26 - Přístup k vyměnitelnému úložišti				
REG	Disk CD a DVD: Odepřít oprávnění ke spouštění	Deny_Execute	1	1= povoleno
REG	Disk CD a DVD: Odepřít přístup ke čtení	Deny_Read	0	0= zakázáno
REG	Disk CD a DVD: Odepřít přístup pro zápis	Deny_Write	0	0= zakázáno
REG	Disketové jednotky: Odepřít oprávnění ke spouštění	Deny_Execute	1	1= povoleno
REG	Disketové jednotky: Odepřít přístup ke čtení	Deny_Read	0	0= zakázáno
REG	Disketové jednotky: Odepřít přístup pro zápis	Deny_Write	0	0= zakázáno
REG	Vyměnitelné disky: Odepřít oprávnění ke spouštění	Deny_Execute	1	1= povoleno
REG	Vyměnitelné disky: Odepřít přístup ke čtení	Deny_Read	0	0= zakázáno
REG	Vyměnitelné disky: Odepřít přístup zápis	Deny_Write	0	0= zakázáno
REG	Všechny třídy vyměnitelného úložiště: Odepřít veškerý přístup	AllowRemoteDASD	0	0= zakázáno
REG	Páskové jednotky: Odepřít oprávnění ke spouštění	Deny_Execute	1	1= povoleno
REG	Páskové jednotky: Odepřít oprávnění ke čtení	Deny_Read	0	0= zakázáno
REG	Páskové jednotky: Odepřít oprávnění pro zápis	Deny_Write	0	0= zakázáno
REG	Zařízení WPD: Odepřít přístup ke čtení	Deny_Read	1	1= povoleno
REG	Zařízení WPD: Odepřít přístup pro zápis	Deny_Write	1	1= povoleno
Článek 27 - Obnovení				
REG	Povolit obnovení systému do výchozího stavu	DisableSetup	1	1= povoleno
Článek 28 - Obnovení systému				
REG	Vypnout konfiguraci	DisableConfig	1	1= povoleno
Článek 29 - Přizpůsobení				
REG	Nezobrazovat zamykací obrazovku	NoLockScreen	1	1= povoleno
REG	Bránit povolení kamery na zamykací obrazovce	NoLockScreenCamera	1	1= povoleno
REG	Bránit povolení prezentace na zamykací obrazovce	NoLockScreenSlideshow	1	1= povoleno
Článek 30 - Přizpůsobení				
REG	Povolit šetřič obrazovky	ScreenSaveActive	1	1= povoleno
REG	Zabránit změnám šetřiče obrazovky	NoDispScrSavPage	1	1= povoleno
REG	Chránit šetřič obrazovky heslem	ScreenSaverIsSecure	1	1= povoleno
REG	Časový limit šetřiče obrazovky	ScreenSaveTimeOut	900	900= doporučená hodnota v sekundách
REG	Vynutit konkrétní spořič obrazovky	SCRNSAVE.EXE		
Článek 31 - Průzkumník Windows				
REG	Nepřesouvat odstraněné soubory do koše	NoRecycleFiles	1	1= povoleno

Tabulka 3: Nastavené hodnoty v konfiguračním souboru

11.3 Spuštění programu

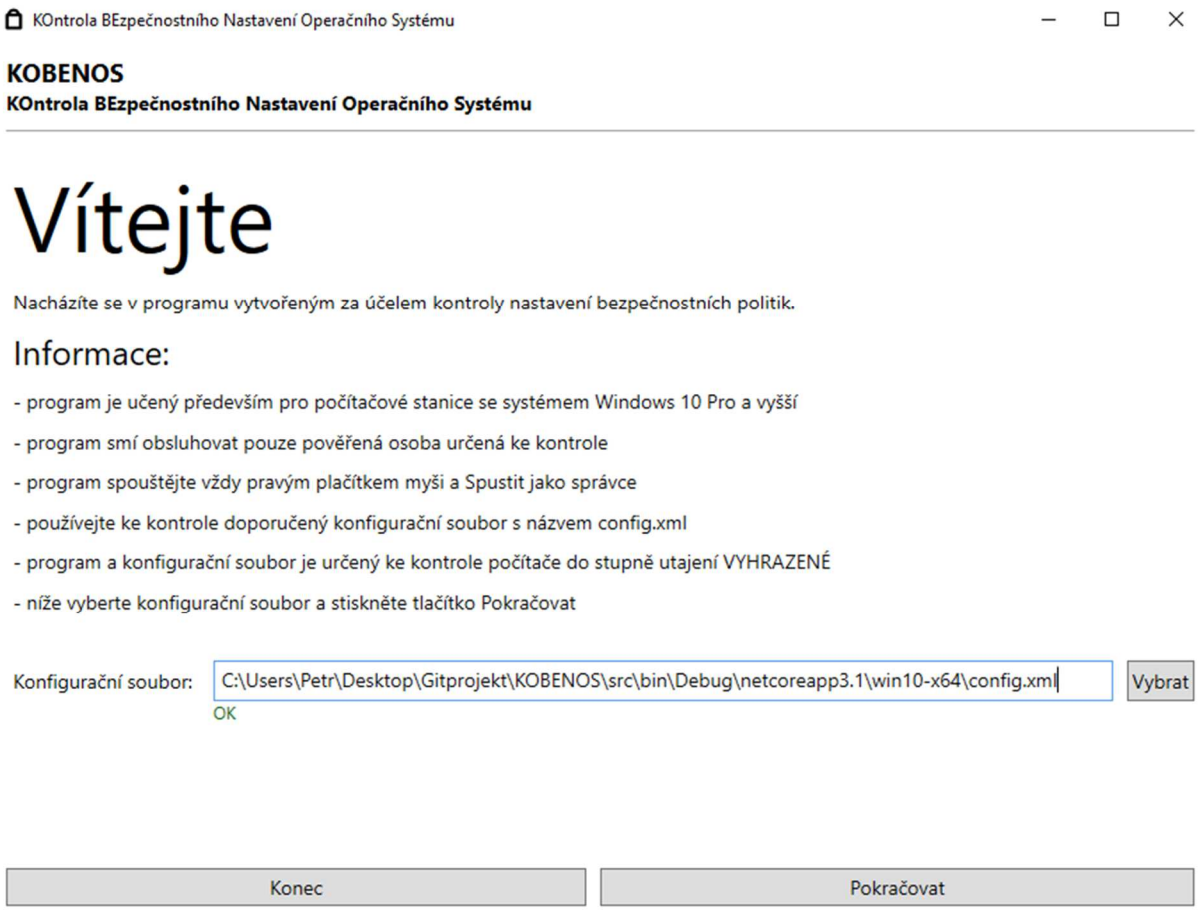
Program KOBENOS je nutné spustit v profilu s právy administrátora a jako správce. Program je nastavený tak, aby vždy vyžadoval spuštění jako správce. Pokud by se tak z neznámých důvodů nestalo, je potřeba ho spustit kliknutím pravým tlačítkem myši na ikonu kobenos.exe a spustit jako správce.



Obrázek 1: Spuštění jako správce

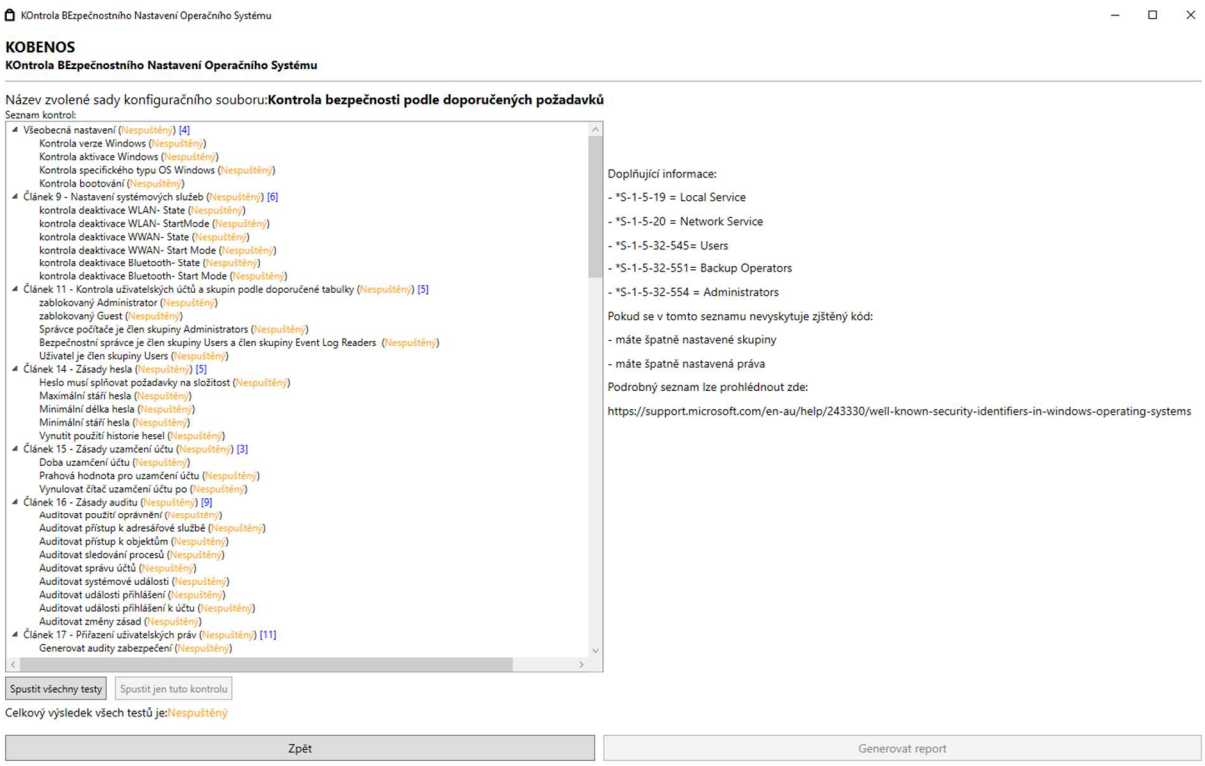
11.4 Obsluha programu

Po spuštění se zobrazí uvítací okno s několika informacemi pro uživatele programu, jak správně zacházet s programem. V uvítacím okně se kliknutím na tlačítko Vybrat zadává přístupová cesta ke konfiguračnímu souboru. Pokud uživatel zadá špatnou nebo neexistující cestu, program to pozná a upozorní ho na to. Program též kontroluje správnou strukturu konfiguračního souboru. Pokud je konfigurační soubor poškozen, ohlásí to.



Obrázek 2: Uvítací obrazovka

Obsluha musí vložit správný konfigurační soubor, aby bylo možné pokračovat na další stranu programu. Kliknutím na tlačítko Pokračovat se načte konfigurační soubor a přejde se na další obrazovku. Po načtení konfiguračního souboru se zobrazí okno s načtenými testy.



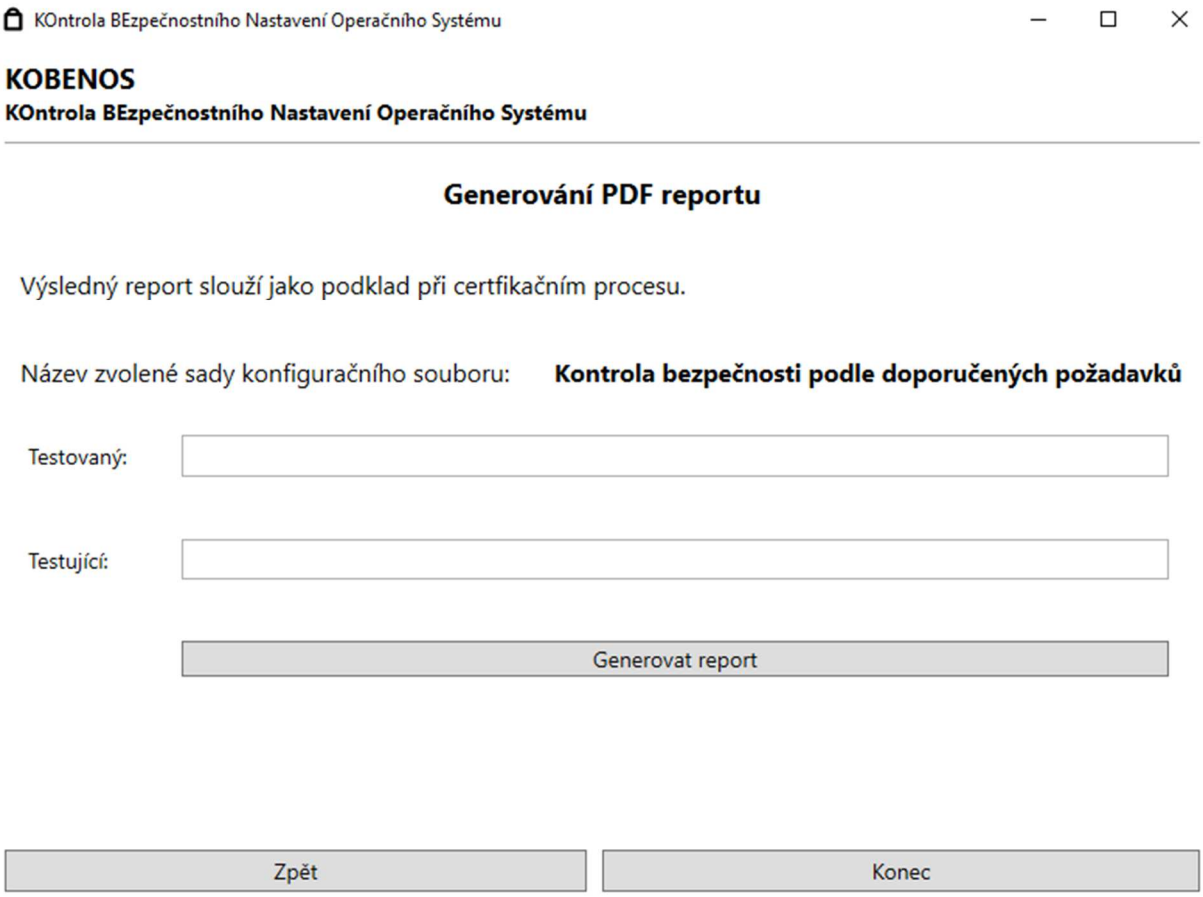
Obrázek 3: Výpis testů

Obsluha programu může pomocí tlačítka Spustit všechny testy spustit testování všech testů nebo může kliknutím na jednotlivé kategorie či konkrétní testy spustit jen tyto vybrané testy.

Program u jednotlivých testů vypisuje jejich aktuální situaci. U testů mohou nastat tři situace. Buď test, nebo testy nejsou spuštěné, nebo vyhověly, nebo nevyhověly.

Výsledky jednotlivých testů lze po kliknutí na název testu vidět v pravé části okna.
Pokud test nebyl spuštěn, zobrazí se Nespuštěno. Pokud test proběhl v pořádku, objeví se u něj OK. Pokud test proběhl a byly v něm nalezeny chyby, zobrazí se u něj popis problému a stav, že nevyhověl. Po spuštění všech testů lze vidět jejich celkové vyhodnocení ve spodní části programu a povolí se tlačítko Generovat report.

Tímto tlačítkem se dostaneme na obrazovku, kde lze generovat report do PDF. Tam je nutné zadat název testovaného subjektu, firmy, organizace nebo konkrétního zařízení.
Je zde nutné přidat i jméno osoby, která prováděla kontrolu.
Výsledný report bude jako PDF soubor vyexportován do požadovaného adresáře.



Obrázek 4: Generování PDF

12 Závěrečné zhodnocení výsledků

12.1 Vyhodnocení požadavků

Podařilo se mi popsat požadované operační systémy z pohledu bezpečnosti. Nejprve jsem nastínil legislativní důvody, proč je nutné zabezpečovat komunikační zařízení. Poté jsem vybrané systémy popsal. Následně jsem popsal typy vhodné k jejich zabezpečení. V jednotlivých kapitolách jsem jednoduše popsal možná bezpečnostní rizika a jejich prevenci. Následně jsem sestavil seznam doporučených požadavků podle legislativního rámce. Nakonec jsem vytvořil program, který kontroluje zabezpečení off-line stanic, jež nejsou v doméně, zpracovávajících utajované informace podle zákona 412/2005.

Z celkových 123 doporučených testů z kapitoly *5.6* se mi nepodařilo splnit 5.

1. Prahová hodnota pro uzamčení účtu – nenalezl jsem v systému cestu, která by umožnila její kontrolu. Našel jsem pouze doporučení [16], kde by se měla tato vlastnost nacházet. Bohužel na žádném z 10 kontrolovaných zařízení tato cesta nevedla k požadované hodnotě.

2. Povolit spořič obrazovky – obdobný problém jako u bodu 1.

3. Chránit spořič obrazovky heslem – obdobný problém jako u bodu 1.

4. Časový limit šetřiče obrazovky – obdobný problém jako u bodu 1.

5. Vynutit konkrétní spořič obrazovky – obdobný problém jako u bodu 1.

12.2 Vyhodnocení vzniklé aplikace

Program KOBENOS je podle mnou dostupných informací jediný program v České republice, který dokáže překontrolovat takto specifická bezpečnostní nastavení. Celkově aplikace splnila mé očekávání. Nebylo náročné ji vytvořit, problém však představovalo vyhledávání požadovaných bezpečnostních nastavení v systému. Bohužel ani výrobce operačního systému, na který je moje aplikace vytvořená, tyto informace nikde veřejně neuvádí ani nepopisuje – nepodařilo se mi dohledat, jak je třeba přistupovat například v registrech k požadovaným hodnotám. Aplikace využívá nejednotný systém kontrol, konkrétně se jedná o kombinaci WMI, registry a PowerShell. Původně jsem ji zamýšlel vytvořit jako 32-bitovou, bohužel vlastnosti registrů ve Windows 10 mi v tom zabránily.

12.3 Vyhodnocení implementace

Pokud vezmu v úvahu, že moje předchozí znalosti se C#, .NET Core a dalšími použitými technologiemi byly naprosto nulové, beru tento program za velmi zdařilý. Při vytváření programu jsem nejprve doufal ve využití pouze jedné technologie, bohužel postupem času jsem musel přidat i další. Určitě by bylo možné vytvořit tuto aplikaci jednotnější. Jak jsem již zmínil, nepodařilo se mi najít potřebnou dokumentaci, aby se mi to podařilo.

12.4 Aplikovatelnost

Program je primárně určen pro kontrolu specifických bezpečnostních nastavení na operačním systému Windows 10 64-bit Pro a vyšší. Jeho využitelnost je především v certifikačním oddělení NÚKIB. Pokud by bylo potřeba, jeho konfigurační soubor lze podle konkrétních požadavků jednoduše pozměnit.

12.5 Testování

Testování probíhalo ve spolupráci s pracovníky certifikačního oddělení. Byl vybrán starší notebook a na něj se nainstaloval čistý 64-bitový operační systém Windows 10 Enterprise (verze 1809, build 17763.503). Na tomto notebooku byly nastaveny veškeré bezpečnostní politiky. Poté se na tomto notebooku spustily testy z programu KOBENOS. Během testování jsem zjistil, že informace přímo od Microsoftu nejsou vždy pravdivé nebo aktuální [15; 17–19]. Musel jsem tedy vycházet z hodnot, jež mi po správném nastavení systém vrátil. Tyto opravené hodnoty jsem změnil v konfiguračním souboru a aplikoval program na již certifikovaný počítač. Naštěstí na tomto počítači proběhly testy dle předpokladu.

12.6 Závěrečné zhodnocení

Při vytváření seznamu bezpečnostních doporučení jsem si ujasnil jejich potřebnost nejen na specializovaných systémech, ale i při běžném používání. Je dobré vždy problémům předcházet než pak litovat. Seznam požadavků vychází ze zkušeností. Bohužel neexistuje jednotný seznam alespoň minimálních požadavků nařizujících jejich aplikovatelnost na potřebném systému. V současné době existuje pouze seznam doporučení. Je tedy vždy jen na bezpečnostním správci, jak a které nastavení uzná za vhodné použít.

Program by určitě uvítal revizi kódu. Moje znalosti programování vycházejí především z jazyka Java, možná jsem tedy nevhodně použil některé funkce. Ale funkčnost programu to neohrozilo.

12.7 Některá možná vylepšení

Jedním z možných vylepšení je vytvoření střediska správy, kde by se dal jednoduše konfigurovat konfigurační soubor. Středisko by vytvořilo jedinečný konfigurační soubor, který by nebylo možné měnit ani klasicky otevřít. Tento soubor by KOBENOS načetl a překontroloval by systém. Výsledný PDF report by obsahoval speciální značku, například hash, již by pracovník certifikačního oddělení mohl překontrolovat s hashem viditelným ve středisku správy. Tím by bylo zajištěno, že

konfigurační soubor nepodlehl nějaké změně a výslednému reportu může pracovník certifikačního oddělení věřit.

13 Rešerše literatury

Pro zpracování této práce jsem využil odborné literatury z oblasti bezpečnosti a informačních technologií. Jednalo se především o zákon č. 412/2005 Sb., zákon č. 181/2014 Sb. a právní předpisy a normy s tím související. Potřebné informace byly vyhledávány na internetu, v tištěné podobě, ale i prostřednictvím osobních konzultací s odborníky z daného oboru.

14 Zdroje literatury

[1] ŘÍHA, Josef. KRITICKÁ INFRASTRUKTURA A RIZIKO MIMOŘÁDNÉ UDÁLOSTI. [online]. [vid. 2020-08-09]. Dostupné z: https://www.uur.cz/images/5-publikacni-cinnost-a-knihovna/casopis/2007/2007-04/08_kriticka.pdf

[2] Povinné osoby. *GOVCERT* [online]. [vid. 2020-04-27]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/povinne-osoby/#od3

[3] *GovCERT.CZ* [online]. [vid. 2020-04-27]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/

[4] INFO@AION.CZ, AION CS-. 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi* [online]. [vid. 2020-04-27]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181?text=informa%C4%8Dn%C3%AD+bezpe%C4%8Dnost

[5] INFO@AION.CZ, AION CS-. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. *Zákony pro lidi* [online]. [vid. 2020-04-27]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412?text=

[6] ČERMÁK, Miroslav. Analýza rizik: Jemný úvod do analýzy rizik. *CleverAndSmart Management Consulting* [online]. 20. květen 2010 [vid. 2020-04-27]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[7] How does Android save your fingerprints? *Android Central* [online]. 26. září 2017 [vid. 2020-04-27]. Dostupné z: https://www.androidcentral.com/how-does-android-save-your-fingerprints

[8] About Touch ID advanced security technology. *Apple Support* [online]. [vid. 2020-04-27]. Dostupné z: https://support.apple.com/en-us/HT204587

[9] Enterprise Mobility Management (EMM). *System4u* [online]. [vid. 2020-05-01]. Dostupné z: https://www.system4u.cz/slovnicek-pojmu/enterprise-mobility-management-emm/

[10] Bring Your Own Device (BYOD). *System4u* [online]. [vid. 2020-05-01]. Dostupné z: https://www.system4u.cz/slovnicek-pojmu/bring-your-own-device-byod/

[11] TECHNION-ISRAEL INSTITUTE OF TECHNOLOGY. *Researchers discover „severe" bluetooth communication breach* [online]. [vid. 2020-04-27]. Dostupné z: https://phys.org/news/2018-07-technion-severe-bluetooth-breach.html

[12] BIHAM, Eli a Lior NEUMANN. *Breaking the Bluetooth Pairing – The Fixed Coordinate Invalid Curve Attack* [online]. 1043. 2019 [vid. 2020-04-27]. Dostupné z: http://eprint.iacr.org/2019/1043

[13] FRANCIS, Lishoy, Gerhard HANCKE, Keith MAYES a Konstantinos MARKANTONAKIS. *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones* [online]. 618. 2011 [vid. 2020-04-27]. Dostupné z: http://eprint.iacr.org/2011/618

[14] Download WMI Explorer. *BleepingComputer* [online]. [vid. 2020-05-09]. Dostupné z: https://www.bleepingcomputer.com/download/wmi-explorer/

[15] *Well-known security identifiers in Windows operating systems* [online]. [vid. 2020-05-09]. Dostupné z: https://support.microsoft.com/en-au/help/243330/well-known-security-identifiers-in-windows-operating-systems

[16] The machine account lockout threshold must be set to 10 on systems with BitLocker enabled. *STIG Viewer | Unified Compliance Framework®* [online]. [vid. 2020-05-14]. Dostupné z: https://www.stigviewer.com/stig/windows_8/2013-10-01/finding/V-36772

[17] DANIHALFIN. *Identity and access management (Windows 10)* [online]. [vid. 2020-05-17]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/identity-protection/

[18] MCLEANBYRON. *Build desktop Windows apps using the Win32 API - Win32 apps* [online]. [vid. 2020-05-17]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/

[19] HONGGIT. *Diagnostika prostřednictvím rozhraní WMI (Windows Management Instrumentation) - WCF* [online]. [vid. 2020-05-17]. Dostupné z: https://docs.microsoft.com/cs-cz/dotnet/framework/wcf/diagnostics/wmi/

15 Přílohy

prilohy.zip- obsahuje :

- zdrojové kódy programu
- flowchart programu
- hodnoty nastavené v konfiguračním souboru- hodnoty_config.xlsx

16 Seznam zkratek

Zkratka	Význam
AČR	Armáda české republiky
ALE	Evaluation Assurance Level
ASR	Attack Surface Reduction
BIS	Bezpečnostní informační služba
BT	bluetooth
BYOD	Bring Your Own Device
CD	compact disk
CIS	Centralizovaný informační systém
DVD	Digital Versatile Disc
ECDH	Elliptic curve Diffie Hellman
EMM	Enterprise Mobility Management
EU	Evropská unie
FBI	Federal Bureau of Investigation
GOVCERT	Vládní CERT
HW	hardware
IS	informační systém
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
KV	kompromitující vyzařování
LAN	Local area network
LSA	Local Security Authority
MDM	Mobile device managament
MO	Ministerstvo obrany
NATO	Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NFC	Near field communication
NT	New tehnology
NTFS	New Technology File Systém
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OCIKS	Oddělení certifikací informačních a komunikačních systémů
OCKPP	Oddělení certifikace kryptografických prostředků a pracovišť
OKVKP	Oddělení kryptologie a vývoje kryptografických prostředků
OS	operační systém
OŠS	Oddělení šifrové služby
PIN	personal identification number
RA	riziková analýza
STK	Stanice technické kontroly
SW	software
ŠIS	Štábní infomační systém
TEE	Trusted Execution Environmenta

Zkratka	Význam
TPM	Trusted Platform Module
UI	utajované informace
USB	Universal Serial Bus
VBS	Virtual Based Security
VIS	Významné informační systémy
VPN	virtual private network
VZ	Vojenské zpravodajství
WMI	Windows Management Instrumental
WPF	Windows Presentation Foundation
WQL	Windows Management Instrumental Query Language
ZKB	zákon o kybernetické bezpečnosti

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Mareš** Jméno: **Petr** Osobní číslo: **425930**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra počítačů**

Studijní program: **Softwarové inženýrství a technologie**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Zabezpečení operačních systémů v informačních systémech pracujících s utajovanými informacemi

Název bakalářské práce anglicky:

Security of information systems processing and storing classified information

Pokyny pro vypracování:

Stručně a přehledně popište v praxi nejpoužívanější operační systémy (iOS, Android, Windows, Linux) z pohledu uživatele, administrátora a útočníka. V práci se zaměřte analýzu rizik, možnosti zabezpečení desktop zařízení, možnosti zabezpečení mobilních zařízení (MDM,EMM.), problematiku el.mag. vyzařování, evidence přístupů a auditování. Navrhněte opatření pro zabezpečení operačních systémů nutná pro splnění požadavků vyplývajících ze Zákona o ochraně utajovaných informací (412/2005) a Zákona o kybernetické bezpečnosti (181/2014). V rámci bakalářské práce navrhněte a zrealizujte pro operační systém Microsoft Windows 10 program, který umožní automatický sběr a vyhodnocení informací o konkrétním zabezpečení off-line stanice (a jejím souladu s požadavky zákona 412/2005 resp. 181/2014) a automatické nastavení bezpečnostních politik v souladu se zvoleným bezpečnostním profilem.

Seznam doporučené literatury:

Zákon č. 181/2014 Sb.
Zákon č. 412/2005 Sb.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

Ing. Tomáš Vaněk, Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **14.02.2020** Termín odevzdání bakalářské práce: **14.08.2020**

Platnost zadání bakalářské práce: **30.09.2021**

Ing. Tomáš Vaněk, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Mgr. Petr Páta, Ph.D. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student bere na vědomí, že je povinen vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

. | Datum převzetí zadání

Podpis studenta