Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Možnosti zabezpečení operačních systémů moderních mobilních zařízení

Vojtěch Šmahel

Bakalářská práce
2023

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Vojtěch Šmahel**
Osobní číslo:	**E19294**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Možnosti zabezpečení operačních systémů moderních mobilních zařízení**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je identifikovat a charakterizovat možnosti zabezpečení operačních systémů využívaných v moderních mobilních zařízeních a vypracovat soubor pravidel a doporučení pro zvýšení zabezpečení při práci s těmito zařízeními.

Osnova:

- Prostudování a vytvoření přehledu o operačních systémech pro mobilní zařízení.
- Identifikace faktorů ovlivňující bezpečnost při používání zařízení s konkrétním systémem.
- Vypracování souboru pravidel a doporučení dle cíle práce.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

ELENKOV, Nikolay. *Android Security Internals: An In-Depth Guide to Android's Security Architecture.* San Francisco: No Strach Press, 2014. ISBN 9781593275815.
FRIED, Stephen. *Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World.* United Kingdon: Taylor and Francis Inc, 2010. ISBN 9781439820162.
KRÁL, Mojmír. *Bezpečný internet: Chraňte sebe i svůj počítač.* Praha: Grada, 2015. ISBN 9788024754536.
LACKO, Ľuboslav : *Mistrovství-Android: Kompletní průvodce vývojáře.* Brno: Computer Press, 2017. ISBN 9788025148754.
MAISNER, Martin. *Základy softwarového práva.* Praha: Wolters Kluwer Česká republika, 2011. ISBN 9788073579647.
THIEL, David. *iOS Application Security.* San Francisco: No Strach Press, 2016. ISBN 9781593276010.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2022**
Termín odevzdání bakalářské práce: **30. dubna 2023**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2022

PROHLÁŠENÍ

Prohlašuji:

Práci s názvem „Možnosti zabezpečení operačních systémů moderních mobilních zařízení“ jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7 /2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne

30.04.2023

Vojtěch Šmahel v. r.

PODĚKOVÁNÍ:

Tímto bych velmi rád poděkoval svému vedoucímu RNDr. Ing. Oldřichu Horákovi, Ph.D za jeho odborné rady a pomoc, které mi pomohly při zpracování této bakalářské práce.

ANOTACE

Tato bakalářská práce se zabývá možnostmi zabezpečení moderních mobilních zařízení. Úvodní kapitola seznamuje se základními bezpečnostními pojmy. Následující kapitola představuje stručný vývoj mobilních zařízení v posledních letech. V další části jsou představeny tato zařízení z pohledu operačních systémů a hlavní důraz je kladen především na nejpoužívanější systémy iOS a Android a dále je zmíněn i také systém Windows. V následující kapitole jsou představeny a popsány nejčastější hrozby a rizika dnešní doby. Následuje seznam doporučených zabezpečení pro konkrétní skupiny uživatelů. Pro potřeby této práce byli rozděleni tito uživatelé do kategorie dítě, běžný uživatel, firemní uživatel a VIP uživatel. V závěru práce je samostatná kapitola na aplikace třetích stran pro zvýšení bezpečnosti zařízení a práce se zařízeními na internetu.

KLÍČOVÁ SLOVA

Mobilní zařízení, Bezpečnost, Android, iOS, Windows

TITLE

Security options for operating systems of modern mobile devices

ANNOTATION

This bachelor's thesis deals with the security possibilities of modern mobile devices. The introductory chapter introduces basic security terms. The following chapter presents a brief development of mobile devices in recent years. In the next part, these devices are presented from the point of view of operating systems, and the main emphasis is mainly on the most used iOS and Android systems, and the Windows system is also mentioned. In the following chapter, the most common threats and risks of today are presented and described. maintains a list of recommended security for specific user groups. For work purposes, these users were divided into the categories child, regular user, company user and VIP user. At the end of the work, there is a separate chapter on the application of the third fear to increase the security of devices and work with devices on the Internet.

KEYWORDS

Mobile device, Security, Android, iOs, Windows

OBSAH

ÚVOD ..... - 12 -

1 TEORIE BEZPEČNOSTI A BEZPEČNOST INFORMACÍ ..... - 13 -

1.1 BEZPEČNOST ..... - 13 -
1.2 INFORMAČNÍ BEZPEČNOST ..... - 13 -
1.2.1 Bezpečnostní funkce ..... - 13 -
1.2.2 Bezpečnostní mechanismy ..... - 14 -
1.2.3 Význam řízení přístupu k informacím ..... - 15 -

2 VÝVOJ MOBILNÍCH ZAŘÍZENÍ A JEJICH ZABEZPEČENÍ ..... - 18 -

2.1 VÝVOJ ZAŘÍZENÍ NA SYTÉMU IOS ..... - 18 -
2.2 VÝVOJ TELEFONŮ NA SYSTÉMU ANDROID ..... - 23 -
2.2.1 Historie a současnost telefonů Android ..... - 23 -
2.2.2 Problém čínských výrobců ..... - 26 -
2.3 VÝVOJ TELEFONŮ WINDOWS PHONE ..... - 27 -

3 OPERAČNÍ SYSTÉMY MODERNÍCH MOBILNÍCH ZAŘÍZENÍ A JEJICH ZABEZPEČENÍ ..... - 28 -

3.1 IOS ..... - 28 -
3.2 ANDROID ..... - 29 -
3.3 WINDOWS ..... - 31 -
3.4 ZÁKLADNÍ ROZDÍLY MEZI IOS A ANDROID ..... - 32 -

4 ZABEZPEČENÍ AKTUÁLNÍCH ZAŘÍZENÍ ..... - 34 -

4.1 NUTNOST ZABEZPEČENÍ ..... - 34 -
4.2 HROZBY DNEŠNÍ DOBY ..... - 34 -
4.2.1 Malware ..... - 34 -
4.2.2 Phishing ..... - 36 -
4.2.3 Neoprávněný přístup k datům ..... - 36 -
4.2.4 Nedostatečná aktualizace software ..... - 36 -
4.2.5 Používání veřejných WI-FI sítí ..... - 37 -
4.2.6 Sociální inženýrství ..... - 37 -
4.2.7 Zálohování dat do cloudu ..... - 37 -
4.2.8 Nedostatečné šifrování dat ..... - 38 -

5 BEZPEČNOSTNÍ STANDARDY A DOPORUČENÍ ..... - 39 -

5.1 ZABEZPEČENÍ „PRO DÍTĚ“ ..... - 39 -
5.1.1 Definování uživatele ..... - 39 -
5.1.2 Rizika ..... - 39 -
5.1.3 Doporučená zabezpečení ..... - 40 -
5.2 ZABEZPEČENÍ BĚŽNÉHO UŽIVATELE ..... - 40 -
5.2.1 Definování uživatele ..... - 41 -
5.2.2 Rizika ..... - 41 -
5.2.3 Doporučená zabezpečení ..... - 41 -
5.3 ZABEZPEČENÍ PRO FIREMNÍHO UŽIVATELE ..... - 42 -
5.3.1 Definování uživatele ..... - 42 -
5.3.2 Rizika ..... - 42 -
5.3.3 Doporučená zabezpečení ..... - 43 -
5.4 ZABEZPEČENÍ SYSTÉMU VIP ..... - 44 -
5.4.1 Definování uživatele ..... - 44 -
5.4.2 Rizika ..... - 44 -
5.4.3 Doporučená zabezpečení ..... - 45 -

6 NÁSTROJE PRO ZVÝŠENÍ BEZPEČNOSTI ..... - 47 -

6.1 BEZPEČNOSTNÍ APLIKACE ..... - 47 -
6.2 APLIKACE PRO IOS ..... - 47 -

6.2.1 Aplikace pro iOS zdarma ..... - 47 -
6.2.2 Aplikace pro iOS placená ..... - 47 -
6.3 APLIKACE PRO ANDROID ..... - 48 -
6.3.1 Aplikace pro Android zdarma ..... - 48 -
6.3.2 Aplikace pro Android placená ..... - 48 -
6.4 APLIKACE PRO WINDOWS ..... - 48 -
6.4.1 Aplikace pro Windows zdarma ..... - 49 -
6.4.2 Aplikace pro Windows placená ..... - 49 -
ZÁVĚR ..... - 50 -
POUŽITÁ LITERATURA ..... - 52 -
PŘÍLOHY ..... - 56 -

SEZNAM ILUSTRACÍ

Obrázek 1 Model CIA ..... - 14 -
Obrázek 2 Možné rozhodovací situace..... - 17 -
Obrázek 3 iPhone 1 . generace ..... - 19 -
Obrázek 4 Poslední představený model iPhone - 14 Pro Max ..... - 23 -
Obrázek 5 HTC Dream - první mobilní telefon se systémem Android..... - 24 -
Obrázek 6 Samsung Galaxy Z Fold 4 - jeden ze symbolů dnešních Android telefonů..... - 26 -

SEZNAM ZKRATEK A ZNAČEK

3G	Třetí generace mobilních telekomunikačních technologií
DDoS	Distributed denial-of-service (typ útoku na internetovou službu)
DNS	Domain Name System (systém doménových jmen)
eSIM	Virtuální karta SIM
EUFI	Unified Extensible Firmware Interface (softwarové rozhraní mezi operačním systémem a firmwarem)
GB	Gigabajt (jednotka množství informace)
GDPR	General Data Protection Regulation (obecné nařízení o ochraně osobních údajů)
GPS	Global Positioning System (globální polohovací systém umožňují určit polohu zařízení)
GSM	Groupé Spécial Mobile (nejrozšířenější celosvětový standard pro digitální mobilní sítě)
HTTPS	Hypertext Transfer Protocol Secure (protokol zabezpečující bezpečnou komunikaci)
ID	Identifikace
IT	Informační technologie
Keynote	Název události pro představení nových produktů společnosti Apple
LED	Light Emitting Diode (dioda vyzařující světlo)
MB	Megabajt (jednotka množství informace)
MMS	Multimedia Messaging Service (služba multimediálních zpráv, služba dostupná většině moderních mobilních telefonů)
MP3	Ztrátový formát kódování audia
NFC	Near Field Communication (technologie umožňující bezdrátově přenášet data na velmi krátkou vzdálenost)
NÚKIB	Národní ústav pro kybernetickou bezpečnost
OLED	Organic Light Emitting Diode (dioda s organickým prvkem vyzařující světlo)
PC	Personal Computer (osobní počítač)

PIN	Personal Identification Number (osobní identifikační číslo)
SIM	Subscriber Identity Module (účastnická identifikační karta, sloužící k identifikaci účastníka v rámci mobilní sítě)
SMS	Short Message Service (služba krátkých zpráv, služba dostupná většině moderních mobilních telefonů)
TB	Terabajt (jednotka množství informace)
TV	Televize
UAC	User Account Control (řízení uživatelských účtů)
UI	User Interface (uživatelské rozhraní)
USB	Universal Serial Bus (univerzální sériová sběrnice)
VIP	Very Important Person (velmi významná osoba)
VPN	Virtual Private Networtk (virtuální privátní síť)
WAP	Wireless Aplication Protocol (sada protokolů umožňující přístup na internet historicky starším telefonům)
WI-FI	Wireless Fidelity (bezdrátové síťové připojení)

ÚVOD

Pokud o nějakém faktoru v rámci informačních technologií můžeme říci, že je naprosto klíčový, pak je to faktor bezpečnosti.

V dnešní době jsou mobilní zařízení běžnou součástí našeho každodenního jak soukromého, tak i pracovního života. Staly se nezbytným nástrojem pro práci, komunikaci, zábavu a mnoho dalších aktivit. S nárůstem hardwarového výkonu a neustálého vyvíjení aplikací se využívání mobilních zařízení stalo plnohodnotným nástupcem a alternativou tradičního způsobu (myšleno prací na stolních počítačích a noteboocích).

Citlivost dat, se kterými se na moderních mobilních zařízeních pracuje, se také velmi zvýšila, a proto je naprosto nezbytné tato zařízení patřičně chránit.

Moderní mobilní zařízení jsou vystavena různým hrozbám, jako jsou například útoky hackerských skupin, krádeže dat nebo škodlivý software. Proto je důležité zajistit, aby byla mobilní zařízení chráněna dostatečně, aby uživatelé byli obeznámeni s nejnovějšími zabezpečovacími opatřeními a zároveň, aby tito uživatelé dokázali tyto hrozby identifikovat a předcházet potenciálním problémům svojí činností.

Jednou z motivací k volbě tématu této práce byly moje dlouholeté profesionální zkušenosti v oblasti IT a její bezpečnosti.

Cílem práce je identifikovat a charakterizovat možnosti zabezpečení operačních systémů využívaných v moderních mobilních zařízeních a vypracovat soubor pravidel a doporučení pro zvýšení zabezpečení při práci s těmito zařízeními.

1 TEORIE BEZPEČNOSTI A BEZPEČNOST INFORMACÍ

V úvodní kapitole se zaměříme na teorii bezpečnosti. Budou vysvětleny základní pojmy týkající se bezpečnosti a pojmy, se kterými se lze setkat, jak při studiu informačních a bezpečnostních systémů, tak jsou standardně využívány v rámci business sféry.

1.1 Bezpečnost

Pod pojmem bezpečnost můžeme chápat ucelenou ochranu systému před hrozbami. V této obecné rovině pod pojmem systém nechápeme pouze systém informační, nebo počítačový, ale i systémy ze společenského, technického, či přírodního života. Tak jako v každé jiné oblasti je nutné neustále zvyšovat bezpečností standardy a eliminovat potenciální hrozby. Na druhou stranu je v rámci těchto standardů nutné brát v potaz i protichůdné faktory, že zvyšující se bezpečností opatření a standardy jdou ruku v ruce s nějakým omezením pro účastníky daného systému.

1.2 Informační bezpečnost

Informační bezpečnost zahrnuje ochranu všech informací bez rozdílu umístění těchto informací na nosičích po celý jejich životní cyklus. Ochrana těchto informací je úzce spjatá s jejich šifrováním. Informace jsou pro mnoho organizací jejich nejdůležitějším aktivem, proto je jejich bezpečnost naprosto klíčová. V rámci těchto požadavků je nutné zajistit důvěrnost těchto dat, dostupnost a obsahovou neporušitelnost (integritu).

Informační systémy na bázi informačních technologií se skládají :

Hardware- fyzické vybavení informačního systému (procesor, paměti..)

Software- operační systémy, aplikační programy..

Data- data uložená v databázi, výstupní sestavy, výsledky..

Lidé- uživatelé, personál..

[1]

1.2.1 Bezpečnostní funkce

Jak již bylo zmíněno v úvodu této kapitoly, základními požadavky (bezpečnostními funkcemi) na bezpečné informace je jejich důvěrnost, dostupnost a integrita.

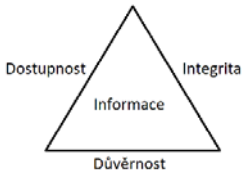
Důvěrnost informací je požadavek, aby dané informace byly dostupné pouze oprávněným uživatelům.

Dostupnost informací je požadavek, aby dané informace byly dostupné v okamžiku jejich potřeby.

Integrita informací je požadavek, aby dané informace byly celistvé, komplexní a správné.

V různých literárních zdrojích se můžeme setkat také s takzvaným trojúhelníkovým modelem CIA, kde jednotlivé písmeno znamená anglické slovo (Confidentality- důvěrnost, Integrity- integrita, Availability- dostupnost).

[2][4]



Obrázek 1 Model CIA

Zdroj: vlastní zpracování

1.2.2 Bezpečnostní mechanismy

Ochranu těchto dat můžeme rozlišit taktéž dle jednotlivých mechanismů, které jsou pro ochranu využívány. Tyto mechanismy se využívají především proto, aby byly splněny bezpečnostní funkce.

V reálném světě rozlišujeme standardně tyto bezpečnostní mechanismy.

Bezpečnostní mechanismy fyzického charakteru:

Jak již vypovídá název, jedná se o různé fyzické překážky (například trezory a zámky). Dále do této kategorie můžeme zařadit i samotné prostory- pro lepší představu například serverovou místnost, kde je nutné zajistit odpovídající protipožární ochranu, záložní generátory energie, odvádění tepla aj.

Bezpečnostní mechanismy logického charakteru:

Mezi bezpečnostní mechanismy logického charakteru lze zařadit velké množství softwarových aktivit. Jedná se například o softwarové řízení přístupu, používání kryptografie, využívání digitálních podpisů, zřizování uživatelských účtů, antivirové programy aj.

Bezpečnostní mechanismy technického charakteru:

Mechanismus je někdy nazývám taktéž jako hardwarový. Lze sem zařadit archivační pásky, firewally, autentizační systémy založeny na bázi identifikačních karet nebo autentizační kalkulátory.

Bezpečnostní mechanismy administrativního charakteru:

Jedná se například o proškolení uživatelů, bezpečností pravidla pro hesla, autorizační postupy, příjímací a výpovědní postupy, zákony, vyhlášky, předpisy apod.

Dle jiného rozdělení lze bezpečnostní mechanismy také rozdělit na slabé bezpečnostní mechanismy, bezpečnostní mechanismy střední síly a silné bezpečnostní mechanismy.

[3][5]

1.2.3 Význam řízení přístupu k informacím

Jedná se o pravděpodobně nejvýznamnější bezpečnostní mechanismus, pomocí kterého definujeme vztah mezi objekty a subjekty daného informačního systému. Objektem v tomto směru chápeme prvek systému, který obsahuje, nebo přijímá informace. Subjektem pak chápeme takový prvek systému, který předává informace mezi objekty, nebo způsobuje změnu stavu systému.

Identifikace:

Pojem identifikace je první z kroků v řízeném přístupu k informacím. Pod pojmem identifikace si můžeme zjednodušeně představit tvrzení subjektu o své identitě. Touto identitou nemusí být pouze totožnost, ale i jiná vlastnost, schopnost, či skupinová příslušnost.

Autentizace:

Druhý krok v rámci řízeného přístupu k informacím je autentizace. Autentizace je proces ověření identity subjektu tak, že splňuje jistou míru záruky.

Znalostní autentizace:

Znalostní autentifikace, jak již název vypovídá, vyžaduje určitou znalost subjektu. Touto znalostí by měl disponovat pouze daný konkrétní subjekt.

Nejtypičtějším představitelem znalostní autentifikace je heslo. Hesla jsou využívána napříč všemi službami, ke kterým je nutné se přihlašovat. V případě moderních mobilních zařízení se jedná například o odemčení systému, přístupu do emailové schránky, nebo k přístupu na internetové bankovnictví. Hesla jsou také nejtypičtějším způsobem autentizace při přihlašování

do WI-Fi sítí. Největší výhodu v implementaci autentizace přes hesla lze spatřovat v její jednoduchosti a nízkých pořizovacích nákladech.

Autentizace přes hesla je navíc uživatelsky přívětivá. Nikoliv v tom smyslu, že by zadání hesla bylo jednoduchou a nejsnadnější metodou, ale v tom smyslu, že uživatelé jsou na tento způsob autentizace zvyklí.

Autentizace prostřednictvím autentizačního předmětu:

Dalším způsob autentizace je prostřednictvím autentizačního předmětu. Tento způsob spočívá ve vlastnictví jedinečného předmětu, který by měl vlastnit pouze ten daný konkrétní subjekt a nikdo jiný. Tyto předměty nejsou tak často využívány, neboť nejsou oproti heslům tak uživatelsky přívětivé. Navíc tyto autentizační předměty mají standardně omezenou životnost, lze je ztratit, mohou být odcizeny, nebo nevědomky mohou být zapůjčeny.

V praxi rozlišujeme dva druhy autentizačních předmětů a to kontaktní, nebo bezkontaktní.

Další rozdělní je pak dle druhu, kde rozlišujeme předměty pouze s pamětí, předměty udržující hesla, předměty s logikou a chytré karty.

Biometrická autentizace:

Biometrická autentizace využívá jedinečných charakteristik lidského těla. Tyto vlastnosti nelze půjčit či vyzradit. Právě biometrická autentizace je momentálně nejpoužívanější způsob autentizace na mobilních zařízeních. Charakteristiky lidského těla mohou mít jak fyziologický, tak behaviorální charakter.

Fyziologické charakteristiky:

Úzce souvisí s parametry lidského těla. Typickými příklady pak jsou:

Otisky prstů- včetně jejich rozmístění, jejich brázd a rozvětvení.

Otisky dlaní- což je v principu rozšířenější verze otisků prstů

Geometrie ruky- tvar ruky, včetně šířky kostí a kloubů na ruce a prstech

Vzory cév na ruce- vzory tepen a žil na dlaních, nebo hřbetu ruky

Znaky v obličeji- znaky jako postavení a tvar nosu, postavení lícních kostí, očních důlků, aj.

Vzory na sítnici- vrstva cév v zadní části oka

Vzory na duhovce- vzor a viditelné charakteristiky duhovky

Behaviorální charakteristiky:

Úzce souvisí s chováním lidského těla. Typickými příklady pak jsou:

Dynamika podpisu- mapování kombinace vzhledu, tvaru, načasování a tlaku v průběhu psaní

Ověření hlasu- tón, intenzita, rytmus, výška hlasu

Dynamika pohybu myší- měření vzdálenosti, úhlu a rychlosti při práci s myší

Dynamika psaní na klávesnici- doba trvání stisku kláves, intenzita stisknutí, rozmístění jednotlivých prstů.

Dvoufázová autentizace:

Vzhledem k neustále se zvyšujícím bezpečnostním standardům a zároveň ochranou proti potenciálnímu zneužití třetí stranou, se čím dál tím více používá dvoufázová autentifikace. Jak již název napovídá, jedná se o dvě po sobě jdoucí autentifikace a s jejím využitím se setkáme v případech, kdy pracujeme s cennými, citlivými daty. Typickou dvoufázovou autentifikací je biometrie se zadáním kódu, nebo například konfirmační údaje vygenerované na jiném zařízení.

Kvantitativní ukazatele autentizace:

Autentizovaný subjekt může nabývat dvou stavů. Buďto se jedná o oprávněného uživatele, nebo o neoprávněného narušitele. Oprávněný uživatel se identifikuje svojí identitou, zatímco neoprávněný narušitel se identifikuje identitou jiného subjektu. Výsledkem této autentizace není nic jiného, než rozhodnutí o přijmutí, nebo odmítnutí identity subjektu.

		Rozhodnutí	
		Přijmout	**Odmítnout**
Situace	**Oprávněný uživatel**	Žádoucí stav	Chybné odmítnutí
	Neoprávněný narušitel	Chybné přijetí	Žádoucí stav

Obrázek 2 Možné rozhodovací situace

Zdroj: Vlastní zpracování

False accept rate- jedná se o podmíněnou pravděpodobnost, že pokud bude autentizován neoprávněný narušitel, tak dojde k chybě přijetí.

False reject rate- jedná se o podmíněnou pravděpodobnost, že pokud bude autentizován oprávněný uživatel, tak dojde k chybě odmítnutí.

[1][2][3]

2 VÝVOJ MOBILNÍCH ZAŘÍZENÍ A JEJICH ZABEZPEČENÍ

V této kapitole se podíváme na stručný vývoj moderních mobilních zařízení. Pokud se však bavíme čistě o moderních mobilních zařízeních a nezasahujeme příliš to historie, je nutné tato zařízení definovat jako zařízení se systémem iOS, Android, nebo jako zařízení se systémem Windows.

2.1 Vývoj zařízení na sytému iOS

iOS je označení operačního systému vyvíjený společností Apple, který byl primárně vyvinut pro mobilní telefony iPhone. Následně se však začal využívat i pro tablety iPad a jeho obdoba watchOS je používána pro chytré hodinky AppleWatch. V následujícím textu se proto seznámíme s těmito ikonickými produkty od prvních verzí, až do dnešní podoby.

Historie a současnost iPhone

Píše se rok 2007 a Steve Jobs představuje iPhone první generace. Revoluční telefon, který na tehdejší dobu disponoval nebývale velkým displejem a který nabídl komfortní rozlišení 320 x 480 pixelů. IPhone první generace přišel s takovými novinkami, jako jsou ignorování nezamýšlených dotyků, víceprstá gesta aj.

Ač se tento první iPhone setkal spíše s pozitivními ohlasy, měl pochopitelně celkem dost nedostatků. Například chybějící služba MMS, chybějící 3G, či nemožnost natáčet videa. Za největší přínos však lze považovat samotný systém, který byl uživatelsky velmi přívětivý a intuitivní.

Obrázek 3 iPhone 1 . generace

Zdroj:[42]

O rok později přišel nástupce původního iPhonu s označením iPhone 3G. Již samotný název jasně definuje, jaký nedostatek původního iPhonu odstraňuje a to chybějící podporu 3G sítí. Novinkou pro něj bylo i GPS. Pokud tento telefon byl v něčem opravdu revoluční, tak to v představení obchodu s aplikacemi App Store. Právě zprovoznění obchodu s aplikacemi udělalo z iPhonu plnohodnotný chytrý telefon. Telefon disponoval velkým displejem a výkonným hardwarem.

V roce 2009 byl představen iPhone 3GS, který vylepšil některé funkcionality předchozí generace, ale hlavně sloužil jako převodní můstek pro chystanou 4. generaci.

4. generace byla uvedena na trh v červnu roku 2010 s velkým očekáváním, která byla bezezbytku naplněna. Za opravdu revoluční věc se dá považovat Retina displej, na kterém nebyl patrný z běžných vzdáleností žádný pixel. Ten samý displej měl 3,5 palce a disponoval rozlišením 480 x 960 pixelů. Telefon také velmi výrazně vylepšil fotoaparát a představil přední kameru, která v kombinaci s taktéž nově představenou aplikaci FaceTime stvořila velmi populární multimediální komunikační platformu. Během uvedení 4. generace došlo také ke změně značení operačního systému, kdy původní označení OS nahradilo iOS.

Iphone 4s, podobně jako v případě 3s se jedná o vylepšenou verzi předchozího modelu. Jednalo se především o vylepšení hardwarových komponent. V rámci softwarového hlediska byla v tomto telefonu poprvé nasazena hlasová asistentka Siri.

Iphone5 byla reakce Apple na konkurenty. Ti do svých telefonů dokázali dostat výrazně větší displeje. Iphone5 poprvé překročil 3,5 palce a uvedl o půl palce větší displej – tzn. displej disponoval čtyřmi palci. Tento model také poprvé představil konektor Lightning. Telefon byl celkově přijat velmi pozitivně i díky velmi zdařilému designu a lehké hliníkové konstrukci.

Iphone 5s a 5C vyšly ve stejnou dobu a to v září roku 2013. Telefon opět vycházel z předešlé verze, nicméně přišel s jednou zcela zásadní novinkou a to úpravou domovského tlačítka. Již se nejednalo pouze o domovské tlačítko, ale bylo do něj přidáno TouchID. Tato technologie je založena na biometrické autentizaci pomocí fyziologické charakteristiky a velmi významně posunula zabezpečení zařízení. Tato technologie využívající jedinečnosti otisku lidského prstu, nejen že umožňuje odemknout zařízení, lze pomocí ní obchodovat se službami Apple v App Store, nebo ji využít k ověřování i v rámci jiných aplikací, včetně například aplikací mobilního bankovnictví.

Apple představuje novinky každý rok a rok 2014 nebyl výjimkou. V tomto roce představil opět dvojici nových modelů. Konkrétně šlo o modelu 6 a 6 Plus. Jednalo se v podstatě o jeden telefon (myšleno po hardwarové stránce), akorát byl provedený ve dvou různých rozměrových variantách. Základní model 6 měl displej o velikosti 4,7 palce, verze Plus pak ještě více- dokonce 5,5 palce. Telefon zároveň ze všech Apple telefonů byl nejtenčí. V rámci hardwaru významný krok dopředu bylo zavedení NFC čipu, který spolu v kombinaci s Apple Pay byl krok dopředu v rámci provádění plateb přes mobilní telefon.

O rok později, tehdy takřka dle zvyku, přišla opět vylepšená řada- 6S a 6S Plus. Ač telefony byly designově velmi podobné svým předchůdcům, nabízel řadu novinek. Mezi ty nejpopulárnější patřila funkce 3D touch, výrazné rozšíření kapacity baterie a vylepšený fotoaparát, který na základě toho umožňoval vytvářet pro iPhony typické Live Photos,

V roce 2016 vyslyšel Apple žádosti trhu a uvedl na trh model, který navrací menší rozměry displeje. Model s označením SE je v podstatě model 6S, přenesený do čtyřpalcového provedení. Zároveň se jednalo o model, který byl velmi slušný v poměru cena/výkon a věci, jako třeba chybějící Touch ID většině zákazníků nevadilo.

Rok 2016 však nebyl jen o SE, ale především o modelech 7 a 7 Plus. Tyto telefony se staly synonymem pro kvalitní fotoaparát. Dvojitá zadní kamera především velmi pomohla při focení portrétů a zajistila modelu dvojnásobný optický zoom. Mnoho lidí popudilo odebrání 3,5 Jacku

pro sluchátka. Na druhou stranu Apple již tehdy správně odhadl vývoj v podobě postupného nahrazování klasických sluchátek bezdrátovými a tento krok se časem ukázal jako správný, čemuž pomohlo ve stejnou dobu i představení Apple AirPods.

O rok později přichází další řada. iPhone 8 a 8 Plus. Po stránce designu se jedná o pokračovatele sedmičky. Tento model opět přichází s vylepšením předchozího modelu po všech stránkách. Za zmínku stojí True Tone technologie, což je technologie na přizpůsobení se barevného podsvícení vzhledem k okolí, čip Neural Engine pro rozšířenou virtuální realitu, nebo integrace bezdrátového nabíjení Qi.

V průběhu stejného keynote, jako byly představeny modely 8, byl představen dlouhou dobu tajemný model X. Jeho označení, které jako jediné není číselné odkazuje na řadu věcí. Primárně odkazuje na číslo 10, ale dá se jeho označením i chápat odkaz na 10 let iPhonů na světě. Zároveň označení může značit výjimečnost a jakýsi „X " faktor, který tato řada má. Tato řada odstraňuje fyzické domovské tlačítko a představuje zcela nový koncept autentizace. Jedná se o FaceID, což je princip na bázi biometrické autentizace, využívající fyziologické charakteristiky v obličeji. Display taktéž premiérově využívá technologie OLED a má zcela nový design, kdy tradiční obdélníkový tvar se rozšiřuje do rohů, kde vzniká prostor pro zobrazování základních ukazatelů (stav baterie, kvalita připojení k síti..). Tento model byl revoluční i cenou, která byla skokově největší, od předchozího modelu v historii všech iPhonů.

O rok později se i model X dočkal vylepšených následovníků. Modely s označením Xs a Xs Max se dočkaly úprav především ve vylepšení fotoaparátů. Poté ještě byla představena verze Xr. Tento model vznikl jako levnější alternativa výše uvedeným modelům. Nedisponoval tak kvalitní soustavou fotoaparátů, nedisponoval displejem OLED, nýbrž pouhým LCD a ani jeho provedení nebylo z takových materiálů, jako v případě Xs řady. I přesto si však získal celkem velkou oblibu. Všechny telefony z této řady pak disponují podporou dalších SIM karet, v podobě podpory tzv. eSIM.

V roce 2019 byl představen iPhone 11. Opět se jednalo o několik verzí, které v pozměněné podobně navazovaly na své předchůdce. V případě levnější verze 11 bez dalšího označení se jednalo o nástupce Xr. Tento model však měl vylepšenou foto soustavu, kdy přibyl na zadní stranu druhý snímač. Dražší verze nesla označení 11Pro a 11ProMax. Rozdíl mezi těmito dvěma typy byl pouze ve velikosti displeje. Oba oproti verzi 11 byly významně povýšené ve foto soustavě, kdy dostaly ještě jeden snímač. Ten umožňoval čtyřnásobný optický zoom a ultra širokoúhlé pořízení fotografií. Design umístění třech čidel se však stal vzorem i dalších modelů.

iPhone SE v nové verzi byl představen v roce 2020. Tento model cílí především na méně náročnější klientelu a jeho pořizovací cena nějak výrazně nevybočuje z kategorie „střední třídy“ v porovnání s prémiovými značkami telefonů na systému Android. Tento telefon vychází z modelu 8, se kterým je na první pohled takřka totožný. Vrací se domovské tlačítko a tím pádem i Touch ID. Zásadní rozdíl oproti verzi 8 je pak hardware. Tento model disponuje procesorem A13 Bionic z modelu 11 a kapacitou až 256Gb, podporuje eSIM. iPhone SE je ideálním modelem pro začínající uživatele iPhonů, nebo je celkem hojně využívám pro zaměstnance společností, jako služební telefon.

V témže roce, jako bylo představeno SE, došlo i k tradičně novému představení hlavních vlajkových lodí. iPhone s označením 12 se dočkal dokonce čtyř různých typových odnoží, které se primárně liší svojí velikostí. Nejmenším z nich je iPhone 12 s označením mini. Tento telefon překvapí relativně malým displejem „pouhých“ 5,4 palce, avšak velmi výkonným hardwarem. V rámci typu 12 bez dalšího označení je povýšena úhlopříčka na 6,1 palce, nicméně u ostatních parametrů je shodný s verzí mini. Prémiové modely v rámci této řady pak jsou verze 12 Pro a 12 Pro Max. Tyto modely oproti stejně pojmenovaným jedenáctkám se dočkaly opět vylepšení foto soustavy a například uvedením bezdrátové technologií MagSafe, která umožnuje spojení s různým dalším příslušenstvím. Například peněženkou, nebo bezdrátovou nabíječkou.

Stejný koncept dělení na jednotlivé verze, jako u modelu 12 má i skupina zařízení s označením 13. Oproti modelům 12 se opět nedočkáme zásadní designové změny. Opět dochází k vylepšení hardware. Tradičně se jedná o novou řadu procesorů, v tomto případě se jedná o Apple Bionic A15. Došlo taktéž ke značnému navýšení maximálního vnitřního úložiště, kdy kapacita modelů 13 Pro může dosahovat až 1TB.

Poslední modely, které v době psaní této bakalářské práce byly představeny, jsou modely s označením 14. Tato řada opět lehce pozměňuje jednotlivé modely, které v rámci ní jsou prezentovány. Oproti předcházející řadě 13 dochází k zrušení modelů mini. Naopak se představuje verze Plus, která jde diametrálně odlišně proti mini a nabízí oproti základnímu modelu větší display a to konkrétně 6,7 palce. U prémiových verzí Pro a Pro Max opět dochází k hardwarovému vylepšení oproti všem předchozím stejně značeným verzím.

Obrázek 4 Poslední představený model iPhone - 14 Pro Max

Zdroj:[43]

[13][14][15][17]

2.2 Vývoj telefonů na systému Android

Android je mobilní operační systém vyvíjený společností Google a založený na jádře Linuxu. Jeho vývoj začal v roce 2003, kdy společnost Android Inc. začala vyvíjet mobilní operační systém pro digitální fotoaparáty. O rok později, v roce 2004, byla tato společnost zakoupena společností Google a vývoj Androidu pokračoval jako projekt společnosti Google a začal se specializovat na vývoj právě pro mobilní telefony a jiná dotyková zařízení. Postupem času se systém Android začal nasazovat i například jako operační systém chytrých TV.

2.2.1 Historie a současnost telefonů Android

V roce 2008 byl uveden první mobilní telefon s operačním systémem Android, kterým byl HTC Dream. Tento telefon byl vyvinut společností HTC ve spolupráci s Googlem. Byl to první telefon, který měl plnou integraci s Google službami, jako jsou Google Maps, Gmail a Google Search.

Obrázek 5 HTC Dream - první mobilní telefon se systémem Android

Zdroj:[44]

V případě iPhonů lze jejich vývoj celkem jasně datovat a definovat. V případě telefonů na systému Android tomu však tak není. V následujících letech se na trhu objevily desítky dalších telefonů s operačním systémem Android, který postupně do svých zařízení nasazovalo čím dál tím více výrobců. V rámci této kapitoly se pokusíme představit a ve stručnosti popsat alespoň ty, které byly nějakým způsobem ikonické, respektive ty, které pomáhaly utvářet a formovat „Androidí“ část světa.

Rok po prvním telefonu s Androidem byl vydán model od výrobce Motorola s označením Droid. Tento telefon disponoval především velmi výkonným hardwarem.

V roce 2010 pak byl uveden na trh Samsung Galaxy S, který odstartoval řadu velmi populární řady S od tohoto jihokorejského výrobce, která přetrvává až do dnešní doby. První modely řad S se staly velmi populární a dalo by se říci, že se okolo roku 2010 se jednalo o nejpopulárnější telefon se systémem Android.

V roce 2013 byl vydán Google Nexus 5, který se díky čisté verzi systému (systém bez jakýchkoliv doplňků a úprav od výrobce nebo uživatele) Android stal velmi populární především u odborné veřejnosti a vývojářů.

O rok později byl vydán Samsung Galaxy Note 4, což byl první telefon, který kombinoval stylus (ovládací prvek pro dotykové displeje) s velkým displejem a byl velmi populární u kreativců a náročných uživatelů.

V roce 2015 se na trh dostává další telefon od Google, tentokrát model Nexus 6P, který podobně jako jeho předchůdce od Google v tomto seznamu se dočkal velké popularity u nadšenců a

vývojářů, neboť opět disponoval čistou verzí operačního systémem. Zároveň disponoval na tehdejší dobu i velmi kvalitním hardwarem.

Celkem zajímavý technologický pokrok přišel v roce 2016, kdy Samsung představil model S7 Edge, což byl první telefon, který představil zakřivený display. Kromě toho disponoval velmi výkonnou kamerou.

V témže roce byl vydán telefon Google Pixel, což byl první telefon, který byl plně navržený a vyrobený Googlem. Tento telefon byl respektován především díky velmi kvalitní kameře a velmi rychle vydávaným updatům.

V roce 2017 představuje Samsung další novinku. Model Galaxy S8 byl prvním telefonem, který představil nekonečný, bezrámečkový displej. Tím vlastně určil standard pro displeje, který se dochoval do až do dnešní doby.

O rok později představil Google vzhledem k historickému hledisku jeden z nejpovedenějších svých modelů. Jednalo se o model Pixel 3, který získal velké uznání za výkon a fotoaparát.

Abych nezmiňoval pouze tyto dva výrobce, zmíním i čínského výrobce Huawei, který v roce 2019 vydal model P30 Pro. Tento telefon byl první svého druhu, který nabízel čtyři fotoaparáty na zadní straně, které mimo jiné umožňoval pětinásobný optický zoom. Právě tato technologie z něj udělala v danou chvíli lídra v oblasti foto telefonů.

Další velmi významný milník přišel ve stejném roce, kdy Samsung poprvé představil model Galaxy Fold. Jak již název napovídá Fold (z anglického fold = složit), jednalo se o první komerční telefon se skládacím displejem. Tato technologie, ač z počátku měla faktické nedostatky, se stala velmi populární a Samsung nadále tento typ telefonů vylepšuje a zdokonaluje a řada Fold je vlajkovou lodí tohoto výrobce až do dnešních dní.

Obrázek 6 Samsung Galaxy Z Fold 4 - jeden ze symbolů dnešních Android telefonů

Zdroj:[45]

[18][19][20]

2.2.2 Problém čínských výrobců

Velmi významné zastoupení výrobců telefonů se systémem Android mají na trhu čínští výrobci. Ti se na výrobu těchto zařízení zaměřují prakticky od počátku systému Android, nicméně obzvláště na našem trhu nastal velký boom čínských výrobců zhruba od roku 2015. Zařízení těchto výrobců nabízí velmi výkonný hardware a fotoaparát, avšak v porovnání s jinými značkami se jedná o zařízení řádově levnější. Mezi tyto výrobce můžeme řadit už výše zmíněný Huawei a dále třeba Redmi, Xiaomi aj.

V tomto bodě je velmi důležité zmínit kontroverzi, která tato čínská zařízení provází. Zhruba od roku 2012 začaly vycházet prvotní zprávy o riziku, které pramení od čínských výrobců, kteří do svých telefonů předinstalovávají software, který sbírá data o uživatelích. Tyto zpočátku spíše spekulativní zprávy byly potvrzeny v roce 2018, kdy americká vláda zakázala vládním úředníkům používat telefony výrobce ZTE. Opravdová bomba v tomto směru však vybuchla až o rok později, kdy ze stejných důvodů tehdy největší čínský výrobce Huawei byl zařazen na černou listinu americké vlády. Důsledkem toho bylo faktické ukončení spolupráce Huawei s americkými technologickými společnostmi a taktéž omezení přístupu k operačnímu systému Android a technologiím Google.

Tato kauza celkově vrhla na čínské výrobce negativní světlo, se kterým se potýká do dnešních dob.

[30][31]

2.3 Vývoj telefonů Windows Phone

Windows Phone byl mobilní operační systém vyvinutý společností Microsoft. Jednalo se o reakci Microsoftu na činnosti dvou největších technologických konkurentů na světovém trhu (Apple, Google) a o snahu proniknout do pro Microsoft tehdy zcela nového prostředí. Ač přes nesporné kvality a technologické novinky, které tento systém a telefony s tímto systémem nabízely, skončila tato etapa Microsoftu špatně.

Vývoj telefonů Windows Phone

První telefony s Windows Phone, tehdy označením 7 jsou uvedeny na trh v roce 2010. Mezi nimi jsou například HTC HD7, Samsung Focus a Dell Venue Pro.

V listopadu roku 2011 je na trh uvedena Nokia Lumia 800, první telefon od Nokie s Windows Phone.

O rok později Microsoft vydává aktualizaci Windows Phone 8 a představuje nové telefony jako Nokia Lumia 920, HTC 8X a Samsung ATIV S .

V roce 2013 je vydána Nokia Lumia 520 – jedná se o první telefon nižší cenové katerogie s Windows Phone 8 a Nokia Lumia 1520, což byl v podstatě první phablet s Windows Phone.

Celkem významný krok, který měl pomoci v konkurenčním boji proti iOS a Android, byla akvizice divize mobilních zařízení Nokia a následná produkce telefonů s označením Microsoft Lumia. Téhož roku, na podzim, Microsoft uvádí Windows Phone 8.1 - update s novými funkcemi, jako je například Cortana, osobní digitální asistentka. To se psal rok 2014.

O rok později Microsoft uvádí první telefony s Windows 10 Mobile, včetně modelů Microsoft Lumia 950 a 950 XL.

Ani tyto modely se však nedočkaly velkého ekonomického úspěchu, a proto v roce 2015 Microsoft oznámil, že se zaměří na vývoj aplikací pro ostatní platformy a Windows Phone již nebude významně aktualizován. V roce 2017 Microsoft definitivně ukončil podporu pro Windows Phone.

Tím skončila cesta Microsoftu ve vývoji vlastního operačního systému pro mobilní zařízení a výroba samotných zařízení. Ač měl systém především v porovnání s Androidem značné výhody v bezpečnosti a v porovnání s iOS v ceně zařízení, nedokázal si najít masivní podporu.

[32][33]

3 OPERAČNÍ SYSTÉMY MODERNÍCH MOBILNÍCH ZAŘÍZENÍ A JEJICH ZABEZPEČENÍ

V této kapitole se podíváme na operační systémy moderních mobilních zařízení. Téma, které by samo vydalo na několik bakalářských prací, se pokusíme jednodušeji shrnout především s ohledem na možnosti zabezpečení těchto systémů a toho, jak se tyto bezpečností funkce v jednotlivých operačních systémech vyvíjely. Tyto funkce a možnosti budeme řadit chronologicky od nejstarších verzí systému až po současnost. Za aktuální systémy lze považovat systémy, o kterých jsme se tu v menší, či větší míře zmínilo, a to o systémy iOS, Android a Windows.

3.1 iOS

Jak již bylo zmíněno v předchozí kapitole o samotném vývoji telefonů iPhone od americké firmy Apple, byl první telefon i operační systém vydán v roce 2007.

Tento systém s označením iPhone OS 1.0 obsahoval pouze základní, přesto na tehdejší dobu celkem pokročilé funkce, jako byl zámek obrazovky pomocí kódu a možnost vzdáleného smazání obsahu prostřednictvím iCloudu.

V roce 2010 s vydáním iOS4 se zvyšuje standard zabezpečení, když Apple představil hardwarové šifrování pro všechna data nacházející se na daném zařízení. To znamená, že data jsou i v případě fyzického získání zařízení chráněna hesly.

V rámci iOS 5 byly představeny další bezpečnostní funkce. Bylo přidáno šifrování emailových zpráv, ale také byla představena funkce „Najdi mě“ v originále „Find me“, která umožňuje zařízení na dálku lokalizovat a případně zařízení smazat.

Za další významný bezpečností krok lze považovat funkce operačního systému spjaté s TouchID, které byla zmíněny již v kapitole věnované vývoji iPhonů.

V roce 2014 představuje Apple funkci „Aktivační zámek“ v originále „Activation Lock“, což je funkcionalita systému, která velmi významně ztěžuje krádež zařízení. S touto aktivovanou bezpečnostní funkcionalitou je zařízení v podstatě blokováno a nelze jej použít jinak, než se s původními spárovanými údaji o majiteli (bez jeho Apple ID a hesla..).

Další významná bezpečností funkcionalita zaměřena především na soukromí samotného uživatele přišla v roce 2016, kdy byl představen nový šifrovací systém nazvaný „Diferenciální soukromí“ v originále „Differential privacy“, který umožňuje sbírat výrobci data ze zařízení, aniž by ohrozil samotné soukromí uživatele.

V rámci iOS 11 Apple představuje funkci „Bezpečný režim“, v originále „Secure mode“. Jedná se o bezpečnostní funkci, která způsobuje možnost odemčení zařízení pouze prostřednictvím hesla, nikoliv TouchID, nebo FaceID. Tento režim také zablokoval možnost vzdáleného přístupu k zařízení přes USB port.

Další bezpečnostní funkce, která se zabývá minimalizováním rizik přicházející z okolí zařízení je „USB Restricted Mode“. Je to funkcionalita, která vypne přístup k USB portu po hodině neaktivity. Tato funkcionalita výrazně zlepšuje zabezpečení proti útokům založeným na připojení k PC.

Další bezpečnostní autentizace, která chrání uživatele a byla vydána v rámci iOS 12, je funkce „Silné heslo“ v originále „Strong password“, která umožnuje uživatelům vytvářet a spravovat silná hesla a zároveň zabraňuje opakovanému užívání stejného hesla. Tato funkce automaticky vyplňuje takto vygenerovaná hesla do formulářů a uživatelé se nemusí starat o pamatování hesel, ani nemusí tato hesla ručně zadávat.

V téže době byla také představena funkce na ochranu soukromí, která chrání soukromí uživatelů blokováním reklamy.

V rámci systému iOS 13 byla představena funkce „Přihlašování Apple“, která umožňuje se přihlašovat na webové stránky a aplikace prostřednictvím Apple ID, ale zároveň toto Apple ID nikde dále nezmiňuje a nezveřejňuje.

V roce 2020 vydal Apple novou funkci nazvanou "Přístupová karta k místům" v originále „Access Cards to Places“, která umožňuje uživatelům přidávat digitální karty pro přístup k různým místům, jako jsou budovy, kanceláře a další zařízení. Tyto digitální karty jsou uloženy v zařízení a mohou být snadno sdíleny s ostatními uživateli.

Poslední významnou funkci, kterou si zde představíme, je funkce, která vyšla v rámci systému iOS 14.5. Jedná se o funkci pro ochranu soukromí uživatelů. „Transparentní sledování aplikací“ v originále „App Tracking Transparency“. Tato funkce umožnuje uživatelům rozhodovat o způsobu sledování jejich činností v rámci jednotlivých aplikací.

[16][27]

3.2 Android

Původní verze operačního systému Android nekladly příliš velký důraz na bezpečnost a systém byl velmi zranitelný vůči bezpečnostním hrozbám. Tehdy bylo celkem snadné si do telefonu stáhnout malware, případně stáhnout jiné nezabezpečené aplikace.

Tuto základní a zásadní hrozbu vyřešil Google v rámci funkce Androidu 2.2. Tato funkce nově umožňovala instalovat aplikace pouze z oficiálního obchodu Google Play a celkově dokázala separovat jednotlivé aplikace v rámci systému.

V dalších verzích Androidu došlo k významnému posunu bezpečnostních funkcí. Ve verzi 2.3 a 4.0 bylo představeno šifrování dat, zabezpečené spouštění aplikací a možnost případně rizikové aplikace zakázat. Tyto verze obsahovaly také novou funkci „Důvěryhodné aplikace“ v originále „Verify Apps“, která před samotnou instalací aplikace skenovala její obsah a případnou přítomnost malware.

I přes tyto nastavené funkce byly právě aplikace třetích stran nadále považovány za největší hrozby pro systém, proto i v rámci dalších verzí Androidu došlo k rozšiřování funkcí právě tímto směrem. Verze 4 .1 (Jelly Bean) a 4 .4 (KitKat) představily mj. funkci „Google Play Protect“, která umožňovala kontinuální skenování a monitorování nainstalovaných aplikací, právě pro případ potenciálních hrozeb těchto aplikací.

Zvýšení ochrany osobních dat a údajů přineslo vydání verze Androidu 6 .0 s označením Marshmallow. Funkce „runtime permissions“ umožňovala uživatelům variabilitu v určování toho, co má jaká aplikace za oprávnění a k čemu má v rámci zařízení přístup. Zjednodušeně by se dalo říci, že tato funkce omezovala neoprávněný přístup k citlivým datům.

S vydáním dalších verzí se 7.0 (Nougat) a 8.0 (Oreo) se Google zaměřil na zlepšování bezpečnosti v oblasti sítě a připojení. V rámci těchto dvou verzí byla představena funkce „File-based encryption“, která podporovala namísto šifrování celého disku šifrování jednotlivých souborů. To jednoznačně celkově usnadnilo správu souborů. Dalším vylepšením byla například vylepšená autentizace, nebo rozšíření funkce „Google play protect“, která nově poskytovala rozšířenější možnosti kontroly ochrany soukromí.

V dalších verzí 9.0 (Pie) a 10 (již bez dalšího označení) došlo k významným změnám vzhledem k nově využívaným funkcím biometrické autentizace. To šlo ruku v ruce s funkcí „Android Protected Confirmation“, která tyto metody využila k vyššímu zabezpečení citlivých aplikací a k přihlašování.

S vydáním Androidu 11 a 12 se Google soustředil na významné zlepšení zabezpečení v případě využívání zařízení jak pro soukromé, tak i pracovní účely. Mezi tuto funkci patří izolace pracovních profilů a ochrana soukromí pomocí omezených oprávnění. Další zajímavá bezpečnostní funkcionalita je „Google Play System Updates“, která umožnovala aktualizace systému a zabezpečení bez nutnosti aktualizovat zařízení celé.

[21][23]

3.3 Windows

Windows je operační systém od společnosti Microsoft. Jedná se o celosvětově nejpoužívanější operační systém pro osobní počítače a servery. Nejnovější verze Windows jsou však přizpůsobené i pro mobilní zařízení, především pro tablety, nebo pro zařízení typu tablet pc. Verze, které jsou uzpůsobené pro tato využívaní začínají od systému Windows 8 a výše. Předchozí verze proto nebudou v rámci této kapitole více zmiňovány.

Verze 8 byla první verze, která byla přizpůsobená primárně pro dotyková zařízení. V rámci bezpečnostních funkcionalit nabídla přímou integraci antivirového a antimalwarového do operačního systému prostřednictvím Windows Defender. Dále systém obsahoval funkci Smart Screen, což je filtr proti spamu a phisningu.

V další verzi systému s označením 8.1, která navazovala na systém 8 a byla více uživatelsky přívětivější, jsme se mohli setkat s další řadou bezpečnostních vylepšení. Za nejvýznamnější lze považovat vylepšené zabezpečení pro UEFI, který chrání zařízení před útoky v rámci bootování. Další, co lze zmínit, je povolení UAC pro aplikace ve Windows Store, který zabraňuje neoprávněným změnám od samotných uživatelů. Do té doby si uživatel z Windows Store mohl nainstalovat prakticky cokoliv a toto funkcionalita mu v tom dále zabraňuje.

I další verze s označením Windows 10 přinesla další vývoj bezpečnostních funkcí. Stejně jako v jiných systémech se Microsoft přizpůsobil autentizaci pomocí biometrie a pro tyto účely představil „Windows Hello“, která právě pomocí těchto údajů umožňovala přihlášení do systému. Významným a populárním vylepšením byl nástroj Bitlocker, který pro zlepšení bezpečnosti šifruje disk. Dalším vylepšením je i software „Windows Defender Exploit Guard“, který je dostupný v rámci „Windows Defender“ a pomáhá především proti útokům využívajících zranitelnosti/ neaktuálnosti systémů a aplikací. Poslední věc, kterou zmíníme v rámci systému 10, je „Microsoft Defender Application Guard“, který pro lepší ochranu izoluje prohlížeč od zbytku systému.

Poslední, relativně nedávno vydaná verze Windows 11, přišla také s několika zajímavými bezpečnostními vylepšeními. Jako první je potřeba zmínit vylepšení pro „Windows Hello“, ve kterém nově kombinuje ověření identity pomocí biometriky v kombinaci s kódem. Pro ochranu soukromí představil takzvané „Virtuální zabezpečené prostředí“, které umožňuje vytvořit izolované a chráněné prostředí pro případ práce v citlivých aplikacích, nebo pro citlivé operace. Další funkcí, která stojí za zmínku je „Encrypted DNS“, která zajišťuje, že veškerý provoz mezi systémem a DNS je šifrován, což opět velmi významně zvyšuje bezpečnost. V neposlední řadě došlo v rámci Windows 11 k vylepšení ochrany proti ramsomwarem. Nástroj, který je v rámci

Windows Defender nejen, že detekuje samotný ramsonware, ale zároveň nabízí možnosti obnovy po případném útoku.

[34][35]

3.4 Základní rozdíly mezi iOS a Android

Oba dva nejpoužívanější systémy moderních mobilních zařízení jsou v určitých směrech rozdílné. Ty nejzásadnější rozdíly si rozebereme dle jednotlivých dílčích parametrů v této kapitole.

Rozdíly v operačním systému:

iOS je výhradně od společnosti Apple, zatímco Android je vyvíjen open-source komunitou.

iOS je k dispozici pouze na iPhonech a iPadech, zatímco Android je k dispozici na široké škále zařízení od různých výrobců, jako jsou Samsung, Huawei nebo Google Pixel.

Rozdíly v uživatelském rozhraní:

iOS má elegantní a snadno použitelné rozhraní, zatímco Android nabízí větší možnosti přizpůsobení.

V iOS jsou notifikace zobrazovány na centrálním místě, zatímco v Androidu jsou více decentralizované a zobrazují se podle aplikací.

iOS poskytuje uživatelům možnost jednoduše získat přehled o své spotřebě dat, zatímco Android nabízí více možností pro vlastní úpravu.

Rozdíly v bezpečnosti:

iOS poskytuje vysokou úroveň bezpečnosti a má přísnější pravidla pro aplikace v App Store, což vede ke snížení rizika malwaru. Android má větší riziko pro malware, protože vývojáři mohou publikovat aplikace bez přísných pravidel, jako v App Store.

iOS je znám svojí rychlostí vydávání aktualizací. V rámci distribuce těchto aktualizací dostává většina iOS aktualizace takřka okamžitě. V případě Androidu velmi závisí na výrobci a stává se, že mnohdy jsou tyto aktualizace zpožděné.

Ač žádný systém není 100% bezpečný, podle nedávné studie předního výrobce antivirového zabezpečení, společnosti Symantec se 99% mobilního malware týká Androidu. Nicméně i tak by měli být uživatelé iOS obezřetní a nespoléhat výhradně na systém samotný.

.

Rozdíly v ceně:

iOS zařízení jsou obecně dražší než Android zařízení.

Rozdíly v aplikacích:

Většina aplikací pro iOS je placená, zatímco většina aplikací pro Android je zdarma.

iOS má v App Store menší výběr aplikací než Android, ale aplikace jsou obvykle kvalitnější a méně náchylné k chybám.

Tyto rozdíly jsou obecné a mohou se lišit v závislosti na konkrétních modelech a verzích operačních systémů. Každý uživatel by měl zvážit své potřeby a preference při výběru mezi iOS a Android.

[13][14][20][21]

4 ZABEZPEČENÍ AKTUÁLNÍCH ZAŘÍZENÍ

V rámci této kapitoly si vysvětlíme, proč je nutné zařízení chránit a s jakými potenciálními hrozbami se můžeme setkat.

4.1 Nutnost zabezpečení

Moderní mobilní zařízení obsahují velké množství osobních informací, jako jsou kontakty, fotografie, bankovní údaje a přístupové údaje k sociálním sítím. Tyto informace mohou být cenné pro kybernetické útočníky, kteří se snaží získat přístup k citlivým informacím.

4.2 Hrozby dnešní doby

V rámci této podkapitoly se seznámíme s aktuálně nejčastějšími hrozbami, se kterými se lze setkat.

4.2.1 Malware

Malware, zkráceně pro malicious software, je obecný termín, kterým se označuje jakýkoli software, který je navržen tak, aby poškodil, infikoval, nebo ovládl cílový počítač, mobilní zařízení, nebo síť. Malware můžeme považovat za slovo nadřazené vůči jednotlivým typům malware, kterými jsou například:

Počítačový vir

Počítačový vir je programový kód, který se může šířit prostřednictvím počítačových sítí nebo sdílených médií. Může se nekontrolovatelně množit, poškozovat soubory nebo celý systém, ukrádat data a škodit uživatelům. Některé viry se mohou aktivovat a šířit bez povšimnutí uživatelem, což zvyšuje jejich nebezpečnost.

Počítačový červ

Počítačový červ je škodlivý program, který se šíří počítačovými sítěmi bez vědomí uživatele. Červ se dokáže sám kopírovat a přenášet na další zařízení bez nutnosti hostitelského programu. Červi mohou mít různé cíle, například odcizení citlivých informací, zpomalení zařízení nebo vytvoření botnetu. Často jsou šířeni prostřednictvím e-mailových příloh, nakažených webových stránek nebo nezabezpečených sítí.

Trojský kůň

Trojský kůň je škodlivý program, který se maskuje jako legitimní software a umožňuje útočníkovi získat kontrolu nad napadeným zařízením. Může sloužit k odcizení hesel, sledování

uživatele nebo instalaci dalšího škodlivého softwaru. Je často šířen prostřednictvím e-mailových příloh, nakažených webových stránek nebo nezabezpečených sítí.

Adware

Adware je škodlivý software, který zobrazuje agresivní reklamy na obrazovce a sleduje uživatele pro zobrazování personalizovaných reklam. Může zpomalit zařízení a snižuje jeho výkon. Obvykle je distribuován jako součást zdarma stahovatelného softwaru.

Ransomware

Ransomware je typ škodlivého softwaru, který kryptuje soubory na napadeném zařízení a požaduje od uživatele výkupné za jejich obnovení. Často se šíří prostřednictvím e-mailových příloh, nakažených webových stránek nebo nezabezpečených sítí. Pokud uživatel nezaplatí výkupné, může dojít k trvalé ztrátě dat. Na druhou stranu ani zaplacení výkupného se v mnohých případech nerovná obdržení dekryptovacího klíče.

Rootkit

Rootkit je škodlivý program, který umožňuje útočníkovi získat neomezený přístup ke kompromitovanému zařízení. Může být skrytý před antivirovým softwarem a je obtížně odstranitelný.

Spyware

Spyware je škodlivý software, který sleduje činnost uživatele počítače nebo mobilního zařízení bez jeho vědomí nebo souhlasu. Může sbírat osobní informace, jako jsou hesla, bankovní údaje, historii prohlížení a další.

Keylogger

Keylogger je škodlivý software, který zaznamenává stisknuté klávesy na počítači nebo mobilním zařízení. Tímto způsobem může útočník získat přístup k citlivým informacím, jako jsou hesla, bankovní údaje a další.

Botnet

Botnet je síť infikovaných zařízení, které jsou ovládány útočníkem pomocí škodlivého softwaru. Tyto počítače mohou být použity k provádění útoků, jako jsou DDoS, odesílání spamu nebo krádeže dat. Obvykle jsou infikovány bez vědomí uživatele.

Scareware

Scareware je škodlivý software, který zobrazuje falešné varování na obrazovce, aby vyděsil uživatele a přiměl ho ke koupi falešného antivirového softwaru nebo k poskytnutí citlivých informací. Může se šířit prostřednictvím reklam nebo e -mailových zpráv.

[24][25][26]

4.2.2 Phishing

Phishing je typ útoku, při kterém útočník vytváří falešnou identitu, obvykle prostřednictvím e-mailu nebo webové stránky, aby získal citlivé informace od uživatele. Tento typ útoku se často zaměřuje na získání přístupových údajů ke službám, jako jsou bankovní účty nebo sociální sítě. Phishing může být velmi sofistikovaný, s použitím falešných webových stránek, e-mailů, které vypadají jako oficiální zprávy od legitimních firem nebo dokonce s podvrženým odesílatelem.

Příklady phishingových útoků zahrnují podvržené webové stránky, které vypadají jako oficiální bankovní webové. Phishingový e -mail může vypadat jako oficiální e-mail od banky, požadující aktualizaci vašich bankovních údajů, nebo od známého e-shopu, který vám nabízí různé slevy a akce.

[37]

4.2.3 Neoprávněný přístup k datům

Neoprávněný přístup k datům je proces, kdy někdo získá přístup k informacím, ke kterým by neměl mít přístup. Tento typ útoku se může stát v důsledku slabých bezpečnostních opatření nebo zneužití oprávnění k přístupu k citlivým datům. Neoprávněný přístup k datům může být motivován různými faktory, včetně finančního zisku, sabotáže, špionáže nebo vydírání.

Příklady neoprávněného přístupu k datům zahrnují útoky hackerů, kteří se pokoušejí získat přístup k bankovním účtům, účtům na sociálních sítích a dalším citlivým informacím. Zaměstnanci mohou také zneužívat svých oprávnění k přístupu k datům, aby se dostali k citlivým informacím o svých kolezích nebo konkurenci. Neoprávněný přístup k datům může mít zničující dopad na jednotlivce, firmy i společnosti jako celek.

4.2.4 Nedostatečná aktualizace software

Nedostatečná aktualizace software je situace, kdy uživatelé neaktualizují své operační systémy, aplikace a další software, který používají. Tento nedostatek může způsobit zranitelnost v softwaru, kterou by mohli zneužít útočníci k provedení útoku. Tato zranitelnost může být využita k ovládnutí systému nebo k odcizení citlivých informací.

[36]

4.2.5 Používání veřejných WI-FI sítí

Používání veřejných Wi-Fi sítí představuje pro uživatele vysoké riziko zranitelnosti a útoků ze strany kyberkriminality. Hlavní příčinou zranitelnosti je fakt, že většina veřejných Wi-Fi sítí není dostatečně zabezpečena, což umožňuje útočníkům snadno získat přístup k uživatelským účtům, heslům a dalším citlivým informacím.

[36]

4.2.6 Sociální inženýrství

Sociální inženýrství je technika, kterou útočníci využívají k získání důvěrných informací nebo k provedení útoků na cílovou osobu, organizaci nebo síť. Útočníci často využívají psychologické a sociální triky, aby nalákali oběť ke sdělení citlivých informací, nainstalovali škodlivý software nebo provedli jiné útoky.

Mezi nejčastější techniku sociálního inženýrství patří již výše samostatně zmiňovaný phishing. Další technikou je pretekstování, kdy útočník využívá důvěryhodné identity, jako jsou například zaměstnanci IT nebo pracovníci technické podpory, aby získal důvěru a informace od oběti. Další technikou je tailgating, kdy útočník využívá fyzického přístupu k místnosti nebo budově, k získání důvěrných informací od zaměstnanců.

[36]

4.2.7 Zálohování dat do cloudu

Zálohování dat do cloudu může být velmi užitečné, ale s sebou nese také určitá rizika. Mezi hlavní rizika patří například riziko ztráty dat, riziko úniku dat, riziko narušení soukromí a riziko závislosti na třetí straně.

Pokud uživatelé ukládají svá data do cloudu, mohou se setkat s rizikem, že tato data budou ztracena kvůli chybě u poskytovatele cloudu nebo kvůli chybě u uživatele při zálohování dat. Další riziko spočívá v tom, že poskytovatel cloudu může být hacknut a data mohou být odcizena.

[25]

4.2.8 Nedostatečné šifrování dat

Nedostatečné šifrování dat může znamenat, že citlivé informace jsou snadno přístupné pro kybernetické útočníky. To může vést k úniku osobních údajů, finanční ztrátě a dalším nepříjemnostem. Příkladem nedostatečného šifrování dat může být použití slabých hesel nebo zastaralých šifrovacích algoritmů.

Je důležité používat silná a unikátní hesla pro každý účet a šifrovat citlivé soubory a komunikaci pomocí moderních a bezpečných algoritmů. Například je důležité používat protokol HTTPS pro zabezpečení webového provozu a používat silné šifrovací algoritmy pro šifrování e-mailů.

[25][24]

5 BEZPEČNOSTNÍ STANDARDY A DOPORUČENÍ

V této praktické části se seznámíme s jednotlivými postupy a doporučení zabezpečení moderních mobilních zařízení dle kategorie uživatelů. Pro účely této bakalářské práce jsou tito uživatelé rozděleni do čtyř různých kategorií. Toto rozdělení především znamená potenciální problémy a důsledky těchto problémů v případě napadení systému daného uživatele.

5.1 Zabezpečení „pro dítě“

Technologický postup je v posledních letech obrovský a dosah chytrých moderních mobilních zařízení se neustále rozšiřuje. Vděčit za to lze především vzhledem k platům nízké pořizovací ceně jednotlivých zařízení. Z toho důvodu tato zařízení používají i uživatelé, pro které to bylo například před deseti lety prakticky nemyslitelné. Mluvím nejen o důchodcích, ale především o dětech. Tato zařízení jsou standardně připojena na internet, a proto je důležité mít tato zařízení dostatečně zabezpečena. Ač se v případě zařízení určených pro děti nejedná o potencionální riziko ztráty citlivých dat, jde především o ochranu dítěte jako osobnosti, zamezení přístupu na případné problematické stránky apod.

5.1.1 Definování uživatele

Za dětského uživatele lze považovat každé dítě v rozsahu od dvou let zhruba po dobu celé základní školy. Respektive do chvíle, než začnou na svých zařízení využívat i jiné aplikace, které mohou být citlivé na ztrátu, nebo odcizení dat. Jedná se o celkem širokou paletu věku. U dětí zhruba do věku deseti let lze předpokládat, že svá chytrá zařízení budou primárně používat na streamovací služby (Youtube, Netflix aj.) a aplikace pro zábavu. U starších lze již předpokládat například využívání sociálních sítí. Se zvyšujícím se věkem stoupá zároveň gramotnost těchto uživatelů, běžně kolem 8. roku života jsou již schopni vyhledávat a stahovat aplikace, které mohou být potenciálním problémem. V rámci ochrany těchto uživatelů se však musíme na problém dívat více směry. Samozřejmě je nutné ochránit systém samotný, zároveň je však důležité mít i přehled nad aktivitami dětí.

5.1.2 Rizika

Jak již bylo zmíněno výše. Na podobných typech zařízení by se neměla nacházet prakticky žádná vyloženě citlivá data. Nicméně nelze říci, že by tato zařízení nepředstavovala riziko. Tato zařízení na jednu stranu nepředstavují riziko sama pro sebe- v případě jakéhokoliv problému lze zařízení snadno obnovit do továrního nastavení, ale celkem významné riziko mohou představovat pro další zařízení ve stejné síti. Na to se velmi často zapomíná. Jedno nějakým

způsobem rizikové zařízení může například způsobit pád sítě, nebo i to, že se po síti začne samo šířit problematický software. Můžeme říci, že se jedná o ukázkový způsob šíření viru.

5.1.3 Doporučená zabezpečení

Základní doporučená nastavení

1. Nastavte silné heslo, případně kód k odemčení zařízení. Vyvarujte se nejběžnějších kombinací (např. 1111, 1234, 4444 apod.) Případně k odemčení zařízení používejte biometrické údaje, umí-li to vaše zařízení.
2. V žádném případě nepoužívejte pro tato zařízení stejný uživatelský účet jako pro jiná zařízení. Používejte jednoúčelový uživatelský účet, v případě dětí rozhodně zvažte používání tzv. „účtu pro dítě“.
3. Omezte přístup k aplikacím. Můžete nastavit omezení pro aplikace, které vaše dítě používá a blokovat aplikace, které jsou pro dítě nevhodné. V moderních mobilních operačních systémech jako je Android nebo iOS lze nastavit speciální módy pro děti, které omezí přístup k aplikacím a webovým stránkám.
4. Mějte povolené a nastavené systémové funkce, které mohou pomoci nalézt ztracená nebo odcizené zařízení. Mezi typický příklad patří funkce „Najít“.

Pokročilá – volitelná zabezpečení

1. Nastavte časové limity pro používání zařízení. Není vždy nutné, aby vaše dítě trávilo u mobilního zařízení více času, než je například denní průměr.
2. Sledujte aktivitu vašeho dítěte. Pokud se jedná o malé děti, můžete použít funkce sledování aktivit a ujistěte se, že vaše dítě používá zařízení bezpečně. Na trhu je velká řada aplikací, které umožní sledování toho, jaké aplikace vaše dítě používá, jaké webové stránky navštěvuje a s kým komunikuje.

Celkově je důležité mít otevřenou komunikaci s dítětem o tom, jak používat mobilní zařízení bezpečně. S těmito kroky můžete pomoci chránit vaše dítě před riziky na internetu a umožnit mu bezpečné a zdravé používání mobilních zařízení.

5.2 Zabezpečení běžného uživatele

Rozvoj technologií a aplikací napomáhá k tomu, že služby, aplikace a data, která ještě například před deseti lety byla výhradně pro klasická zařízení, jsou momentálně hojně používána i na mobilních zařízení.

5.2.1 Definování uživatele

Pod pojmem běžného uživatele si můžeme představit běžného dospělého člověka, který své zařízení využívá čistě pro soukromé účely. Předpokládá se, že tento uživatel na svém zařízení nijak nepracuje s citlivými firemními údaji. Tito uživatelé tudíž používají mobilní zařízení na běžné činnosti, jako je pořizování dokumentů (fotografií, textů apod.) a mají na zařízeních aplikace třetích stran. V dnešní době zcela běžné sociální sítě, či aplikaci mobilního bankovnictví. Tento člověk v nějaké míře používá komunikační aplikace a prostředky.

5.2.2 Rizika

Jak již bylo zmíněno v předchozím odstavci, tak uživatel nějakým způsobem pracuje s pro něj citlivými daty. Pokud budeme vycházet z výše napsaného, můžeme se bavit například o fotografiích, které ač nemají nějakou zásadnější hodnotu, jsou velmi citlivé čistě z osobní perspektivy. Fotky obecně velká část uživatelů považuje za právě to nejcennější, co ve svém zařízení má, a proto jejich případná ztráta může mít pro tento typ uživatelů významný dopad. Podobně citlivé jsou pro dané lidi i sociální sítě, kdy v případě napadení systémů může být spárovaný účet na sociální síti využit například pro rozesílání spamu. Případně může využívat principů socio techniky pro získávání citlivých údajů o jiných osobách. V definování uživatele bylo taktéž zmíněno využívání mobilního bankovnictví. Tyto aplikace jsou však velmi robustní a právě samy dané banky definují přísné principy. Mezi ně může patřit například využívání dvoufázové autentizace, fungování pouze na podporovaných verzích systémů aj.

5.2.3 Doporučená zabezpečení

Základní doporučená zabezpečení:

1. Používejte silné heslo, případně kód k odemčení zařízení. Vyvarujte se nejběžnějších kombinací (např. 1111, 1234, 4444 apod.) Případně k odemčení zařízení používejte biometrické údaje, umí-li to vaše zařízení.
2. Mějte povolenou automatickou aktualizaci jak systému, tak i jednotlivých aplikací. To zajistí, že budou pravidelně instalovány bezpečnostní záplaty a aktualizace.
3. Mějte povolené a nastavené systémové funkce, které mohou pomoci nalézt ztracená nebo odcizené zařízení. Mezi typický příklad patří funkce „Najít“.
4. Nepoužívejte neznámé aplikace. Stahujte pouze aplikace z ověřených zdrojů – AppStore, GooglePlay.

5. Mějte nastaveno automatické zálohování pro případ ztracení nebo fatálního poškození zařízení. Zvažte rozšíření základního cloudového úložiště.

Pokročilá – volitelná zabezpečení:

1. Používejte placený antivirový programu, podobně jako například u stolních PC. Drtivá většina výrobců antivirového softwaru nabízí své produkty i pro operační systémy mobilních zařízení.
2. Mějte správně nastavená oprávnění pro aplikace. Některé aplikace mohou získat přístup k vašim osobním údajům a sítím. Uživatel by měl tato práva na přístup udělovat pouze prověřeným aplikacím.
3. Používejte dvoufaktorové ověření. Dvoufaktorová autentizace ztíží přístup, pokud by bylo heslo nějakým způsobem ohroženo. Uživatel musí zadat nejen heslo samotné, ale také kód, který mu bude zaslán na jiné zařízení.
4. Používejte silné zabezpečení pro síť, ve které se pohybuje vaše zařízení. Standardně se jedná o domácí WI-FI síť. Mějte přehled, která zařízení se nacházejí ve stejné síti.
5. Mějte vypnutý Bluetooth a NFC ve chvíli, kdy se nepoužívají.

5.3 Zabezpečení pro firemního uživatele

V rámci praktické části bakalářské práce se jedná o pravděpodobně nejpodstatnější skupinu uživatelů. Firemních uživatelů je velká řada a navíc pracují s citlivými údaji. Z toho důvodu lze jednoduše říci, že zranitelnost této skupiny je vysoká. Tento fakt si velká část společností uvědomuje a nastavuje své procesy tak, aby tato rizika minimalizovali na co nejnižší možnou úroveň.

5.3.1 Definování uživatele

Pod pojmem firemního uživatele si můžeme představit libovolného zaměstnance společnosti, který ke své práci využívá moderní mobilní zařízení a který pracuje s citlivými firemními údaji. Moderní mobilní zařízení využívá například na vyřizování emailů, komunikaci s kolegy a zároveň může mít v zařízení taktéž nějakého klienta, který mu slouží k přístupu do cloudu a tím pádem k další řadě velmi citlivých údajů.

5.3.2 Rizika

Rizika pro tento typ uživatelů jsou pochopitelně dána tím, k jakým datům přistupují, jak jsou citlivá a samozřejmě jakým způsobem jsou potenciálně zneužitelná. Je rozdíl, zda-li uživatel je

například skladník a své svěřené mobilní zařízení využívá na jednu konkrétní činnost- například jako čtecí zařízeních čárových kódů a nahrávání do interního systému. Tato data, respektive tyto údaje mají určitou váhu pouze směrem do společnosti. Tito uživatelé většinou pracují se zařízeními k těmto činnostem uzpůsobených.

Jiný příklad může být například zaměstnanec personálního oddělení, který v menší, či větší míře pracuje s osobními údaji. Ač spousta společností (většinou velkých společností) má nastavené principy a pravidla s ohledem na GDPR, tak nelze tvrdit, že se tak týká všech. Ztráta těchto údajů má pochopitelně nejen reálnou možnost zneužití (například rodná čísla, čísla dokladů, čísla bankovních spojení apod.), ale pochopitelně to má značný dopad na renomé společnosti ve chvíli, kdy by se informace o úniku těchto dat dostaly na světlo světa.

5.3.3 Doporučená zabezpečení

Základní doporučená nastavení:

Kromě způsobů, které jsou uvedeny v předchozích typech uživatelů, lze přistupovat k firemním uživatelům ještě mnoha jinými způsoby. Mnoho, obzvláště větších společností má vlastní IT Security zaměstnance, kteří definují pravidla a principy pro využívání mobilních zařízení. Mezi ně může patřit například:

1. Školení zaměstnanců - Poskytujte školení zaměstnancům ohledně bezpečného používání firemních mobilních zařízení a upozorňujte je na nejnovější hrozby týkající se kybernetické bezpečnosti. Pomůže zaměstnancům rozumět rizikům a udržovat firemní mobilní zařízení bezpečná. Na osvětu uživatelů se v rámci vnitřních školení spousta firem soustředí.
2. Používání bezpečného připojení k síti. Ujistěte se, že firemní mobilní zařízení jsou připojena k bezpečné síti s dostatečnou šifrovací ochranou. To pomůže zabránit úniku citlivých informací a chránit zařízení před útoky z venku. V rámci vnitrofiremního používání vyhraďte pro mobilní zařízení speciální sítě a nadefinujte rozsahy těchto sítí. Běžným mobilním telefonům zabraňte v rámci rozsahu přístup do vnitřní sítě. Jednoúčelové mobilní zařízení (například tablety pro práci ve skladech…) naopak nepouštějte do internetu.
3. Používejte vzdálenou správu mobilních zařízení. Tato správa umožňuje nasazení velké řady bezpečnostních principů. Mezi nejpoužívanější pak můžeme řadit například.
    a. Omezení instalací aplikací, které zakáže instalaci z neověřených zdrojů, nebo které zakáží instalaci aplikace, která není schválená.

b. Vzdálené vymazání dat, jakožto funkcionalita, která zabrání ztrátě a případnému zneužití dat v případě odcizení, nebo ztráty zařízení.

c. Omezení používání určitých funkcí se hodí obzvláště pro zařízení, která mezi sebou zaměstnanci sdílí nebo jsou využívány na jednu konkrétní činnost v rámci společnosti. Například čtečky pro načítání.

Pokročilá – volitelná zabezpečení:

1. Šifrování dat. Šifrování dat pomocí specializovaných nástrojů pomůže ochránit citlivá firemní data v případě ztráty nebo krádeže zařízení.
2. Vzdálené mazání dat. Opět se jedná o specializovaný nástroj nebo o vlastnost systému, které umožní smazání všech dat v zařízení. Vzdálené mazání vychází z teze, že pro společnosti jsou data na zařízení cennější, než zařízení samotné.

5.4 Zabezpečení systému VIP

Poslední modelový příklad zabezpečení jsme vydefinovali VIP.

5.4.1 Definování uživatele

Pod pojmem VIP si lze představit jakéhokoliv uživatele, pro kterého případné napadení systému a ztráta dat může znamenat významné následky nejen pro něho samotného, ale i například pro společnost pro kterou pracuje, nebo pro ně samotné. Na tyto druhy uživatelů se můžeme dívat několika směry. První směr jsou vysocí manažeři a ředitelé významných společností, které jsou například špičky ve svých oborech a v rámci své práce pracují tito lidé s opravdu velmi citlivými údaji. Za další kategorii můžeme považovat obecně známé osobnosti. Pro ně například únik citlivých informací může způsobit závažné ohrožení profesní kariéry a svého renomé. Samostatnou kategorií v této skupině mohou státní představitelé. O zabezpečení jejich zařízení můžeme jen spekulovat, neboť to spadá do kategorie tajných informací a nejsou pro to volně dostupná relevantní data. Přesto se pokusíme i na tuto otázku odpovědět.

5.4.2 Rizika

Rizika pro daného uživatele jsou v obecné rovině úplně stejná, jako pro běžného uživatele nebo pro firemního uživatele. Podstatný rozdíl je však v rozsahu dopadu, pokud by dané zařízení bylo napadeno, případně by došlo k úniku dat a jejich následnému zneužití. Na druhou stranu

tito lidé jsou obecně velmi zodpovědní v práci se svými zařízeními a není pro ně problém do těchto zařízení investovat nemalé částky za specializovaný bezpečnostní software a nástroje. Zároveň z podstaty jsou tito lidé daleko více odolní například vůči nástrahám phishingu.

5.4.3 Doporučená zabezpečení

Základní doporučená zabezpečení:

V rámci zabezpečení můžeme vycházet z již výše psaných doporučení pro jiné kategorie uživatelů. V případě V.I .P uživatele jsou ke zvážení ještě tyto principy.

1. Používání VPN, která ochrání a umožní zabezpečený přenos dat a ochranu proti potenciální špionáži.
2. Zcela vynechat používání veřejných, případně předem neprověřených bezdrátových sítí a to i například v rámci zahraničních cest, kde poplatky za využívání mobilních dat mohou být vysoké, nicméně tyto sítě můžeme považovat obecně za bezpečné.
3. Mít nastavený svůj systém nebo minimálně aplikace tak, aby zařízení šlo na dálku zablokovat, dohledat nebo smazat.
4. Zatímco u běžných uživatelů zmiňujeme šifrování dat jako možnou pokročilou ochranu, u V.I .P uživatele to lze považovat za standard.

Pokročilá – volitelná zabezpečení:

1. Mít více zařízení. Například v případě vysoce postaveného manažera velké společnosti striktně oddělit používání svých zařízení. Jedno zařízení si ponechat čistě pro pracovní účely s minimem aplikací a omezením se činností na něm výhradně pro pracovní účely a druhé pro soukromé účely.

V rámci zařízení pro představitele státu lze předpokládat využívání speciálně navrženého zařízení, s šifrovaným systémem a hardwarovými klíči. Tato zařízení mají zcela jistě pokročilé funkce dohledání těchto a v případě krizových situací pokročilé možnosti vzdálené správy. Další předpokládaný způsob zabezpečení spočívá již mimo dané zařízení. S vysokou mírou pravděpodobnosti tato zařízení využívají soukromé sítě. Tyto sítě samy o sobě disponují pokročilým zabezpečením a do těchto sítí se mohou připojovat pouze předem autorizovaná zařízení.

Zabezpečení těchto zařízení, obzvláště v dnešní době, kdy probíhají mezi různými národy informační války a tradiční válčení se ve velké části přesouvá do kyberprostoru, je extrémně důležité. Existují celé instituce, které se zabývají kybernetickou bezpečností jednotlivých zemí.

V rámci České republiky tyto služby pro stát zařizuje NÚKIB spadající pod ministerstvo vnitra. V rámci agendy tohoto ústavu rozhodně spadá i definování pravidel a směrnic pro ochranu zařízení představitelů státu a významných státních institucí.

6 NÁSTROJE PRO ZVÝŠENÍ BEZPEČNOSTI

V rámci ochrany jednotlivých uživatelů byla zmíněna spousta různých mechanismů a i aplikací třetích stran v obecné rovině, které mohou vést ke zvýšení bezpečnosti samotného zařízení. Nyní se podíváme na konkrétní aplikace, které mohou zvýšení bezpečnosti zařídit.

6.1 Bezpečnostní aplikace

Na trhu je velká řada aplikací od různých výrobců, které mohou chránit zařízení proti malware a dalším druhům hrozeb. Nicméně tyto aplikace neslouží jen a pouze jako prevence vůči těmto hrozbám. Tyto aplikace jsou jakýmsi bezpečnostním balíčkem pro ochranu moderního mobilního zařízení. Aplikace lze rozdělit do několika kategorií ať už podle operačního systému, tak i dle toho, jestli se jedná o placenou službu, nebo je aplikace nabízena zdarma.

6.2 Aplikace pro iOS

Ač se bezpečnost a funkcionality systému iOS obecně považují za velmi bezpečné a riziko jakéhokoliv útoku na tato zařízení jsou nízká, nejsou stoprocentní. I z toho důvodu se vyvíjejí aplikace pro lepší zabezpečení zařízení na tomto systému.

6.2.1 Aplikace pro iOS zdarma

V rámci zabezpečení iOS zařízení zdarma lze doporučit Avira Free Mobile Security for iOS.

Tato aplikace poskytuje zdarma pravděpodobně nejvíce funkcionalit oproti konkurentům. Mezi ně patří například VPN s denním limitem, ochrana proti krádeži, skener sítě, analyzátor zařízení, správce úložiště fotografií, zálohování kontaktů, blokování hovorů aj. Všechny tyto funkce jsou uživatelsky přívětivé a je schopen je nastavit a dále s nimi pracovat prakticky jakýkoliv uživatel. Jedinou nevýhodou, kterou lze spatřit je nepodporovaná čeština.

6.2.2 Aplikace pro iOS placená

V rámci placeného zabezpečení iOS zařízení lze doporučit aplikaci Norton Mobile Security pro systém iOS.

Jak již bylo zmíněno, tak tato aplikace není zdarma, ale jedná se o placenou službu. Nicméně Norton nabízí 60denní záruku vrácení peněž v případě ročního předplatného. To činí 575,- korun na rok přímo přes web společnosti. Jedná se o licenci pro jedno zařízení.

Norton Mobile Security pro systém iOS nabízí pokročilé služby v zabezpečení WI-FI sítě, zabezpečení internetu, čímž je myšlena primárně ochrana procházení webu. Dále nabízí VPN s

neomezeným denním tokem dat a dále například pokročilý monitoring krádeže identity využívající technologie LifeLock.

6.3 Aplikace pro Android

Bezpečnost systému Android je obecně na nižší úrovni, než systému iOS. I z toho důvodu jsou aplikace třetích stran pro vyšší zabezpečení hojněji používány, než v případě iOS. V rámci Androidu se při doporučování aplikací zdarma soustředíme především na výběr aplikací, které mají velmi kladné hodnocení v oblasti detekce malware, což je i patrně největší slabina a zároveň riziko pro daná zařízení s tímto systémem

6.3.1 Aplikace pro Android zdarma

V rámci zabezpečení iOS zařízení zdarma lze doporučit aplikaci ESET Mobile Security pro Android.

V rámci bezplatné verze se uživateli dostane velmi slušných služeb. Především se jedná o bezplatný antivirus, který chrání zařízení pomocí technologie nod32. Antimalware ochrana běží na pozadí a příliš ani nesnižuje samotný výkon zařízení a kapacitu baterie. Nabízí ochranu před viry v reálném čase, má uživatelsky přívětivý report zabezpečení a historii aktivit.

6.3.2 Aplikace pro Android placená

V rámci placeného zabezpečení Android zařízení lze doporučit aplikaci Malwarebytes Mobile Security

Jak bylo zmíněno v úvodu, v rámci zařízení Android primárně cílíme na ochranu proti malware a aplikace Malwarebytes je v tomto hledisku velmi oceňována. Kromě této primární funkcionality aplikace, která dokáže například díky rychlosti odhalit ransomware dříve, než začne kryptovat obsah zařízení, tak nabízí i funkce bezpečného prohlížení internetu, bezpečnostní audit aplikací aj. V rámci kombinace s Privacy VPN pak nabízí Malwarebytes opravdu komplexní zabezpečení pro mobilní zařízení. Předplatné stojí 5 $ na měsíc a aplikace není česká. Na druhou stranu její UI je velmi zdařilé a přehledné.

6.4 Aplikace pro Windows

Vzhledem ke složitosti vývoje malware cílí útočníci především na nejmasivněji používané systémy. Tím je, pokud se v tuto chvíli nebavíme pouze o mobilních zařízení, ale o všech zařízení, systém Windows.

6.4.1 Aplikace pro Windows zdarma

V rámci zabezpečení Windows zařízení zdarma lze doporučit Microsoft Defender.

Jedná se o aplikaci přímo od společnosti Microsoft a v poslední době se dočkala celkem zajímavých vylepšení, které nenáročné uživatele toužící po ochraně zdarma uspokojí. Nabízí detekci hrozeb v reálném čase, ochranu firewallem, cloudovou knihovnu antivirové ochrany aj. Další významné plus je možnost využívat toto zabezpečení s dalším antivirovým programem, aniž by se vzájemně narušovaly.

6.4.2 Aplikace pro Windows placená

V rámci placeného zabezpečení Windows zařízení lze doporučit Kaspersky Internet Security.

Placená verze, jejíž roční předplatné pro jedno zařízení je cca 600,- Kč disponuje velmi pokročilou antivirovou ochranou v reálném čase, ochranou proti phishingu, zabezpečením plateb, blokování reklam, ochranou prohlížení na internetu a například blokováním nevhodného obsahu pro děti. Tato placená verze disponuje i VPN o denním datovém limitu 300MB. Ač například denní datový limit nabízejí konkurenční produkty vyšší, je tato verze Kaspersky Internet Security v poměru cena/ výkon opravdu špička.

ZÁVĚR

V rámci této bakalářské práce byli čtenáři v první kapitole seznámeni se všeobecně známými pojmy ohledně informační bezpečnosti. Seznámení s těmito pojmy je velmi důležité pro pochopení fungování samotného zabezpečení a z důvodů pochopení těchto mechanismů v širším pohledu a měřítku. V další kapitole dochází k seznámení se zařízeními v dnešní době nejčastěji používanými. Byly detailně popsány modely, které pomáhaly utvářet trend moderních mobilních zařízení až do dnešní doby. Vzhledem k současnému rozpoložení trhu se tato kapitola orientovala především na zařízení iPhone a různá zařízení s operačním systémem Android, které nelze jednoznačně označkovat.

Zatímco předcházející kapitola byla zaměřena především na vývoj hardwarové stránky jednotlivých zařízení, v další kapitole jsme se pak podívali na vývoj samotných systémů. Vzhledem k obsáhlosti tohoto tématu bylo nutné zkrátit popis jednotlivých systémů především na jejich bezpečnostní prvky a mechanismy, se kterými postupně vývojáři přicházeli. Tato kapitola může představovat jakousi časovou osu vývoje bezpečnostních mechanismů, které jsou přímo součástí daných systémů. V rámci této bakalářské práce jsme se zabývali především systémy, které jsou momentálně pro mobilní zařízení nejpoužívanější a to systémy iOS, Android a Windows.

V posledním bodě v rámci této kapitoly došlo na základě základních vlastností k porovnání mezi systémy Android a iOS opět s důrazem na bezpečnost těchto systémů.

Další kapitola nám představuje nejčastější hrozby, se kterými se mohou dnešní uživatelé setkat. Na toto téma volně pak navazuje praktická část, kde na příkladech čtyřech typů uživatelů jsou představeny standardy, kterými by se měli před riziky vyplývající z předchozí kapitoly uživatelé, případně správci daných zařízení bránit. V tomto směru jsme nezacházeli do přehnaných detailů, ale spíše popisovali, jakými směry se lze vydat. Tyto směry jsme rozdělili do dvou úrovní. Jako první je taková úroveň, která by měla být minimálním standardem pro dané typy uživatelů. Druhá by se dala považovat za kategorii „nice to have“ a poskytuje uživatelům vzhledem k jejich povaze už výrazně vyšší stupeň zabezpečení.

V poslední kapitole došlo k představení možností pro zabezpečení moderních mobilních zařízení, pomocí aplikací třetích stran, které poskytují uživatelům široké spektrum zabezpečení jak proti hrozbám samotným, tak i ochranu těchto zařízení při jejich používání. I toto téma jsme rozdělili podle operačních systémů a dále dle toho, jestli je software zdarma a jaké funkce tento software nabízí, nebo zda-li se jedná o placený software a jaké funkce má, třeba i v přímém porovnání se softwarem zdarma.

Cílem celé práce je to, aby čtenář získal ucelenou představu o moderních mobilních zařízení, jejich operačních systémech, aby se dokázal orientovat v základních bezpečnostních pojmech, aby znal rizika dnešní doby a aby dokázal vyhodnotit optimální možnosti ochrany těchto zařízení.

POUŽITÁ LITERATURA

[1] PŘIBYL, Jiří a Jindřich KODL. Ochrana dat v informatice. Praha: České vysoké učení technické, 1996. ISBN 80-01-01664-1 .

[2] ZELENKA, Josef. Ochrana dat: kryptologie. Hradec Králové: Gaudeamus, 2003. ISBN 80-7041-737-4 .

[3] DOBDA, Luboš. Ochrana dat v informačních systémech. Praha: Grada, 1998. ISBN 80-169-479-7 .

[4] DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9 .

[5] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z .s .p .o ., 2019. CZ.NIC. ISBN 978-80-88168-31-7 .

[6] KLEMENS, Guy. The cellphone: the history and technology of the gadget that changed the world. Jefferson: McFarland, 2010. ISBN 978-0786458677.

[7] MAJEED, Ahmad. Smartphone: Mobile Revolution at the Crossroads of Communications, Computing and Consumer Electronics. CreateSpace Independent Publishing Platform, 2011. ISBN 978-1461033158

[8] MILLER, Daniel. Global Smartphone. UCL Press. 2021. ISBN 1787359638

[9] DOZ, Yves a Keeley WILSON. Vyzvánění: vzestup a pád mobilních telefonů NOKIA. Přeložil Jaroslav KONVIČKA. Praha: Dobrovský, 2021. Via. ISBN 978-80-7585-011-9 .

[10] GRIC, Kamil. Mobilní telefony. [Brno]: UNIS Publishing, 2000. PC World edition. ISBN 80-86097-55-2 .

[11] The History of Mobile Phone Technology - Redorbit. Home - Redorbit [online]. Dostupné z : https://www.redorbit.com/reference/the-history-of-mobile-phone-technology/

[12] RETROBRICK - the home of vintage and rare mobile phones. Wayback Machine [online]. Dostupné z : https://web.archive.org/web/20061022171936/http://www.retrobrick.com/moto8000.html

[13] POGUE, David. IPhone: průvodce s tipy a triky. Brno: Computer Press, 2008. ISBN 9788025121887.

[14] JURICK, David, Adam STOLARZ a Damien STOLARZ. Velká kniha tipů a triků pro iPhone. Brno: Computer Press, 2009. ISBN 9788025126455.

[15] ZANDL, Patrick. Apple: cesta k mobilům. Praha: Mladá fronta, 2012. ISBN 978-80-204-2641-3 .

[16] LACKO, Ľuboslav. Vývoj aplikací pro iOS. Přeložil Martin HERODEK. Brno: Computer Press, 2018. ISBN 978-80-251-4942-3 .

[17] MERCHANT, Brian. The One Device: The Secret History of the iPhone. Back Bay Books, 2018. ISBN 978-0 -316-54624-9 .

[18] HOENA, Blake. Cell Phones and Smartphones: A Graphic History (Amazing Inventions). Graphic Universe, 2021. ISBN 978-1541581494

[19] GOOKIN, Dan. Android. For Dummies, 2nd Edition, 2020. ISBN 978-1119711353

[20] BERNSTEIN, James. Android Smartphones Made Easy: The Beginners Guide Made For Beginners: 10 (Computers Made Easy). Independently published, 2019. ISBN 978-1086026832

[21] ELENKOV, Nikolay. Android Security Internals: An In-Depth Guide to Android's Security Architecture. San Francisco: No Strach Press, 2014. ISBN 9781593275815.

[22] FRIED, Stephen. Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World. United Kingdon: Taylor and Francis lnc, 2010. ISBN 9781439820162.

[23] LACKO, Ľuboslav : Mistrovství- Android: Kompletní průvodce vývojáře. Brno: Computer Press, 2017. ISBN 9788025148754.

[24] KRÁL, Mojmír. Bezpečný internet: Chraňte sebe i svůj počítač. Praha: Grada, 2015. ISBN 9788024754536.

[25] KIM, Carol. Are Smartphones a Threat to Privacy? (Smartphones and Society). Referencepoint Press, 2020. ISBN 978-1682829394

[26] MAISNER, Martin. Základy softwarového práva. Praha: Wolters Kluwer Česká republika, 2011. ISBN 9788073579647.

[27] THIEL, David. iOS Application Security. San Francisco: No Strach Press, 2016. ISBN 9781593276010.

[28] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze, 2012. ISBN 978-80-7251-378-9 .

[29] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n @ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3 .

[30] The HUAWEI ban: Everything you need to know - Android Authority. Android Authority: Tech Reviews, News, Buyer's Guides, Deals, How-To [online]. Authority Media. All rights reserved.. Dostupné z : https://www.androidauthority.com/huawei-google-android-ban-988382/

[31] ZTE and the U .S .: Everything You Need to Know | Digital Trends. Digital Trends | Tech News, Reviews, Deals, and How-To's [online]. Dostupné z : https://www.digitaltrends.com/mobile/commerce-bans-zte-from-exporting-technology-from-the-us/

[32] CAMERON, Rob. Pro Windows Phone 7 Development. Springer A Pr Trade. ISBN 9781430232193

[33] POSEY, Brien. My Windows Phone 8 . Pearson Education. ISBN 0789748533

[34] TUMBARELLO, Matt. Mastering Windows Security and Hardening - Second Edition. Packt Publishing. ISBN 180323654X

[35] MIROSHNIKOV, Andrei. Windows Security Monitoring. John Wiley & Sons Inc. ISBN 9781119390640

[36] EVANS, Lester. Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social En. Independently Published. ISBN 1791553583

[37] MITNICK, Kevin a William SIMON. Umění klamu. Gliwice: Helion, 2003. ISBN 9788373612105.

[38] SHOSTACK, Adam. Threat Modeling: Designing for Security. Wiley; 1st edition. ISBN 978-1118809990

[39] Just a moment.... Just a moment... [online]. Dostupné z : https://www.pmi.org/learning/library/top-50-projects-dynatac-8000x-11725

[40] Deset klíčových Nokií, aneb konec jedné legendy - 3 . kapitola – MobilMania.cz. MobilMania.cz – O mobilech víme vše [online]. Copyright © 2023 Copyright CZECH NEWS CENTER a .s . a dodavatelé obsahu.. Dostupné z : https://mobilmania.zive.cz/clanky/deset-klicovych-nokii-aneb-konec-jedne-legendy/1992---startuje-era-gsm/sc-3 -a -1324718-ch-1059694/default.aspx

[41] IBM Simon, World's First Smartphone, Enters Science Museum. Silicon UK | TECHNOLOGY POWERING BUSINESS [online]. Copyright © Copyright 2023 All rights reserved. Part of NetMediaEurope.. Dostupné z :

https://www.silicon.co.uk/workspace/first-smartphone-ibm-simon-enters-science-museum-150984

[42] Idnes.cz [online]. Dostupné z : http://www.idnes.cz/mobil/telefony/iphone-prvni-generace-2007-retro-recenze-apple.A170628_203854_iphone_ada

[43] Alza.cz. Alza.cz [online]. Dostupné z : https://www.alza.cz/iphone-14-pro-max?dq=7403225

[44] Wholesale HTC Dream G1 Black T -Mobile Unlocked Cell Phone. Buy Wholesale Cell Phones & Smartphones Online [online]. Copyright © 2020 All rights reserved. [cit. 19.03.2023]. Dostupné z : https://www.todayscloseout.com/Wholesale-p /htc-g1-black-rb-a .htm

[45] Alza.cz. Alza.cz [online]. Dostupné z : https://www.alza.cz/samsung-galaxy-z -fold-4 ?dq=7327222&o =1

PŘÍLOHY

Účel příloh

Přílohy této bakalářské práce rozšiřují informace a skutečnosti, které jsou popsány v hlavní části práce samotné. Příloha 1 seznamuje s vývojem mobilních zařízení až do doby, kdy o nich lze říci, že se jedná o moderní mobilní zařízení tzn. mapuje situaci vývoje do představení systému iOS a Android. Druhá příloha se pro změnu týká praktické části bakalářské práce a představuje nasazení aplikace třetí strany na zařízení iOS.

Příloha 1:

Příloha č. 1 rozšiřuje historický vývoj mobilních zařízení a dalo by se říci, že skutečnosti v ní popsané předchází kapitole 2.

Počátky mobilních telefonů

První mobilní telefony vznikly v 50. letech a z počátku se jednalo především o součást vybavení osobních automobilů. Tyto telefony však byly vázány čistě k automobilu, takže se spíše jednalo o pojízdné pevné linky. První přenosné telefony se začaly objevovat až v průběhu 70. let. Tyto telefony však byly velmi velké a na tehdejší dobu velmi drahé, co se týká samotné pořizovací ceny, tak i následného provozu. I z toho důvodu se zdálo, že se mobilní telefony nedočkají masivního rozšíření. Tato teze přetrvávala ještě v 80. letech. Ještě v průběhu vývoje technologie GSM se nepředpokládalo takové rozšíření, jakého jsme byli svědky v následujících obdobích.

[6][7]

První mobilní telefony

Za první sériově vyráběný komerční telefon lze považovat Motorolu DynaTac 8000x. Vývoj tohoto mobilního telefonu trval více než 10 let a na trh byl po všech procedurálních náležitostech uveden v roce 1984. Jeho tehdejší cena byla přibližně 4000$, což je částka, která zhruba odpovídá dnešním 12000$. Tento telefon byl velký zhruba 25 centimetrů a vážil 1 kg. Telefon po desetihodinovém nabíjení umožnil provést půlhodinový telefonát. Disponoval LED displejem a umožňoval vybrat jedno ze třiceti telefonních čísel v seznamu. V rámci zabezpečení telefon disponoval pouze zámkem klávesnice. Jinak stejně jako všechny tehdejší telefony disponoval spíše možností zabezpečením fyzického charakteru (například možností uzamčení v kufru).

Obrázek přílohy 1 č.1 - Motorola DynaTac 8000x

Zdroj: [39]

Druhý telefon, který v tomto bodě zmíníme, neboť byl v určitém slova smyslu revoluční, je Nokia 1011. Tento telefon z roku 1992 byl prvním masově vyráběným telefonem, který využíval standardu GSM, který se v rozšířené formě využívá do dnešní doby. Telefon měl monochromatický displej a mohlo se do něj uložit 99 čísel. Tento telefon byl zároveň už technologicky schopen přijímat a odesílat SMS, ač se rozvoj této technologie proslavil spíše až u jeho nástupce Nokia 2110. V rámci zabezpečení Nokia 1011 disponovala zámkem klávesnice.

Obrázek přílohy 1 č.2 - Nokia 1011

Zdroj:[40]

Pokud lze o některém telefonu z tohoto období tvrdit, že svojí dobu velmi výrazně předběhl, pak je to telefon IBM Simon, který se dá považovat za první smartphone vůbec, ačkoliv v době jeho vzniku v roce 1994 toto označení nebylo ještě definované. Kromě funkcí, tehdy již pro telefony běžné uměl Simon na tehdejší dobu opravdu revoluční věci. Zařízení umělo odesílat a

přijímat emaily a faxy a disponovalo na tehdejší dobu i jiným nebývalým softwarovým vybavením. Například plánovačem schůzek, poznámkovým blokem, kalkulačkou aj. Telefon disponoval operačním systémem Datalight ROM-DOS a dotykovým LCD displejem. Masové rozšíření však velmi výrazně brzdila slabá kapacita baterie, která vydržela v provozu pouze hodinu, takže velmi často se se zařízením pracovalo v dokovací stanici a velké rozměry tohoto zařízení. Mnoho zákazníků v tu dobu dávalo přednost spíše rozměrově menším a cenově dostupnějším vyklápěcím modelům, což vedlo k zániku IBM Simon.

Obrázek přílohy 1 č.3 - IBM Simon

Zdroj:[41]

Doba byla tehdy velmi dynamická v tom slova smyslu, že se jednotliví výrobci předháněli v novinkách, které do svých telefonů uvedou, tudíž každou chvíli docházelo k technologickým pokrokům.

V této době byly typické externí antény. V roce 1997 přišel na trh telefon od společnosti Hegenuk s označením GlobalHandy, který jako první externí anténu integroval. Ve stejný rok přišla na trh i legendární Nokia 5110, která sice disponovala externí anténou, ale byl to telefon extrémní odolnosti a výdrže baterie a stal se jedním ze symbolů masivního využívání mobilních telefonů.

O rok později v roce 1998 došlo k dalšímu významnému milníku, kdy byl představen první telefon s barevným displayem a to Siemens S10.

Za další milník lze považovat Nokii 7110, která jako první telefon přišla s WAP prohlížečem umožňujícím připojení k internetu, to se psal rok 1999. Ve stejném roce pro změnu společnost

Samsung přišla s modelem SPH-M100 Uproar, který byl kombinací telefonu a přehrávače MP3 a zároveň to byl první telefon, který pro tento účel vybudoval nadstandardní interní kapacitu- 64MB. Ve stejném roce Nokia představila voděodolný model 5210 a v rámci modelu 3210 přišla s prediktivním textovací službou známou jako T9. Opět v roce 1999 vznikl i Benefon Esc!, což byl pro změnu první komerční telefon, který přišel se službou GPS.

V posledním roce 20. století, v roce 2000 byl vydán jeden z nejikoničtějších telefonů všech dob- Nokia 3310. Tento telefon sám nepřišel s ničím revolučním, spíše využil již objevených vlastností telefonů výše zmiňovaných. Náročnější klientele pak byl představen model Nokia 9210, který nabídl pokročilejší využívání internetu a na něj navázaných služeb. Ve stejném roce byl i představen telefon Sharp J -SH04, který jako první nabídl fotoaparát.

Pokud se máme zmínit o možnosti zabezpečení těchto telefonů, tak nebylo příliš velké. Většina z nich disponovala pouhých zámkem klávesnice, který zabezpečoval zařízení spíše symbolicky proti nechtěnému zmáčknutí klávesnice a tím pádem nevyžádané činnosti. Za největší zabezpečení těchto telefonů proto musíme brát PIN kód od SIM karty.

Tím lze uzavřít kapitolu o prvních mobilních telefonech. Jak můžeme vidět i takto historická zařízení již znala a uměla technologie, se kterými pochopitelně v rozšířenějším slova smyslu pracujeme do dnes.

[6][7][10]

Vývoj zařízení v 21. století

Značný pokrok technologií pokračoval i v novém tisíciletí a hned v roce 2001 byl představen další telefon a to s technologií, která opět přežila do dnešní doby a to technologií Bluetooth. Jednalo se o model Ericsson T39. O rok později byla vydána Nokia 7650, která obsahovala operační systém Symbian, což byl operační systém vyvinut čistě pro telefony Nokia a jednalo se v podstatě o předchůdce dnešních operačních systémů. V následujících letech došlo k masivnímu rozšíření 3G sítě a telefony se spíše zdokonalovaly, aniž bychom byli svědky nějakých přehnaných technologických novinek. Telefony postupně získávaly větší vnitřní paměť, zlepšovaly se fotoaparáty aj. Nicméně vývoj lehce přešlapoval na místě.

Toto přešlapování na místě však v dalších letech vytrhlo několik opravdu velmi významných událostí, které udávají trend prakticky až do dnešní doby. Toto období lze shrnout zjednodušeně do třech kapitol, kdy každá kapitola popisuje směr, kterým se tehdy vývoj mobilních zařízení vydal a každý je spjatý se specifickým operačním systémem. Jedná se o představení zařízení iOS, Android a Windows Phone, o kterých se zmiňuji samostatně v hlavní části této bakalářské práce.

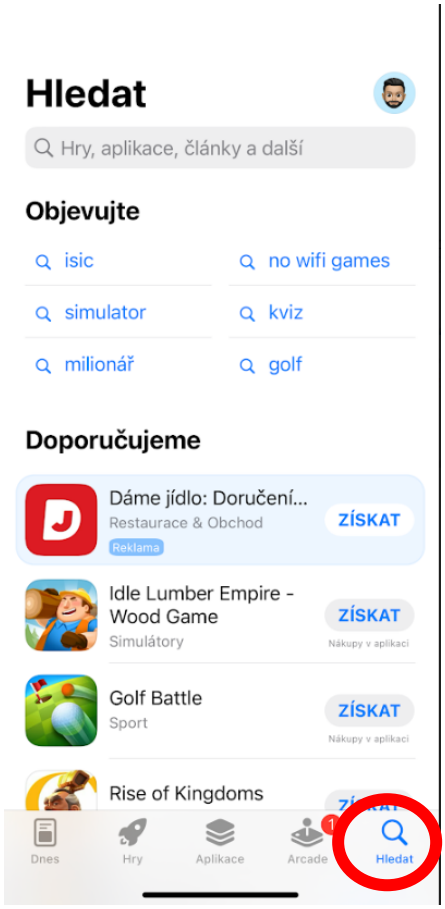
[8][9][11][12]

Příloha 2

V rámci druhé přílohy této bakalářské práce si ukážeme prakticky nasazení bezplatné aplikace Avira Free Mobile Security for iOS na zařízení iPhone11 Pro. Tento postup autor zdokumentuje a vyzkouší na svém vlastním zařízení. Detailně, včetně obrazové dokumentace pořizované formou výstřižků obrazovky popíše jednotlivé kroky v rámci nasazení této aplikace a představí její funkcionality. Ač autor představuje řešení pro tuto konkrétní aplikaci, dá se říci, že velmi podobně je nasazování řešeno i v rámci jiných aplikací. V obecném hledisku se jedná o nasazení aplikace třetí strany pro běžného uživatele a tato příloha rozšiřuje na konkrétním příkladu pokročilé zabezpečení pro běžného uživatele dle kapitoly 5.2.3

Instalace aplikace Avira Free Mobile Security for iOS

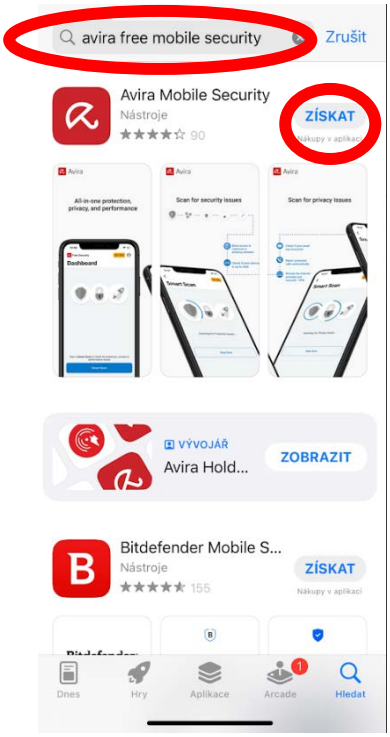
V prvním kroku si spustíme obchod s aplikacemi App Stores a zadáme možnost „Hledat“.



Obrázek přílohy 2 č . 1 – Domovská stránka App Store

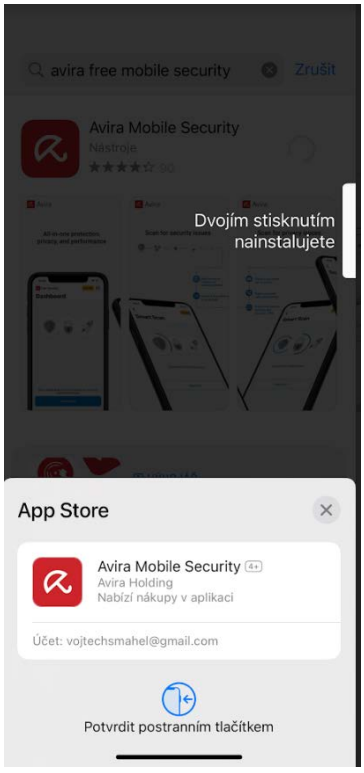
Zdroj: vlastní zpracování

Do pole vyhledávání zadáme název požadované aplikace a klikneme na „hledat“.
Byla nalezena požadovaná aplikace, instalaci do telefonu vyvoláme tím, že zaklikneme „Získat“



Obrázek přílohy 2 č . 2 - Výsledky vyhledávání

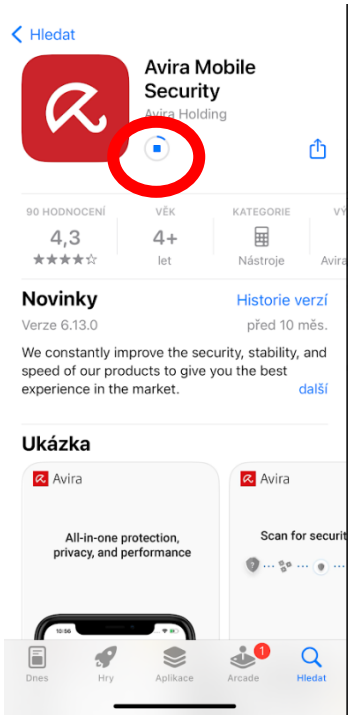
Zdroj: vlastní zpracování



Obrázek přílohy 2 č . 3 - Potvrzení „nákupu“ aplikace

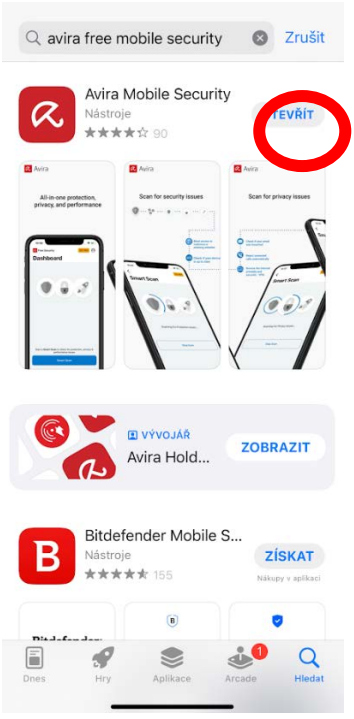
Zdroj: vlastní zpracování

Vzhledem ke způsobu nastavení zabezpečení daného zařízení musí dojít k ověření identity pro tento „nákup“ (myšleno pro i aplikace zdarma). To provedeme dvojím stisknutím bočního tlačítka a autentizací pomocí FaceID.



Obrázek přílohy 2 č . 4 - Průběh instalace aplikace

Zdroj: vlastní zpracování



Obrázek přílohy 2 č . 5 - Aplikace je nainstalována, lze ji spustit

Zdroj: vlastní zpracování

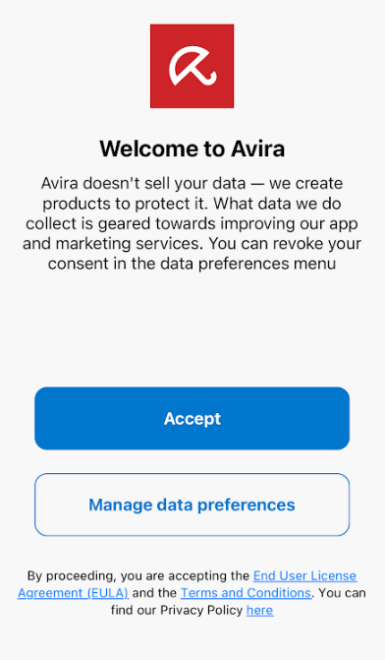
První spuštění aplikace

Po spuštění aplikace dochází k načítání aplikace. Načítání trvá několik málo sekund.

Obrázek přílohy 2 č . 6 - Spouštění aplikace

Zdroj: vlastní zpracování

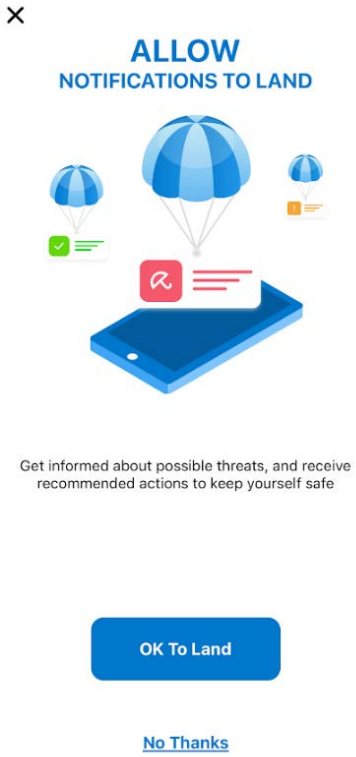
V dalším kroku je okno potvrzení sběru dat pro účely vývoje a licenční podmínky. Lze rozkliknout a zkontrolovat co konkrétně je sbíráno za data během využívání.



Obrázek přílohy 2 č . 7 - Potvrzení akceptování sběru dat

Zdroj: vlastní zpracování

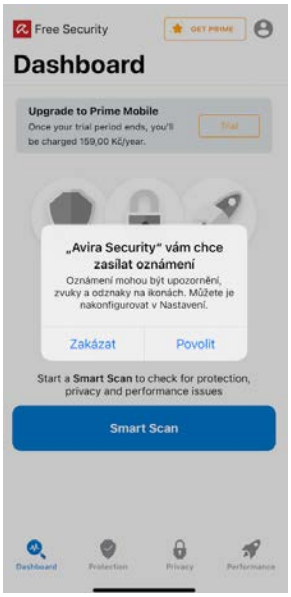
V dalším kroku se nám nabízí možnost, zda-li chceme od Aviry dostávat notifikace (upozornění). Můžeme přijmout, nebo odmítnout. Záleží na volbě uživatele.



Obrázek přílohy 2 č . 8 - Povolení/ zamítnutí notifikací aplikace

Zdroj: vlastní zpracování

Chceme-li tyto notifikace dostávat, budeme v dalším kroku ještě vyzváni systémem k potvrzení přijímání notifikací.

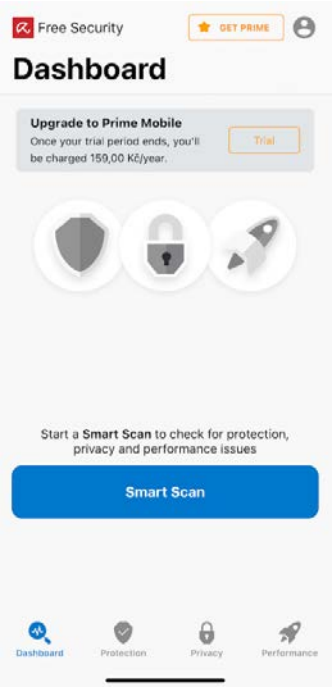


Obrázek přílohy 2 č . 9 - Výzva systému k přijímání notifikací

Zdroj: vlastní zpracování

Aplikace a její funkcionality

Nyní se již dostáváme do aplikace samotné. Po každém spuštění se aplikace dostává do Dashboardu, což můžeme volně nazvat domovskou stránkou aplikace.

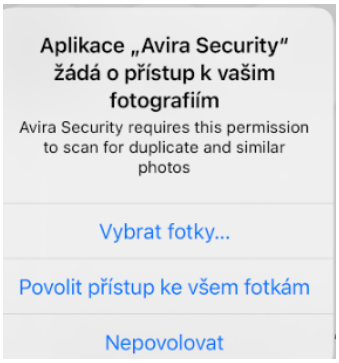


Obrázek přílohy 2 č . 10- Dashboard aplikace Avira

Zdroj: vlastní zpracování

Dashboard ve svém výchozím nastavení nabízí okamžitý „Smart Scan“, který provádí kontrolu zařízení ve třech různých skupinách. Protection- ochrana, Privacy- soukromí a Performance- výkon. Pojďme si ho vyzkoušet.

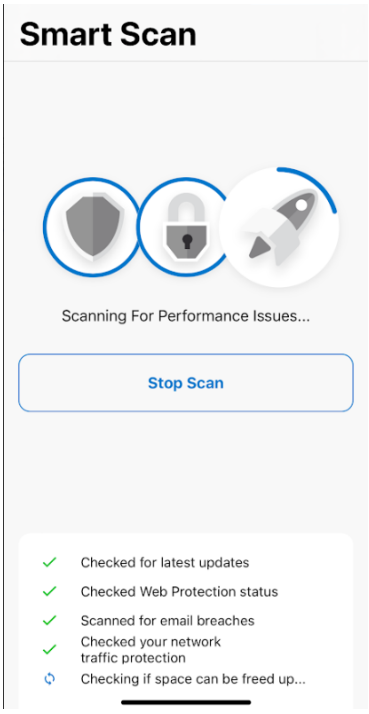
Vzhledem k tomu, že jedna z funkcionalit je prohledávání duplicitních fotografií, jsme vyzváni k povolení aplikace k přístupu k fotografiím. Na podobné hlášky žádosti k přístupu můžeme narážet i v dalších bodech a nastavování. Například funkce Antitheft bude vyžadovat přístup k poloze, Contacts backup ke kontaktům apod.



Obrázek přílohy 2 č . 11- Žádost o přístup

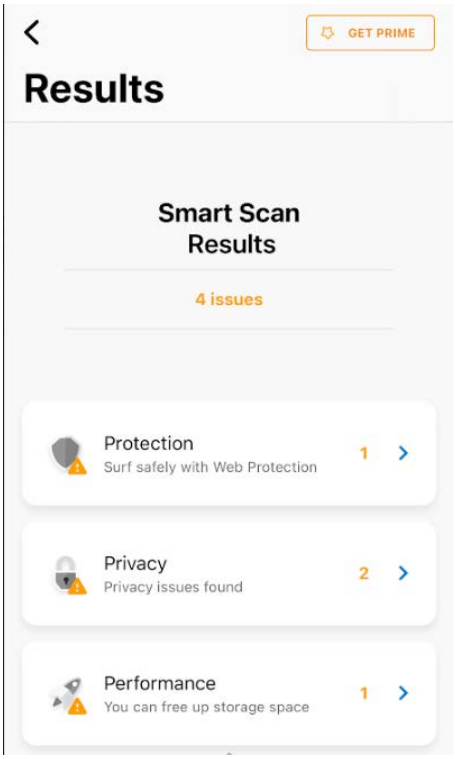
Zdroj: vlastní zpracování

Ač o povolování přístupu toho v rámci této bakalářské práce bylo napsáno mnohé, považujeme aplikaci za bezpečnou a povolujeme přístup ke všem fotkám. Po potvrzení již přichází samotné skenování.



Obrázek přílohy 2 č . 12- Průběh Smart Scan

Zdroj: vlastní zpracování



Obrázek přílohy 2 č . 13- Výsledky

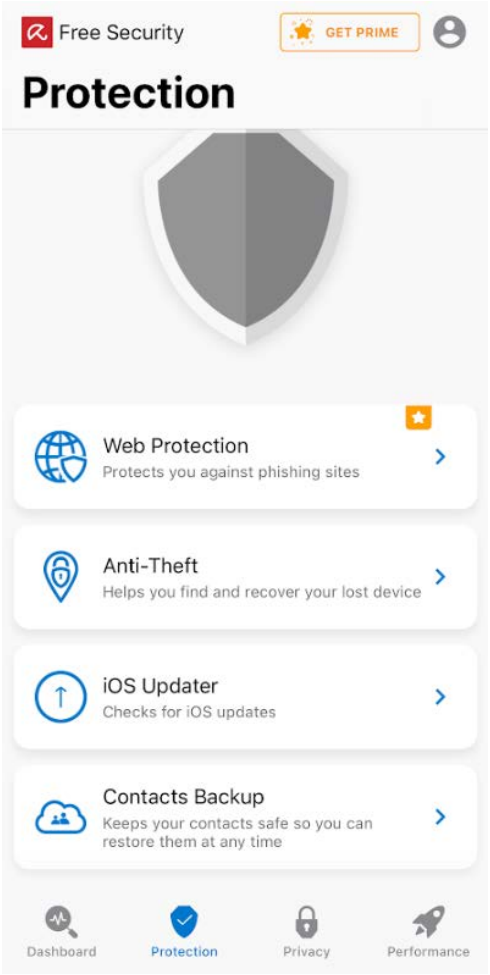
Zdroj: vlastní zpracování

Z výsledku vyplývají 4 problémy, kliknutím na šipku u dané kategorie můžeme zjistit o problému více.

Po rozkliknutí lze zjistit, o jaké problémy se jedná. Zjistili jsme, že se nejedná o žádný závažný bezpečnostní problém a tyto problémy lze odkliknout ignorováním. Většina výsledků nás odkazují na vyšší stupeň zabezpečení, které jsou již v placené verzi.

Nyní se lze vrátit zpět do Dashboardu a můžeme prozkoumat jednotlivé další funkcionality.

Jako první prozkoumáme kategorii Protection



Obrázek přílohy 2 č . 14- Jednotlivé funkcionality v rámci skupiny Protection

Zdroj: vlastní zpracování

Kategorie Protection nám nabízí 4 různé způsoby možnosti zabezpečení

Web Protection je placená služba a nelze ji nějak více zkoumat.

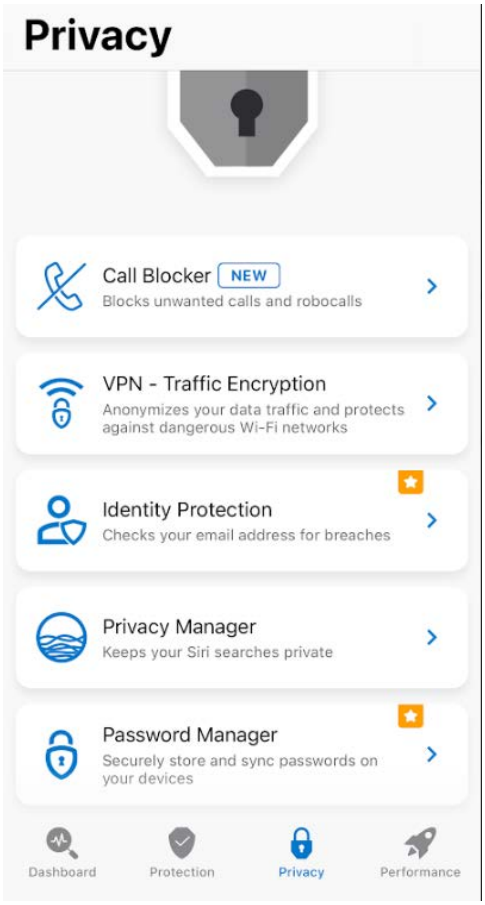
Anti-Theft je funkcionalita, která pomáhá se vyhledáváním ztraceného zařízení.

iOS Updater je funkcionalita, která hlídá aktuálnost systému.

Contacts Backup je funkcionalita, pomocí které je možnost zajistit zálohu kontaktů

Druhá kateogire je Privacy

Tato kategorie nabízí 5 funkcionalit a z toho jsou 3 zdarma.



Obrázek přílohy 2 č . 15- Jednotlivé funkcionality v rámci skupiny Privacy

Zdroj: vlastní zpracování

Call Blocker pomáhá s blokováním nevyžádaných telefonátu, nebo strojových hovorů.

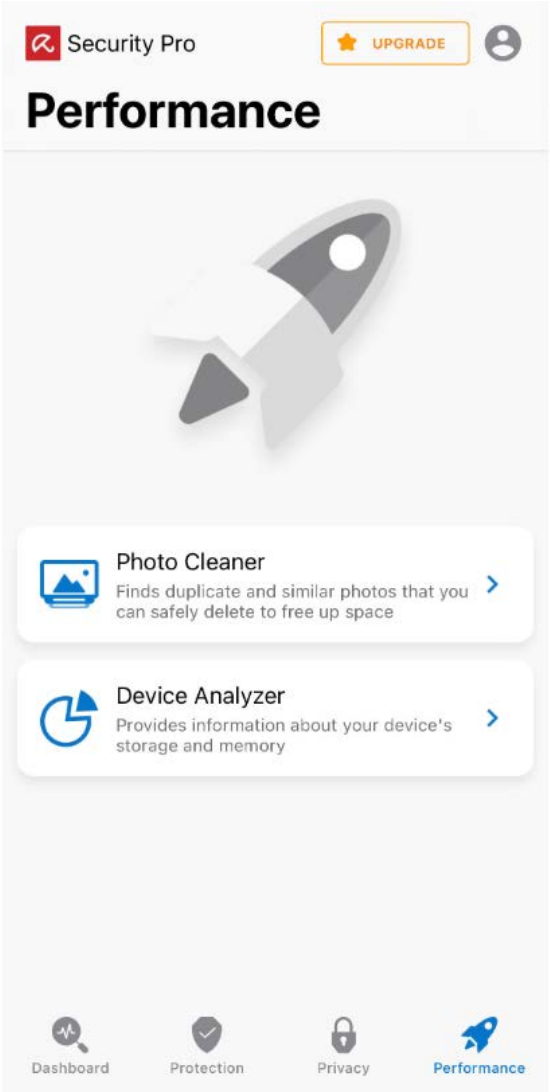
VPN – Traffic Encryption nabízí anonymizování datového toku se zařízením a prostřednictvím toho zvýšenou ochranu připojení. Denní limit ve verzi zdarma je 100MB.

Privacy Manager je funkcionalita, která zajišťuje ochranu vyhledávání pomocí hlasové asistentky Siri.

V rámci kategorie Privacy jsou placená funkcionality Indentity Protection a Password Manager.

Poslední kategorie je Performance, která pomáhá ve zlepšování výkonu zařízení.

Tam se nacházejí dvě kategorie a obě jsou zdarma.



Obrázek přílohy 2 č . 16- Jednotlivé funkcionality v rámci skupiny Performance

Zdroj: vlastní zpracování

Photo Cleaner vyhledává duplicitní fotografie, dokáže je případně smazat a tím dochází k úspoře úložiště v zařízení.

Device Analyzer ukazuje momentální stav úložiště.

Všechny výše psané funkcionality lze prostřednictvím uživatelsky přívětivého prostředí aktivovat a výrazně tak zvýšit zabezpečení svého zařízení.