Analýza bezpečnosti mobilních zařízení se systémem Android

Jakub Němec

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub Němec**
Osobní číslo:	**L16494**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**prezenční**

Téma práce: **Analýza bezpečnosti mobilních zařízení se systémem Android**

Zásady pro vypracování:

1. **Zpracujte rešerši současného stavu vztahující se k dané problematice s důrazem na monografie a analytické materiály.**
2. **Analyzujte bezpečnost vybraných mobilních zařízení s odpovídající verzí operačního systému Android.**
3. **Navrhněte doporučení pro zvýšení bezpečnosti těchto zařízení.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] JIRÁSEK Petr, NOVÁK Luděk a POŽÁR, Josef. Výkladový slovník Kybernetické bezpečnosti: Třetí doplněné a upravené vydání. 3. Praha: Policejní akademie České republiky v Praze, 2015. ISBN 978-80-7251-436-6.

[2] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[3] BUREŠ Miroslav, Miroslav RENDA, Michal DOLEŽEL, Peter SVOBODA, Zdeněk GRÖSSL, Martin KOMÁREK, Ondřej MACEK a Radoslav MLYNÁŘ. Efektivní testování softwaru: klíčové otázky pro efektivitu testovacího procesu. Praha: Grada, 2016. Profesionál. ISBN 978-80-247-5594-6.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.
③

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Jakub Němec

.....
podpis studenta

ABSTRAKT

Tato práce je rozdělena na část teoretickou a praktickou. Teoretická část práce se zabývá vysvětlením základních pojmů a seznámením se s legislativou vztaženou na tuto problematiku. Dále se zabývá popisem operačního systému Android a jeho dostupností na mobilních zařízeních. Poslední kapitolu teoretické práce tvoří vyjmenování a popis jednotlivých prvků, které chrání mobilní zařízení se systémem Android. Praktická část se věnuje především samotné analýze bezpečnosti mobilních zařízení se systémem Android. Na začátku praktické části práce je definováno, jaké informace jsou umístěné v mobilním zařízení a následně jsou popsány možné hrozby, které tyto informace mohou ohrozit. Následně je provedeno multikriteriální hodnocení pro zjištění nejlepšího způsobu zabezpečení pomocí zámků obrazovky. Na nejlepší z těchto druhů zámků je provedena SWOT analýza a dále je zde provedena analýza přístupu uživatelů mobilních zařízení s operačním systémem Android, a to za pomoci dotazníkového šetření. Všechny tyto analýzy jsou vyhodnoceny a na konec jsou navrženy doporučení pro zvýšení bezpečnosti těchto zařízení.

Klíčová slova: android, bezpečnost, informace, mobilní, odcizení, osobní, systém, útok, zařízení

ABSTRACT

This thesis is divided into theoretical and practical part. The theoretical part deals with the explanation of basic terms and with the legislation related to this issue. It also describes the Android operating system and its availability on mobile devices. The last chapter of the theoretical work includes the enumeration and description of the elements that protect the Android mobile device. The practical part deals mainly with the analysis of the security of Android mobile devices. At the beginning of the practical part is defined what information is placed on the mobile device and then the possible threats that these assets can threaten are described. Subsequently, a multicriterial assessment is performed to determine the best way of securing using the screen locks. A SWOT analysis is performed on the best of these types of locks, and there is an analysis of the access of users of mobile devices with the Android operating system using a questionnaire survey. All of these analyzes are evaluated and recommendations for improving the safety of these devices are suggested.

Keywords: android, attack, device, information, mobile, personal, security, system, theft

Rád bych poděkoval svému vedoucímu Ing. Petru Svobodovi za cenné rady, jeho ochotu a věnovaný čas. Děkuji Mgr. Miroslavu Sklenářovi za pomoc při anglickém překladu. Za pomoc při gramatické kontrole bych chtěl poděkovat Ing. Renatě Ondrůškové a Mgr. Tomáši Ondrůškovi.

Velké díky patří také mé rodině za možnost studovat a jejich podporu po celou dobu studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V současné době jsou mobilní telefony velkou součásti života většiny lidí. S tím, jak se mobilní telefony vyvíjí, se postupně rozšiřuje i jejich možnost využití. Zatímco dříve mobil sloužil hlavně k volání, dnes slouží velkému množství uživatelů jako pomocník s připojením na internet, bez kterého by se neobešli.

Mobilní systém Android je aktuálně nejpoužívanějším systémem, který je instalován do většiny mobilních telefonů od různých výrobců[1]. Proto je důležité analyzovat jeho bezpečnost a schopnost ochránit citlivá data umístěné na mobilních zařízeních.

Mobilní telefony jsou využívány pro mnohé účely, ať už jako hlavní prostředek pro ukládání dat, jako multimediální zařízení, anebo jako zařízení pro prohlížení obsahu na internetu. Právě z těchto důvodů je již dost často používán místo stolního počítače. Stejně jako na stolní počítač, tak i na mobilní telefon si můžeme ukládat různé důležité, a i osobní informace. Jenže oproti stolnímu počítači může být mobilní telefon lehce odcizen a pro nás důležité informace mohou být zneužity.

Teoretická část se bude věnovat především rešerši vztažných materiálů. Bude objasněno několik základních pojmů, které je potřeba znát pro pochopení této problematiky. Dále budou vypsány legislativní dokumenty, které se vztahují k dané problematice. Na konci teoretické části budou popsány prvky, které mohou zabezpečit mobilní zařízení.

Praktická část se bude věnovat samotné analýze bezpečnosti mobilních zařízení se systémem Android. Jako první budou popsány aktiva, které je potřeba v mobilních zařízeních chránit a také budou vypsány možná rizika, které mohou ohrozit tyto aktiva. Následně bude provedeno multikriteriální hodnocení zámků obrazovky a poté analýza jednoho druhu zabezpečení. Součásti práce je i dotazníkové šetření, týkající se analýzy přístupu uživatelů mobilních zařízení se systémem Android k bezpečnosti informací umístěných v jejích přístrojích. Nakonec bude navrženo několik způsobů, jak zlepšit bezpečnost těchto zařízení.

Cílem této práce je analyzovat bezpečnost mobilních zařízení, které obsahují operační systém Android. Následně doporučit, jakým způsobem se dá tato bezpečnost zlepšit.

[1] Podle serveru IDC, Android najdeme na 86.8 % smartphonů.

I. TEORETICKÁ ČÁST

1 NÁZVOSLOVÍ A LEGISLATIVA

V této kapitole je vysvětleno základní názvosloví a pojmy týkající se mobilních zařízení a jejich bezpečnosti. Dále zde bude zmíněna legislativa týkající se mobilních zařízení a jejich bezpečnosti. Jako poslední je seznámení s národním úřadem pro kybernetickou a informační bezpečnost.

1.1 Základní pojmy

Oblast mobilních zařízení obsahuje několik základních pojmů, které jsou důležité po pochopení řešené problematiky. Proto je důležité si tyto pojmy vysvětlit.

Mobilní zařízení

Jedná se o jakýkoliv elektronický přístroj s vlastním napájení. Nejčastěji je vybaven dotykovým displejem, anebo miniaturní klávesnicí. Často jsou vybaveny možností připojit se na internet.

Informační a komunikační technologie

Skládají se z technologií a nástrojů, které lidi používají ke sdílení, distribuci a sběru informací a ke komunikaci mezi sebou prostřednictvím počítačů, či telefonů nebo propojených počítačových sítí. [1]

Bezpečnost

„Stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.“ [4]

Informační bezpečnost

Jedná se ochranu informací ve všech jejich formách a po celý jejich životní cyklus – během jejich vzniku, zpracování, ukládání, přenosu a likvidace. [2]

Operační systém

Je v informatice označení pro základní programové vybavení telefonu, které je zavedeno do paměti zařízení při jeho startu a zůstává v činnosti až do jeho vypnutí. Hlavním úkolem operačního systému je zajistit uživateli možnost ovládat telefon, vytvořit pro procesy aplikační rozhraní a přidělovat jim systémové zdroje. [5]

Kyberprostor

Je virtuální svět, přesněji elektronické médium tvořící světovou, globální síť, která je základem online komunikace. Je to rozsáhlá síť tvořena menšími, po světě rozesetými sítěmi, které užívají TCP/IP protokol. Ten jim umožňuje komunikaci a výměnu dat. [6]

Kybernetický útok

Lze definovat, jako nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový, či mobilní systém či počítačovou síť. Tato akce může být zaměřena například na krádež osobních údajů, spam či jiné obtěžování, zpronevěru, šíření či držení dětské pornografie. [1]

GDPR

Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation). Představuje právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji. [33]

Osobní údaj

Je jakákoliv informace týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaje vztahují.

Mezi tyto informace patří:

- Adresní a identifikační údaje,
- citlivé údaje,
- popisné údaje,
- údaje o jiné osobě.

Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam. [7]

Citlivé osobní údaje

Citlivé osobní údaje jsou speciální kategorií podle GDPR, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Tyto údaje mohou subjekt údajů samy o osobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Do kategorie citlivých údajů

GDPR nově zahrnuje genetické a biometrické údaje. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů. [32]

1.2 Legislativa

- Zákon č. 40/2009 Sb., trestní zákoník.
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.
- Zákon č. 141/1961 Sb., o trestním řízení soudním.
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže.
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti.
- Zákon č. 273/2008 Sb., o Policii České republiky.
- Zákon č. 89/2012 Sb., občanský zákoník.
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví.
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích.
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

1.3 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017. [8]

2 OPERAČNÍ SYSTÉM ANDROID

Operační systém Android je otevřeným softwarem, který je používaný na mobilních telefonech (smartphonech), tabletech a chytrých televizích. Jedná se o nejpoužívanější operační systém na mobilních telefonech.

Vývoj je veden firmou Google. Podoba samotného systému je prakticky u každé značky telefonu jiná. Google prodává výrobcům základní verzi svého operačního systému Android a ti ho později vylepšují a snaží se ho zdokonalit do takové podoby, aby byl co nejkompatibilnější s mobilním telefonem, který vyrábějí. Výsledná podoba operačního systému má tedy velký vliv na to, jestli bude jejich mobilní telefon, čí jiné zařízení, dobře prodáváno, či ne.

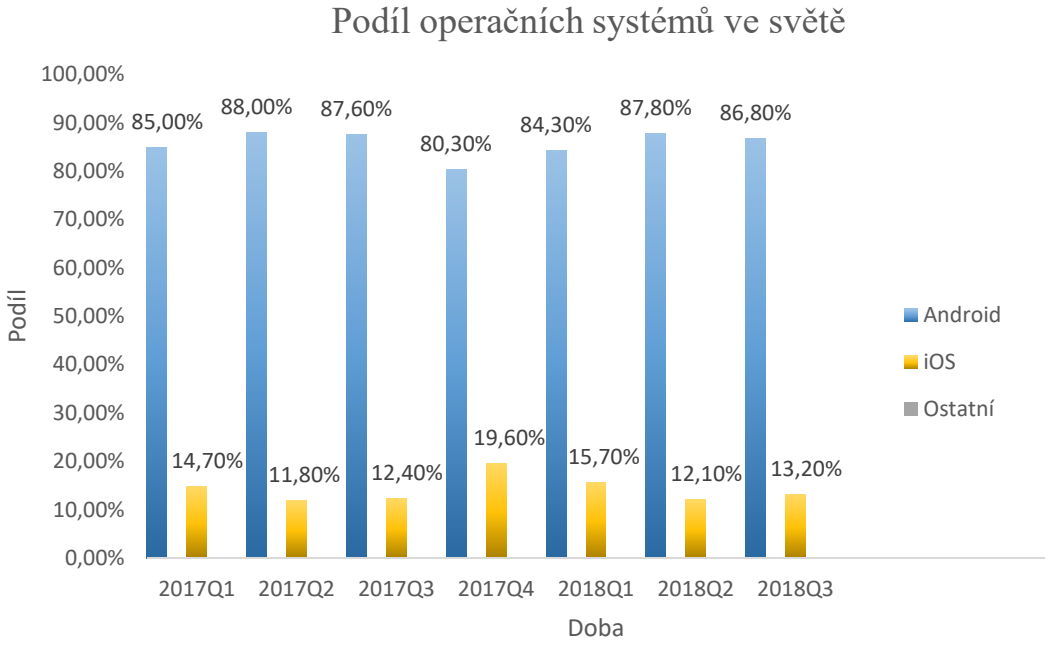
Obr. 1 - Znak Androidu [9]

2.1 Dostupnost operačního systému Android na mobilních telefonech

Co se týká operačních systému na mobilním zařízení, existuje aktuálně několik společností, které se zabývají vývojem operačních systému. Mimo nejdominantnější operační systém Android, můžeme na trhu najít i operační systém iOS (iPhone operační systém), Windows, BlackBerry, Linux, anebo také Symbian OS, který se používal na starších mobilních zařízení značky Nokia.

Nejznámějším a nejvíce používaným operačním systémem na mobilních zařízeních je Android. Tento operační systém si drží první místo mezi mobilními operačními systémy již několik let. Důkazem o tom jsou pravidelné, čtvrtletní průzkumy společností, jako například IDC. Tato společnost provádí průzkumy, které ukazují podíly jednotlivých operačních systémů na vyrobených mobilních zařízeních.

Podle serveru IDC, Android najdeme na 86.8 % smartphonů, iPhony tvoří 13,2 % trhu. Objem dodávek smartphonů s jinými systémy se už rovná nule. [10]

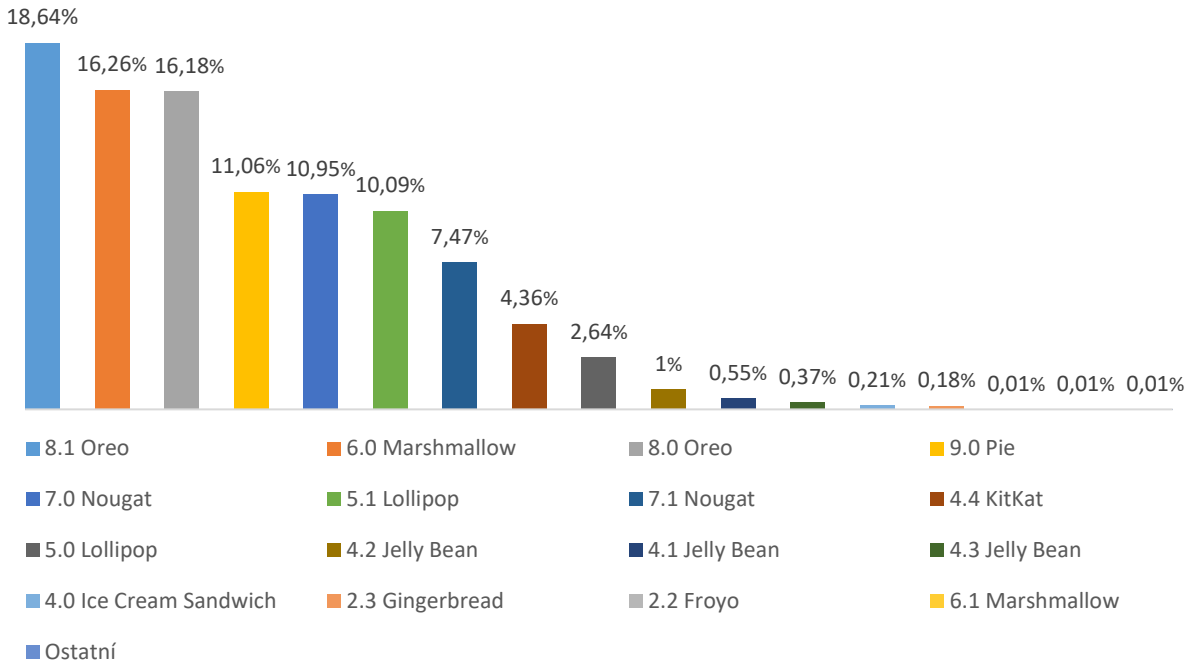


Obr. 2 – Graf podílu OS ve světě [10]

2.2 Porovnání obsazení jednotlivých systému v zařízeních

Na obrázku níže můžete vidět podíl jednotlivých systému Android na mobilních zařízeních. Android verze 8.1 (Oreo) má podíl 18.64 % na světovém trhu mezi majiteli smartphonů, kteří používají operační systém Google Android. Což je poměrně malé číslo. Vzhledem k bezpečnosti to znamená, že více než 65 % mobilních telefonů se systémem Android má starý systém, který už nemusí být schopen perfektně chránit uživatele proti novým hrozbám.

Nejnovější operační systém Android 9.0 Pie je nainstalován na 11.06 % zařízení z celého světa. Jelikož se jedná o poměrně nedávno vydaný operační systém, dá se očekávat, že jeho podíl bude růst. I tak ale nebude obsazenost tohoto operačního systému příliš veliká, z části nahradí předchozí verzi Oreo, největší podíl budou mít ale nadále mnohem starší verze operačních systémů Android.



Obr. 3 - Porovnání obsazení verzí systému v mobilních zařízení [11]

Jelikož je mobilní systém Android, tak dominantním systémem, je důležité analyzovat jeho bezpečnost a schopnost chránit osobní data.

3 ZABEZPEČENÍ SYSTÉMU ANDROID

V této kapitole budou vypsány vybrané prvky, které mají vliv na zabezpečení mobilních zařízení a také popsaná jejich funkce a využití pro zabezpečení citlivých dat v zařízení.

3.1 Anonymita uživatele

Každý mobilní telefon se systémem Android má možnost připojit se na internet a procházet tak webové stránky a sociální sítě. Při každém takovém připojení k internetu se stane, že jsou o nás sbírány informace. To se děje většinou bez vědomí uživatele. Je ale potřeba si uvědomit, že jakékoliv zveřejnění naších osobních informací na internetu sebou nese velká rizika. Tyto osobní informace pak může kdokoliv zneužít. [1] [2] [3]

Většina webových stránek, sociálních sítí anebo aplikací shromažďují naše osobní údaje a informace. Většina z nich tyto informace přímo nepotřebuje, nebo pro ně nejsou důležité a dokáži fungovat i bez nich. Tyto informace jsou důležité především pro poskytovatele služby informační společnosti. Díky tomu že získají naše informace a osobní údaje, mohou poskytovat svoje služby zadarmo, a hlavně také cílit jejich nabídky. Pro poskytovatele služby informační společnosti jsou důležité informace, jako jsou například naše jméno, příjmení, e-mailová adresa bydliště, anebo telefonní číslo. Kromě těchto informací jsou pro ně důležité i například citlivé údaje, jako soubory cookies, verze aplikací používaných v mobilním zařízení a celkově informace a zařízení. Dále jsou pro poskytovatele důležité informace týkající se lokalizace a umístění mobilních zařízení. Mezi tyto informace můžeme zařadit například informace o Wifi, GPRS anebo souřadnice GPS. Tyto informace využívají například pro cílenější reklamy či doplňkové služby. [1]

Pokud by se naše osobní údaje používaly pouze pro výše zmíněné účely, nebyli bychom v tak velkém ohrožení, a kromě cílenějších reklam na naši osobu bychom jinak využívání těchto informací nepocítili. Největší riziko, ale spočívá v jejich lehkém odcizení a tím pádem i zneužití. [1]

Je tedy důležité snažit se o co největší anonymitu na internetu. Když naše informace a osobní údaje nikomu neposkytneme, nemohou být tím pádem ani zneužity (pokud nebudou z našeho zařízení odcizeny). Pokud se chceme pohybovat v tomto kyberprostoru bez rizika zneužití naších osobních údajů, musíme si být vědomi tak zvaných digitálních stop. Jedná se informace, které po sobě zanecháváme při pohybu na internetu. Základně se dají rozdělit na digitální stopy ovlivnitelné a neovlivnitelné. [1]

Digitální stopa neovlivnitelná

- Informace z mobilního systému,
- připojení k sítím, zejména internetu,
- využívání poskytovaných služeb.[1]

Digitální stopa ovlivnitelná

- Vědomé využití služeb,
- dobrovolné zveřejnění informace,
- blogy, fóra,
- sociální sítě,
- e-mail,
- datová úložiště,
- cloudové služby. [1]

Obecně ve světě informatiky a kyberprostoru platí, že pokud nahrajete do tohoto prostoru jakoukoliv informaci nebo osobní data, zůstanou tam navždy. Vždy totiž bude existovat kopie naších dat. Proto je důležité, dávat si pozor jaké digitální stopy po sobě na internetu zanecháváme. [1]

3.2 Virtuální privátní síť (VPN)

Zkratka VPN vychází z anglického spojení Virtual Private Network, které můžeme přeložit jako virtuální privátní síť. Virtuální proto, že zajišťuje pomyslné přímé spojení s jakýmkoliv mobilním zařízením nebo webovou stránkou na světě. Privátní proto, že veškerá komunikace je šifrovaná, a pokud není určeno jinak, je vždy realizována pouze mezi uživatelem a navštívenými stránkami. Jedná se o síť, protože ke své realizaci využívá rozsáhlou síť VPN serverů umístěných po celém světě. [22]

3.2.1 Výhody VPN

Využívání veřejné privátní sítě má mnoho výhod. Mezi nejvýznamnější výhody, které dělají z VPN výborný prostředek pro bezpečné prohlížení obsahu na internetu patří:

Ochrana soukromí

Použití VPN značně sníží počet informací, které o vás poskytovatel připojení i navštěvované servery mohou získat. V některých zemích, bohužel už včetně evropských, poskytovatelé

musí uchovávat informace o internetové aktivitě klienta. S použitím VPN o něm nezjistí téměř nic. V České republice to naštěstí ještě není, ale i tady vás VPN ochrání např. při připojení k veřejným (a silně nedůvěryhodným) Wi-Fi hotspotům. [22]

Mixování provozu

Jde o další způsob ochrany soukromí, kdy jeden VPN server obvykle používá mnoho lidí zároveň, někdy až stovky. Pro potenciálního špióna je tak velmi obtížné oddělit váš provoz od ostatního a sledovat, kdy a kam na internetu chodíte. A to i tehdy, kdyby měl možnost číst metadata ze všech koncových serverů. [22]

Obejití geoblokace

Nemalá část internetového obsahu a služeb je přístupná pouze z určitých zemí, resp. je v některých zemích blokována. Řešením je připojit se k VPN serveru v zemi, ve které je obsah dostupný. VPN služby obvykle mají servery v mnoha zemích na více kontinentech, mezi kterými můžete libovolně přepínat. Pokud však služby blokaci obsahu myslí vážně, mohou celkem snadno najít IP adresy alespoň největších VPN služeb a zablokovat je, což se v poslední době děle čím dál častěji (např. Netflix). [22]

Obejití lokální cenzury

V podstatě totéž jako obejití geoblokace, ale naopak. Pokud daný poskytovatel blokuje přístup na nějaké stránky, ať už z vlastní vůle nebo vládního nařízení, VPN opět pomůže. [22]

3.2.2 Nevýhody VPN

Samotné využívání veřejné privátní sítě má ovšem několik nevýhod. Tyto nevýhody souvisí spíše s určitým omezením, které sebou nese zvýšené bezpečí při prohlížení obsahu na internetu.

Horší rychlost

Samotné použití VPN protokolu o něco sníží rychlost přenosu dat, ale nepříliš významně (přibližně 5–10 %). Potom jde samozřejmě o to, jakou rychlost dokážou zvládnout datová centra poskytovatele VPN. Zde se služby hodně liší, ale většinou dosahují rychlostí kolem 100 Mbps i vyšších. [22]

Cena

Provoz serverů, které odbavují a maskují datový tok uživatele, něco stojí, stejně tak samotná konektivita. Cena VPN služeb se typicky pohybuje v rozmezí 3–10 eur měsíčně, které bude

muset uživatel připočíst ke svému účtu za internetové připojení. Existují sice i VPN zdarma, ale ty lze použít maximálně pro nárazové použití bez seriózního zájmu o ochranu soukromí. [22]

IP na blacklistech

VPN služby jsou také zneužívány k různým záškodnickým aktivitám, což často vyústí v to, že takový uživatel dostane IP adresu VPN služby na tzv. blacklist (černou listinu). A jelikož jsou IP adresy sdílené, nedostane se na dané stránky ani jiný uživatel. Tento problém je poměrně častý hlavně u větších VPN služeb, které někdy mají blokované rovnou celé rozsahy IP adres, a tedy nemusí pomoci ani změna serveru. [22]

3.3 Zámky obrazovky

Jedná se o základní způsoby, jak zabezpečit mobilní zařízení před vniknutím. Starší telefony měly základní typy zámku, jako například zabezpečení pomocí hesla, číselného kódu anebo gesta. Novější telefony obsahuj pokročilejší, a z hlediska bezpečnosti, lepší typy zabezpečení. Jedná se například o sken obličeje, otisku prstu, pomocí podpisu anebo rozpoznání hlasu. Tyto způsoby zabezpečení budou analyzovány v praktické části.

3.4 Antivirus

Pro mobilní zařízení s operačním systémem Android jsou dostupné antivirové programy, které by měly být schopny detekovat a odstranit škodlivý software. Pokud ale stahujeme aplikace jen z důvěryhodných zdrojů, jako je například Google Play, je velká pravděpodobnost, že zařízení nebude infikováno škodlivým softwarem.

Samotný operační systém Android, v novějších telefonech, již obsahuje určité způsoby ochrany před škodlivých softwarem. Antivirový program je tedy potřeba spíše na starších telefonech, které ještě nemají tak dobře vyvinutou základní ochranu proti virům.

3.5 Google Play Protect

Jedná se o službu, která slouží pro kontrolu, zda určité aplikace neobsahují škodlivý software.

Tato služba se stará o tři základní postupy ochrany před viry:

1) Před stažením aplikací z Obchodu Google Play provádí kontrolu zabezpečení.

2) Vyhledává v zařízení potenciálně škodlivé aplikace z jiných zdrojů. (Škodlivé aplikace se někdy označují jako malware.)
3) Na nalezené potenciálně škodlivé aplikace vás upozorní. Známé škodlivé aplikace ze zařízení odstraní. [12]

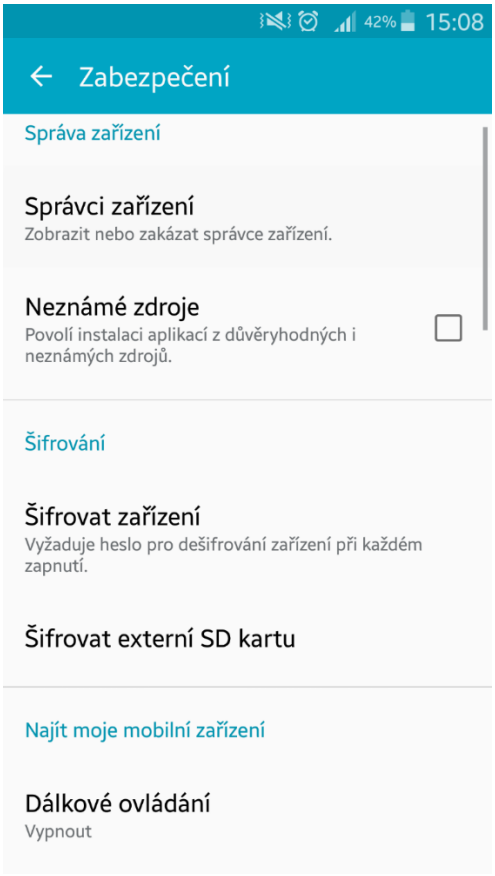
Z hlediska bezpečnosti se jedná o nejdůležitější službu, která se stará o ochranu proti vniknutí škodlivého softwaru.

Ochrana proti škodlivým aplikacím pomocí Google Play Protect

Je důležité, aby uživatel stahoval aplikace z ověřeného zdroje, a to pomocí aplikace Google Play. Jelikož je tato aplikace vybavena službou Google Play Protect, která zabraňuje instalaci škodlivého softwaru do zařízení, je tedy nejvhodnějším zdrojem pro instalaci nových aplikací.

V případě že uživatel instaluje aplikace z neověřených stránek, může dojít k infikaci zařízení škodlivým softwarem. Ten se do zařízení dostane společně se soubory instalované aplikace. Po umístění umožnuje majiteli tohoto škodlivého softwaru sledovat aktivitu daného mobilního zařízení a celkově umožňuje plně kontrolovat a ovládat zařízení.

Je tedy důležité instalovat aplikace pouze z Google Play. Aby nedošlo k tomu, že do zařízení nainstalujeme aplikaci z nedůvěryhodného zdroje, je možné si v nastavení zakázat instalaci aplikací z nedůvěryhodných zdrojů. Tento zákaz je primárně v zařízení již udělen.



Obr. 4 - Zákaz instalace aplikací

[Vlastní]

3.6 Vliv lidského faktoru na bezpečí dat v telefonech

Mobilní zařízení může mít tu nejlepší ochranu proti vniknutí škodlivého softwarů, anebo nepřekonatelné způsoby, jak zabránit vniknutí cizí osoby do paměti telefonu, ale nejdůležitějším faktorem je, zda uživatel dělá vše pro to, aby zabránil ohrožení jeho bezpečí. Důležitá je velká uživatelská rozvážnost a schopnost zabezpečit si svoje mobilní zařízení před odcizením osobních dat. Je tedy potřeba, aby majitel používal například nejlepší zámky displeje, nainstaloval antivirus, a hlavně instaloval aplikace jen z důvěryhodných zdrojů. Mezi další kroky potřebné pro co největší zabezpečení mobilního zařízení je například nepřihlašovat se na veřejných sítích k účtům, jako je bankovní účet nebo Facebook.

4 CÍLE A METODY ZPRACOVÁNÍ BAKALÁŘSKÉ PRÁCE

Hlavním cílem této práce je analyzovat a zhodnotit bezpečnost mobilních zařízení s operačním systémem Android.

Dílčími cíli práce je definovat základní pojmy, určit aktiva, které je potřeba chránit, popsat možné hrozby a následně provést samotnou analýzu bezpečnosti mobilních zařízení se systémem Android. Mezi poslední dílčí cíl patří navrhnout doporučení pro zvýšení bezpečnosti těchto zařízení.

V práci byla zpracována rešerše současného stavu problematiky s důrazem na monografii a analytické materiály.

Další metodou je vědecký popis, což byl výsledek pozorování. Zde byl kladen důraz na správnou volbu pojmů, úplnost záznamů a objektivitu.

Metoda explanace byla použita především pro vysvětlení, jakým způsobem může být mobilní zařízení napadeno a také pro vysvětlení technik sociálního inženýrství.

V práci byla použita komparace, a to pro porovnání jednotlivých druhu zabezpečení pomocí zámků obrazovky. K lepší komparaci zde bylo použito multikriteriálního hodnocení.

Další metodou je analýza, a to bezpečnosti jednotlivých způsobů zabezpečení. Analyzován byl i přístup uživatelů mobilních zařízení se systémem Android, a to z hlediska bezpečnosti jejich osobních informací umístěných v těchto zařízení. Z metod analýzy zde bylo také využito SWOT analýzy.

Metodou indukce bylo zjištěno, jaký postoj by měli mít uživatelé mobilních zařízení s operačním systémem Android k bezpečnosti informací v jejich přístrojích.

V práci bylo z největší části využito metod sběru dat a informací.

II. PRAKTICKÁ ČÁST

5 ANALÝZA BEZPEČNOSTI MOBILNÍCH ZAŘIZENÍ

V této kapitole bude provedena samotná analýza mobilních zařízení se systémem Android. Využito bude multikriteriálního hodnocení pro porovnání různých způsobu, jak zamknout obrazovku proti vniknutí cizí osoby. Dále bude provedena SWOT analýza, a nakonec bude zanalyzován přistup uživatelů mobilních zařízení s operačním systémem Android k bezpečnosti informací v jejích přístrojích, a to pomocí dotazníkového šetření. Jako první je potřeba si definovat aktiva, které je potřeba chránit (informace umístěné v mobilních zařízeních). Dále uvést možné hrozby, které mohou ohrozit mobilní zařízení. Poté budou provedeny vlastní analýzy, a nakonec budou navržena opatření pro zlepšení zabezpečení.

5.1 Informace umístěné v mobilních zařízeních

V mobilních zařízeních můžeme najít obrovské množství informací. Tyto informace mohou mít pro uživatele osobní charakter. Takovéto informace mohou obsahovat mnoho údajů o majitelovi zařízení. Některé z těchto informací nejsou příliš důležité, ale mnoho z nich dokáží uživateli svojí ztrátou způsobit velké potíže. Charakter a důležitost těchto informací se liší podle toho, zda je zařízení využíváno pro osobní nebo pracovní účely. Pracovní zařízení často obsahují méně osobních informací. Tyto informace jsou ovšem spíše důležité pro firmu či společnost a jejich ztráta mnohdy znamená přímé ohrožení dané společnosti a jejich dobrého jména.

Mezi osobní informace umístěné v mobilních zařízeních můžeme zařadit například:

5.1.1 Telefonní kontakty

V každém mobilní telefonu se nachází mnoho telefonních kontaktů. Telefon může být využíván buď pro osobní, anebo pro pracovní účely.

Při využívání mobilního telefonu pro osobní účely máme v zařízení uložené většinou pouze telefonní čísla na naše známé, rodinu či přátele. Odcizení a následné možné zneužití je v tomto případě velmi nepříjemné a může nám způsobit nemalé problémy. Mnohem větší problémy nám může způsobit ztráta telefonních kontaktů umístěných v telefonu, který je využíván pro pracovní účely. Odcizení a následné zneužití pracovních kontaktů může vést až k ohrožení společnosti či firmy.

5.1.2 Historie komunikace (SMS, MMS, hlasová, e-mail)

Zde můžeme pro příklad uvést zprávy SMS, MMS či hlasové zprávy. V těchto způsobech komunikace můžeme najít velice důležité informace. Především u SMS zpráv. Mobilní telefon je dnes již klasicky propojený s různými účty jako jsou Facebook, e-mail či různé účty v e-shopech. Nejvíce rizikové je ovšem propojení mobilního telefonu s bankovním účtem. Pokud používáme například internetové bankovnictví, jsou nám skrze zprávy SMS doručovány informace a stavu zůstatku na účtu, potvrzovací kódy pro platby a další informace týkající se našeho bankovního účtu. V mnoha případech se propojenost s mobilním telefonem využívá pro obnovení hesla na různých účtech. Odcizení těchto zpráv by pro nás znamenalo ztrátu peněz, osobních informací, údajů, ale hlavně soukromí.

Samostatnou skupinou jsou e-maily. E-mail se využívá ještě častěji pro propojení s různými účty a na většině e-mailových účtů můžeme najít zprávy obsahující nejen přihlašovací jméno na různé účty, ale i hesla. Riziko, že bude tento druh komunikace zneužit útočníkem je tedy velice velké a je potřeba chránit si své zprávy.

5.1.3 Poloha uživatele

Poloha mobilního zařízení je jednou z věcí, které se mohou stát objektem možného útoku. Poloha uživatel je v mobilním telefonu zaznamenávaná v několika případech. Jako první příklad je pomocí aplikaci Google Maps, která polohu uživatele zdokumentuje už při jejím samotném otevření.

Dalším způsobem, jakým je zjišťována poloha mobilního zařízení, je pomocí automatických denních zpráv o počasí na telefonech s Androidem. Ty zjišťují jen rámcově, kde se uživatel právě nachází. [23]

5.2 Možné hrozby

Existuje několik způsobů, jak by mohlo dojít k odcizení osobních údajů a jiných citlivých dat. Budou zde vypsány ty nejzásadnější a nejčastější, které se v dnešní době vyskytují.

5.2.1 Překonání zámků obrazovky

Mezi první způsob může být zařazeno proniknutí pomocí překonání zámků obrazovky. Každý mobilní telefon, který má nainstalovaný operační systém Android, má několik základních zámků obrazovky. Jedná se o zamčení obrazovky pomoci číselného kódu, hesla anebo gesta, či dalších.

Některé novější telefony chrání telefon před nepovoleným vstupem pomocí otisků prstů, skenu obličeje, anebo podpisu.

5.2.2 Zanedbání ochrany ze strany uživatele

Vše záleží na tom, jak moc si majitel mobilního zařízení je vědom možnosti, že by se jeho zařízení mohlo stát cílem útoku. Pokud si je majitel telefonu vědom možného odcizení jeho osobních dat, může podniknout velké množství opatření, které tento útok odrazí. V opačném případě se může stát, že uživatel nepodniká žádné kroky pro zabezpečení telefonu. Pokud uživatel nenastaví na zařízení, ani základní zámek obrazovky, není problém s bezpečností na straně zařízení, ale uživatele. Proto by měl uživatel mobilního zařízení podniknout co nejvíce kroků pro zabezpečení dat.

5.2.3 Instalace škodlivého softwaru

Další možností, jak by mohlo dojít k odcizení citlivých dat je, že uživatel si nainstaluje do mobilního telefonu aplikaci, která obsahuje škodlivý software. Ten po vniknutí do telefonu způsobí, že umožňuje jinému uživateli sledovat aktivitu majitele telefonu, prohlížet všechny jeho data a měnit nastavení. V podstatě má nad telefonem plnou kontrolu.

Existují dva způsoby, jak se dají instalovat aplikace na mobilní zařízení se systémem Android. Buď se instalují přímo z aplikace Google Play, anebo z jakýchkoliv jiných webových stránek.

První způsob je nejbezpečnější, a to z důvodu, že je zde každá aplikace kontrolována pomocí služby Google Play Protect. Tato služba kontroluje aplikace, zda neobsahují škodlivý software.

Ovšem může existovat aplikace, která sice neobsahuje virus, ale po jejím otevření, nás přesune na stránku, ze které se tento vir může stáhnout.

Instalace z jiných zdrojů než přes Google Play, může způsobit vniknutí škodlivého softwaru do našeho mobilního zařízení, a to právě z důvodu, že tyto aplikace nejsou kontrolovány žádnou službou.

5.2.4 Vniknutí malwaru do systému

Za malware je možné označit jakýkoli software využitý k narušení standardní činnosti mobilního systému, zisku informací (dat), či využitý k získání přístupu k systému. Malware

může mít celou řadu podob, přičemž mnohé druhy malware jsou pojmenovány podle toho, jakou činnost provádějí.

Ransomware

Ransomware je malware, který brání či omezuje uživatele v řádném užívání systému do doby, než dostane útočník zaplaceno „výkupné“. Ransomware se nejčastěji dostane do zařízení pomocí malware (trojského koně či červa), který je umístěn na webových stránkách nebo je přílohou e-mailu. Jakmile je tento malware bezpečně „usídlen“ v systému, dojde ke stažení vlastního ransomware. [1]

Existují dva typy ransomware. Dělí se podle toho, jak zasahují do chodu zařízení.

- **První typ** – omezí funkčnost celého systému a neumožní uživateli tento systém vůbec využívat (např. zabráněním spuštění operačního systému či zablokováním systémové obrazovky). [1]
- **Druhý typ** – ponechá systém funkční, avšak dochází k uzamčení a znepřístupnění dat uživatele. [1]

V současnosti dochází spíše k využívání druhého typu ransomware. Účelem tohoto malware je zašifrovat pevný disk nebo vybrané typy souborů v mobilním systému, přičemž primárně má tento malware za cíl zašifrovat soukromé soubory uživatele jako jsou obrázky, textové či tabulkové dokumenty, videa aj. Po skončení šifrování se zpravidla uživateli zobrazí zpráva, že jeho soubory jsou zašifrovány, a pokud je chce získat zpět (dešifrovat), musí poslat určitý obnos na účet útočníka. K transakcím jsou obvykle využívány virtuální měny jako je Bitcoin nebo různé předplacené služby. Ve většině případů je stanovena časová lhůta pro zaplacení. Po uplynutí této lhůty dochází k smazání klíče, jenž může zašifrované soubory otevřít. [1]

5.2.5 Zneužití technik sociálního inženýrství

Nezjednoduším způsobem, jak získat osobní informace od majitele mobilního zařízení je právě ten, že tyto informace sám uživatel (nevědomě) útočníkovi poskytne. Útočníci k získání těchto informací využívají právě techniky sociálního inženýrství. To znamená, že často využívají podvodné či klamavé jednání.

Sociální inženýrství není samo o sobě přímo kybernetický útok, nicméně je předpokladem pro to, aby byla řada kybernetických útoků úspěšná.

Definovat pojem sociální inženýrství bylo by možné tak, že jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli. Základním krokem je v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je. Zjednodušeněji by se dalo říci, že se jedná o „umění klamu“. Tyto techniky jsou využívány nejen vůči firmám, ale i vůči jednotlivcům. Útok primárně nemusí vypadat jako podvod, ale následně mohou být tyto informace prodány či zneužity k závažnějšímu útoku. [1] [2] [3]

Hlavní myšlenkou sociálního inženýrství je nevyužívat technické přístupy či nástroje, když mnohem jednodušší je uvést oběť v omyl, ve kterém sama dobrovolně toto heslo prozradí. Nejslabším článkem bezpečnostního systému je a vždy bude člověk. [1]

Mobilní systém nemůže existovat bez závislosti na člověku (ať již jde o zprovoznění, nastavení, či údržbu mobilního systému), a právě proto je nejjednodušší cestou k získání potřebné informace, právě využití člověka. Jednoduchost tohoto útoku cíleného na nejslabší článek celého systému z něj zpravidla činí tu nejúčinnější formu. [1]

Jedním z klíčových faktorů pro sociální inženýrství je zisk co největšího množství informací o cíli útoku (ať již mobilním systému, právnické či fyzické osobě). Mnohdy útočník dlouhodobě působí na klíčovou osobu a buduje si u ní důvěru. Útočník typicky využívá lidské neopatrnosti, důvěřivosti, ochoty pomoci jiným, lenosti, slabosti, strachu (např. aby se osoba nedostala do problémů), neodpovědnosti, hlouposti dalších vlastností.

V oblasti informatiky je možné v poslední době sledovat stále sofistikovanější a propracovanější útoky. Například kvalitně připravené podvodné e-maily, reálné instituce (použité jako domnělý odesílatel), přesměrování na podvodné stránky či instalace malware obsaženého v příloze dokumentu nebo na paměťovém médiu a jiné. [1]

Metody útoků sociálního inženýrství

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit:

1) **Podvodný e-mail či falešná webová stránka**
2) **Telefonický hovor**
3) **Útok „tváří v tvář“**
4) **Prohledávání odpadků**
5) **Prohledávání webu, sociálních sítí aj.** Jedná se o lehce dostupný zdroj dat pro potencionální útočníky sociálního inženýrství, díky kterému mohou zjistit, anebo ověřit

informace a možném cíli. Můžeme mezi ně zařadit například veřejné informace typu životopisy, práce, teze, návrhy a jiné dokumenty uveřejněné na internetu.

6) **Doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči**
7) **Ponechání paměťového média** (USB aj.) **v zájmové oblasti** (např. firmě, u domu zaměstnance aj. toto médium pak typicky obsahuje malware).
8) **Nabídka vyzkoušení služby online** (např. nabídka cloudového uložiště, či některé zajímavé služby zdarma aj.)
9) **Dodávka či nalezení zařízení**
10) **Falešný servisní technik**
11) **Jiné**

Cíl útoků sociálního inženýrství

Pokud jde o cíl útoků sociálního inženýrství v rámci organizace, pak se možnými cíli mohou stát například:

- IT oddělení,
- pracovníci technické podpory,
- recepční (sekretariáty),
- bezpečnostní pracovníci,
- správa budov,
- úklid aj.

K redukci rizik sociálního inženýrství je nezbytné zvyšovat povědomí o možných hrozbách nejen v rámci organizace, ale v rámci celé společnosti. Pro útočníka je mnohem snazší zaměřit svůj útok na masy nezkušených a neznalých lidí než na relativně dobře chráněnou společnost. [1]

Techniky využívající sociálního inženýrství

Níže budou popsány jednotlivé techniky útoků, využívající sociálního inženýrství. Tyto techniky jsou využívány jako hlavní prostředek pro nezákonný zisk osobních informací o jiných lidech. U každé techniky bude popsáno, jakým způsobem by mohl daný útok být proveden.

Phishing

Pojmem phishing se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, anebo PIN. [1] [3]

Základ této techniky spočívá v donucení uživatele navštívit podvodnou stránku (zobrazující např. webovou stránku internetového bankovnictví, online obchodu) a následné vyplnění „přihlašovacích informací".

Za phishing se může tedy označit jakékoli podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem. V tomto případě již nemusí uživatel vyplňovat údaje, avšak je mu doručena zpráva (či je uživatel přesměrován na stránku) typicky obsahující malware, který si uvedené údaje posbírá sám. [1] [3]

V obou dvou případech dochází k oklamání uživatele, který je cílem phishingového útoku, rozdíl spočívá především v tom, jaká míra interakce je po uživateli vyžadována. [1] [2]

Pharming

Pharming představuje sofistikovanější a nebezpečnější formu phishingu. K útoku dochází v momentě, kdy uživatel zadá na internetovém prohlížeči adresu webového serveru, na kterou chce přistoupit. Nedojde však k připojení na příslušnou IP adresu originálního webového serveru, ale na IP adresu jinou, na tu, která byla vytvořena pro účely útoku. Webové stránky na falešné adrese jsou zpravidla velmi věrné a co nejpřesněji imitují originální stránky, a to až tak, že jsou od nich k nerozeznání (což je cílem útočníka). Uživatel následně zadá přihlašovací údaje, které získá útočník. Tento útok je nejčastěji proveden při přístupu uživatele na stránky internetového bankovnictví. [1]

Falešné webové stránky mohou být použity k instalaci virů nebo trojských koní do uživatelova zařízení nebo se pomocí nich mohou útočníci pokusit získat osobní či finanční údaje, které mohou být následně zneužity k odcizení osobních údajů. [1]

Pharming je zvlášť nebezpečná forma kyberkriminality, dokonce ani pokud dodržujete preventivní opatření, například zadáváte internetové adresy ručně nebo používáte výhradně důvěryhodné záložky, nejste před útokem tohoto druhu ochráněni, protože k nechtěnému přesměrování dochází až poté, co zařízení odešle žádost o spojení. [13]

Druhým typickým způsobem pharmingu je napadení mobilního zařízení uživatele pomocí malware, kde se dá předpokládat menší míra zabezpečení. Tento malware změní soubor hostitelů s cílem odklonit přenos od zamýšleného cíle a přesměrovat uživatele na falešnou webovou stránku. [1]

Spear-Phishing

Spear-phishing je jednou z forem phishingového útoku, avšak s tím rozdílem, že spear-phishing je přesně cílený útok, na rozdíl od phishingu, který je útokem spíše nahodilým. Cílem útoku bývá určitá skupina, organizace nebo jednotlivec, konkrétně informace a data, která se v této organizaci nacházejí (např. duševního vlastnictví, osobní a finanční údaje, obchodní strategie, anebo utajované informace.). Spear-phishing se liší oproti klasickému phishingu v tom, kdo je odesílatelem předmětných zpráv. V počátku útoku je to vlastní útočník, který využije otevřené zdroje, aby zjistil co nejvíce informací o napadané organizaci, její struktuře atd. Dále vytvoří co nejkvalitnější e-mail či jinou zprávu a začne komunikovat s osobou uvnitř organizace jako s kolegou. Tuto osobu pak útočník využije jako prostředek pro šíření dalších zpráv (např. infikovaných malware) v rámci organizace. Jelikož se jedná o osobu obětem známou, nemají problém s ní komunikovat a méně, pokud vůbec, prověřují její zprávy. [1] [2] [3]

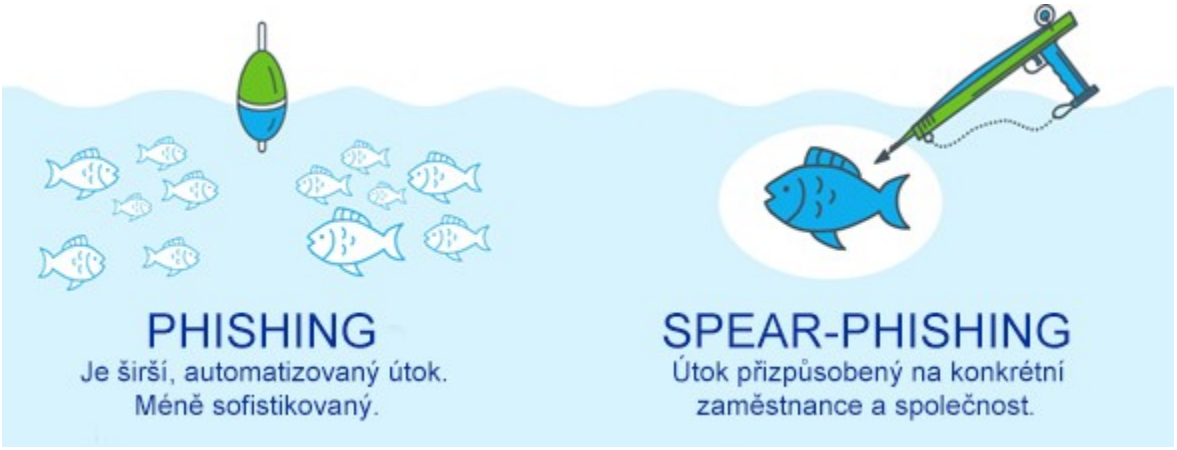
Útok pak vypadá následovně:

Útočník si vyhlédne organizaci pracující s důležitými informacemi. Dále analýzou webových stránek získá informace o personální struktuře, zaměstnancích a procedurách (pro získání podrobnějších informací o zaměstnancích může využít jejich soukromé stránky a diskusní fóra). V dalším kroku útočník vytvoří zprávu, jejíž obsah, forma a vzhled napodobuje vnitřní komunikaci v organizaci. Ve zprávě požádá zaměstnance o zadání citlivých informací pro přístup do sítě. [14]

V praxi by to mohlo vypadat následovně:

1. Útočník si vybere společnost, či organizaci.
2. Najde pracovníka, který zná přístupová hesla a důležité informace.
3. Najde dalšího zaměstnance, kterého může oběť znát (nadřízený nebo spolupracovník).
4. Vytvoří falešnou, ale důvěryhodnou e-mailovou adresu.
5. Díky této adrese, předstírá, že je například jeho nadřízený, či spolupracovník.

6. Útočník odešle e-mail s odkazem na podvodnou stránku.
7. Zaměstnanec bez strachu otevře e-mail, v domnění, že přijímá zprávu od osoby, kterou znám.
8. Otevře odkaz na škodlivou stránku.
9. Otevřením podvodné stránky, dojde ke stažení malwaru do mobilního zařízení.
10. Útočníkovi jsou tak naprosto volně přístupné všechny hesla a důležité informace společnosti.



Obr. 5 - Rozdíl mezi phishingem a spear-phishingem [15]

Vishing

Pojem vishing (Jedná se o kombinaci slov voice (hlas) a phishing) označuje telefonický phishing, při kterém útočník využívá technik sociálního inženýrství a snaží se od uživatele dostat osobní informace (např. čísla účtů, přihlašovací údaje – jméno a heslo, čísla platebních karet atd.). Útočník se záměrně snaží zfalšovat svoji identitu. Útočníci se často představují jako zástupci skutečných bank či jiných institucí, aby u uživatele vyvolali co nejmenší podezření. [1] [2]

Smishing

Smishing (Jedná se o kombinaci slov SMS a phishing) funguje na podobném principu jako vishing či phishing, ale je využíváno SMS zpráv. V rámci smishingu jde primárně o snahu donutit uživatele zaplatit částku (například zavolat na placenou linku, poslat dárcovskou SMS atd.) nebo kliknout na podezřelé URL odkazy. Pokud uživatel uvedené URL navštíví, je přesměrován na stránku, která zneužívá určité zranitelnosti mobilního systému, případně je uživatel vyzván k zadání osobních údajů či k instalaci malware. [1] [2]

5.3 Multikriteriální hodnocení zámků obrazovky

Jak bylo zmíněno v teoretické části práce, existuje mnoho způsobů, jak zabezpečit mobilní zařízení. Mezi těmito druhy je i zabezpečení obrazovky. Tedy různé zámky obrazovky, které zabraňují vstupu útočníka do prostoru našeho mobilního zařízení, a tím pádem zabránění odcizení osobních dat. V podstatě existuje 6 základních způsobů zabezpečení mobilního zařízení pomocí zámků obrazovky. Tyto druhy budou níže porovnány, a to z několika hledisek. K porovnání bude použito multikriteriální hodnocení. Různé hlediska nám vytvoří potřebná kritéria.

5.3.1 Použití multikriteriální hodnocení

Posouzením, zda vybrané zabezpečení splňuje, či nesplňuje určité kritérium, zjistíme, jaký druh zabezpečení je nejlepší pro mobilní zařízení se systémem Android.

Pro multikriteriální hodnocení je využito vzorce pro výpočet váženého průměru. Tento vzorec vychází z předpokladu souboru n hodnot kdy:

$$X = \{x_1, \dots, x_n\}$$

a k nim odpovídající váhy:

$$W = \{\omega_{1,} \dots, \omega_n\},$$

je dán vzorec:

$$\bar{x} = \frac{\sum_{i=1}^{n} \omega_i x_i}{\sum_{i=1}^{n} \omega_i}$$

Dále je potřeba vybrat komparační kritéria, díky kterým se dá objektivně zhodnotit kvalita daného zabezpečení. Nejdůležitějšími komparačními kritérii je síla zabezpečení a obtížné prolomení dané ochrany.

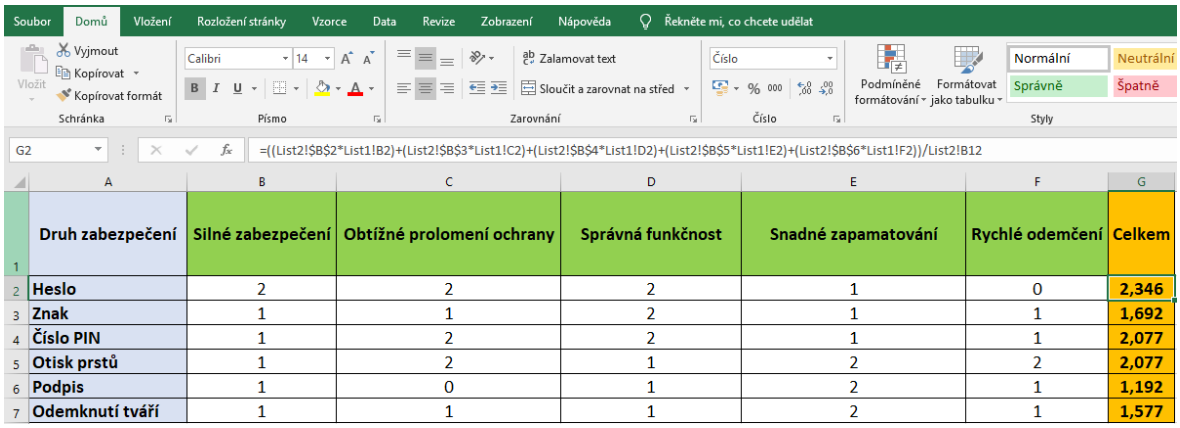
Pro jednotlivá kritéria (tedy soubory hodnot n) jsou přiděleny váhy, (v matematickém vzorci jako ω) označující důležitost tohoto kritéria pro výběr vhodného druhu zabezpečení. Následující tabulka zobrazuje, jaké váhy jsou kritériím přiřazeny. Čím vyšší je hodnota čísla, tím je důležitost pro dané kritérium vyšší.

Tab. 1 - Hodnoty vah kritérií pro multikriteriální hodnocení [vlastní]

Kritérium	Přiřazená váha
Silné zabezpečení	10
Obtížné prolomení ochrany	10
Správná funkčnost	8
Snadné zapamatování	5
Rychlé odemčení	3

Dalším parametrem vzorce je x, která obsahuje číselné hodnocení zabezpečení. Toto hodnocení je zvoleno v rozmezí 0 – 2. Označuje se jím váha splnění kritéria, kdy 0 označuje nesplnění, hodnota 1 částečné splnění a úplné splnění hodnotou 2.

Pro usnadnění výpočtu je tento vzorec zanesen do programu Excel, díky čemuž byl vytvořen nástroj pro komparaci jednotlivých zabezpečení.



	A	B	C	D	E	F	G
1	Druh zabezpečení	Silné zabezpečení	Obtížné prolomení ochrany	Správná funkčnost	Snadné zapamatování	Rychlé odemčení	Celkem
2	Heslo	2	2	2	1	0	2,346
3	Znak	1	1	2	1	1	1,692
4	Číslo PIN	1	2	2	1	1	2,077
5	Otisk prstů	1	2	1	2	2	2,077
6	Podpis	1	0	1	2	1	1,192
7	Odemknutí tváří	1	1	1	2	1	1,577

Obr. 6 - Výpočet multikriteriálního hodnocení zabezpečení v Excelu [vlastní]

Takto jsou propočítány hodnoty pro každý druh zabezpečení a výsledná čísla byla zanesena do společné tabulky, kde jsou následně sestupně, podle získaného hodnocení, seřazeny.

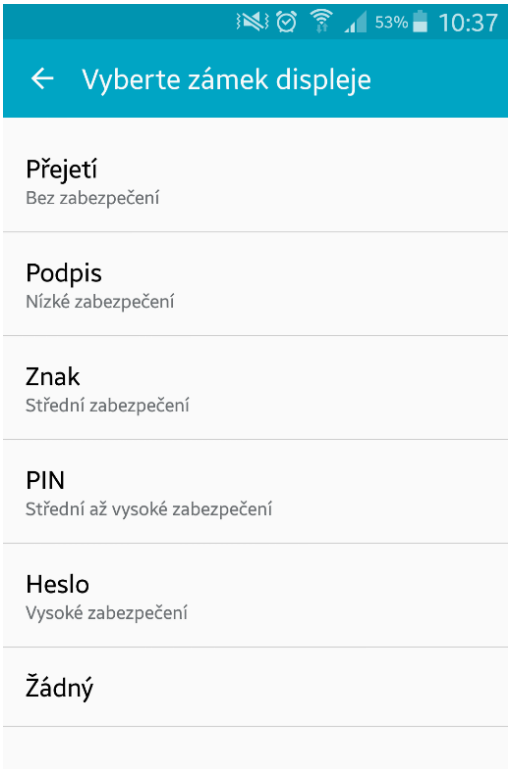
5.3.2 Komparace způsobů zabezpečení mobilního telefonu pomocí zámků obrazovky

Ztráta nebo odcizení mobilního telefonu je jedna z nejčastějších příčin ztráty osobních údajů. Mobilní zařízení se ztrácejí nebo končí v rukou někoho jiného pravidelně. Ať už se jedná o služební mobilní telefon nebo vlastní, skutečnost, že nakonec skončí v rukou jiného člověka, je vážný bezpečnostní problém. Je to jeden z nejhorších scénářů, protože mobilní telefon v dnešní době obsahuje obrovské množství informací o uživateli, ať už se jedná

o osobní údaje, hesla nebo e-maily. Krokem pro zabezpečení mobilního zařízení je nastavení uzamykací obrazovky po každém uspání zařízení.

Většina novějších mobilních zařízení obsahují tyto způsoby zamknutí obrazovky:

- Heslo.
- znak,
- PIN,
- otisky prstů,
- podpis,
- odemknutí tváří.



Obr. 7 - Zámky obrazovky u Samsungu Galaxy Note 3 [vlastní]

Pomocí multikriteriálního hodnocení může být zjištěno které z těchto způsobů zabezpečení je nejlepší. Popis multikriteriálního hodnocení a postupu, jakým způsobem se může postupovat při výpočtu hodnot multikriteriálního hodnocení jednotlivých zabezpečení, bylo zmíněno výše. Nyní je potřeba tyto druhy zabezpečení blíže popsat, podle výsledků multikriteriálního hodnocení porovnat, a tak zjistit tak nejlepší variantu pro zabezpečení mobilního zařízení se systémem Android. U každého způsobu zabezpečení bude zároveň navrženo doporučení pro zlepšení zmíněného zámku.

Heslo

Co se týká bezpečnosti. je heslo, pravděpodobně nejlepším řešením pro zabezpečení zařízení, které je dostupné na každém mobilním zařízení s operačním systémem Android.

Je ale ovšem důležité, jak dlouhé a kombinované heslo si zvolíme. Je potřeba, aby heslo obsahovalo malá a velká písmena, čísla a popřípadě i speciální znaky. Pokud je heslo dostatečně silné a dlouhé, nemusí se uživatel bát, že by heslo mohlo být poznáno díky otiskům na displeji, či přímým vizuálním kontaktem útočníka. Oproti PINů je u hesla možné používat i písmena. [25]

I zde je stejně jako u všech zabezpečení 5 pokusů na správné vložení hesla, a stejně jako u ostatních zámků je zde třicetisekundová čekací doba, pro další pokusy.

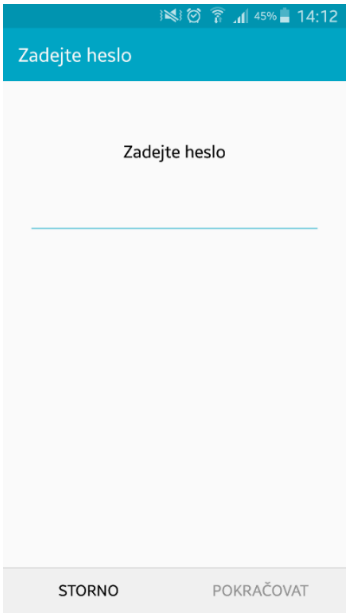
Ovšem jak je výše uvedeno, je důležité dát si pozor, aby bylo heslo co nesložitější.

Existuje několik způsobů, kterými by mohl útočník proniknout k naším citlivým datům.

Jeden z nich je pomocí chyby operačních systému. Verze Androidu 5.0/5.1 obsahuje chybu, která způsobuje pád zámků. K tomuto pádu dojde po vložení velkého množství znaků za krátký čas.

Další možností, jak obejít zabezpečení heslem je pomocí ladění USB. Po připojení zařízení k počítači můžeme pomocí ADB příkazů[2], který odstraní dosavadní zámky obrazovky.[26]

[2] Android Debug Bridge: Univerzální nástroj, pracující v režimu příkazové řádky, který umožní komunikovat s připojeným zařízením.



Obr. 8 - Zadání hesla

[vlastní]

K výpočtu výsledného hodnocení byl použit výše zmínění vzorec:

$$\bar{x} = \frac{\sum_{i=1}^{n} \omega_i x_i}{\sum_{i=1}^{n} \omega_i}$$

Zde jde vidět, jakým způsobem byla získána výsledná hodnota

$$\bar{x}_1 = \frac{(2 \times 10) + (2 \times 10) + (2 \times 8) + (1 \times 5) + (0 \times 3)}{10 + 10 + 8 + 5 + 3}$$

$$\bar{x}_1 = 1{,}694$$

Tento vzorec byl převeden do programu Excel pro snadnější a rychlejší výpočet. Níže je uvedena tabulka, která obsahuje bodové ohodnocení, podle toho, zda zabezpečení splňuje (= 2), částečně splňuje (= 1), či nesplňuje (= 0) jednotlivá kritéria.

Tab. 2 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Zabezpečení heslem				
Silné zabezpečení	**Obtížné prolomení ochrany**	**Správná funkčnost**	**Snadné zapamatování**	**Rychlé odemčení**
2	2	2	1	0
Výsledek: **1,694**				

Znak

Zabezpečení pomocí nastavení jedinečného gesta, které si uživatel zvolí a zapamatuje, se zdá být na první pohled poměrně dobrým způsobem, jak zabezpečit zařízení.

Tento druh zámku nám dává pět pokusů na vložení správného gesta. Po pátém pokusu je zařízení na 30 sekund zablokované.

Existuje už mnoho případů, kdy díky otisků na obrazovce byl tento znak útočníkem rozeznán a bylo tak pro něj poměrně lehké dostat se k citlivým datům. Tyto otisky mohou vzniknout v důsledku mastnosti prstů. Vznik tohoto jevu záleží na vlastnostech dotykového obrazovky. Povrchy některých zařízení jsou velice náchylné na vznik viditelných stop, kterých může útočník využít. [18]

Studie nazvaná Towards Baselines for Shoulder Surfing on Mobile Authentication ukazuje, že kdyby někdo pozoroval uživatele mobilního zařízení při odemykání pomocí gesta, šance, že úspěšně zjistí danou kombinaci je 64,2 % (při opakovaném pozorování dokonce 79,9 %). Při vypnutí stopy gesta je míra úspěšnosti odhalení 35,3 % (při opakovaném pozorování 52,1 %). [18]

Pro porovnání, použitím šestimístného PIN kódu se šance útočníků na úspěšné odhalení hesla sníží na 10,9 % (při opakovaném pozorování 26,5 %). [18]

Studie také potvrzuje tvrzení, že zařízení s větším displejem jsou proti těmto typům útoků zranitelnější.

Při volbě tohoto zabezpečení je tedy velmi důležité, aby gesto nebylo příliš jednoduché. Čím více kombinované bude, tím bude ochrana proti vniknutí lepší. Dále je důležité, aby uživatele při zadávání znaku nikdo nepozoroval. [18]

Obr. 9 - Zabezpečení znakem [vlastní]

Tab. 3 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Zabezpečení znakem				
Silné zabezpečení	**Obtížné prolomení ochrany**	**Správná funkčnost**	**Snadné zapamatování**	**Rychlé odemčení**
1	1	2	1	1
Výsledek: **1,222**				

PIN

Z hlediska rychlosti odemknutí je tento způsob poměrně dobrou variantou, jak si zabezpečit mobilní zařízení.

Stejně jako u gesta máme i zde 5 pokusů na vložení správného kódu. Po vyčerpání limitu musíme 30 sekund čekat na další pokusy.

Opět je zde důležité dávat si pozor na otisky na obrazovce. Jelikož je vyžadován minimálně čtyřmístný kód, je potřeba aby se čísla příliš neopakovali, a není dobré volit čísla, jako je například rok narození, čí stejné číslo, jako PIN k platební kartě.

V případě dodržení těchto pravidel, je poměrně dost velká pravděpodobnost, že zabezpečení mobilní zařízení nebude prolomeno a osobní data zůstanou tím pádem v bezpečí.

Tab. 4 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Zabezpečení číslem PIN				
Silné zabezpečení	**Obtížné prolomení ochrany**	**Správná funkčnost**	**Snadné zapamatování**	**Rychlé odemčení**
1	2	2	1	1
Výsledek: **1,500**				

Otisky prstu

Tento způsob zamčení obrazovky, je poměrně novým. Aktuálně je automaticky instalován do většiny nových telefonů výší třídy.

Jedná se o způsob zabezpečení, který využívá biometrické údaje, pro vyhodnocení, zda se jedná o majitele telefonu či nikoliv.

Snímače otisků jsou umístěny buď pod zadním fotoaparátem, nebo v prostředním tlačítku.

Spolehlivost tohoto zabezpečení je poměrně dobrá a vzhledem k rychlosti prověření, je i příjemné na používání. Je ale potřeba, aby prst s otiskem byl správně přikládán na snímač a bylo tak co nejvíce usnadněno snímači číst informace.

Ale i toto zabezpečení není nepřekonatelné. Objevili se již případy, kdy útočníkovi stačilo získat otisk majitele telefonu a tento otisk nechat vytisknou na 3D tiskárně. Je to poměrně složitý způsob útoku, ale je potřeba brát na vědomí jeho existenci.

Tab. 5 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Zabezpečení otiskem prstu				
Silné zabezpečení	**Obtížné prolomení ochrany**	**Správná funkčnost**	**Snadné zapamatování**	**Rychlé odemčení**
1	2	1	2	2
Výsledek: **1,500**				

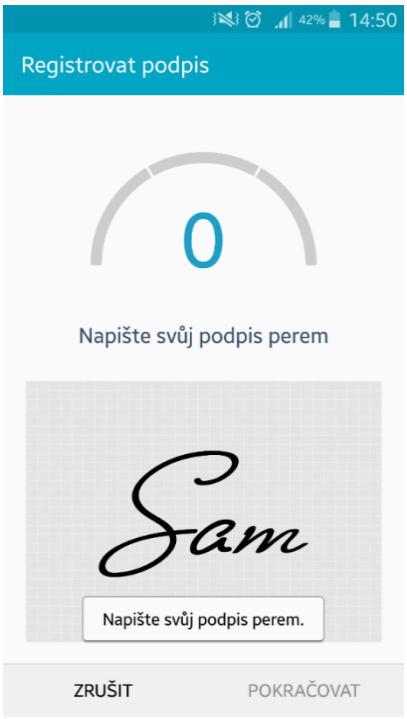
Podpis

Tento způsob zabezpečení je možný u mobilních zařízení vybavených perem pro psaní na displeji. Jedná se o poměrně rychlý způsob odemknutí obrazovky.

Efektivita zabezpečení není na tak velké úrovni, jako u předešlých způsobů zabezpečení.

Možnost překonání tohoto zabezpečení je poměrně velká. Stačí znát podpis majitele zařízení a ten opsat. Stejně jako u předchozích zabezpečení máme pět pokusů na odemčení.

Možností, jak tento druh zabezpečení zlepšit není mnoho. Je určitě dobré mít podpis co nejsložitější.



Obr. 10 – Zabezpečení podpisem [vlastní]

Tab. 6 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Zabezpečení podpisem				
Silné zabezpečení	**Obtížné prolomení ochrany**	**Správná funkčnost**	**Snadné zapamatování**	**Rychlé odemčení**
1	0	1	2	1
Výsledek: **0,861**				

Odemknutí tváří

Jedna z novinek nové verze Androidu 4.0 Ice Cream Sandwich je možnost využít k odemknutí telefonu tvář.

Odemykání telefonu pouhým "pohledem" je na první pohled velmi efektní. Uživatel se nemusí pamatovat žádný bezpečnostní kód, displeje se vůbec nemusí dotknout. Stačí telefon zapnout, nasměrovat ho na svou tvář a dojde k odemčení.

Z hlediska bezpečnosti se ale nejedná o nejlepší způsob zabezpečení. Existují případy, kdy k odemčení zařízení stačilo mít pouze fotku majitele telefonu a jelikož současná technologie, když obraz snímá jen za pomocí kamery, nemá žádnou rozumnou možnost, jak rozeznat 2D fotografii od 3D modelu tváře. Ostatně sám systém Android při použití odemknutí za pomocí rozeznání obličeje upozorní, že to není způsob, na který se dá bezpečně spolehnout.

Navíc bude patrně problém i u telefonů během jejich odemykání v šeru nebo ve tmě. [24]

Tab. 7- Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Zabezpečení tváří				
Silné zabezpečení	**Obtížné prolomení ochrany**	**Správná funkčnost**	**Snadné zapamatování**	**Rychlé odemčení**
1	1	1	2	1
Výsledek: **1,139**				

5.3.3 Výsledná komparace a sestupné seřazení

Zde jde již vidět výsledná tabulka, ve které jsou vypsány jednotlivé druhy zabezpečení a jejich výsledné hodnocení, které bylo získáno díky multikriteriálnímu hodnocení. Jednotlivým způsobům zabezpečení bylo v tabulce přiřazeno pořadové číslo, a to na základě výsledného hodnocení. Čím vyšší hodnocení zabezpečení má tím lepší je.

Tab. 8 - Výsledky hodnocení jednotlivých zabezpečení [vlastní]

Druh zabezpečení a pozice	Hodnocení
1. Heslo	1,694
2. Číslo PIN	1,500
3. Otisk prstů	1,500
4. Znak	1,222
5. Odemknutí tváří	1,139
6. Podpis	0,861

Na posledním místě se umístilo zabezpečení pomocí podpisu. Důvodů, proč je tento druh zabezpečení špatný je několik, například:

- **Síla zabezpečení je velice malá** – Stačí, aby si kdokoliv zjistil, jaký je podpis majitele mobilního zařízení a jen tento podpis napsal na displej. S tím souvisí zároveň i **velká pravděpodobnost prolomení této ochrany.**
- **Funkčnost a spolehlivost** je velice malá. Pro úspěšné odemčení mobilního zařízení je důležité napsat přesný vzor podpisu na displej. Ve spěchu je velice obtížné tento vzor podpisu napsat, proto je důležité soustředit se na psaní, a na co nejlepší napodobení uloženého vzoru.

Jak jde v této tabulce vidět, na prvním místě se umístilo **zabezpečení pomocí hesla**. Ze všech způsobů zabezpečení dostalo nejvyšší hodnocení.

Důvody, proč je tento druh zabezpečení jedním z nejlepších, jsou:

- Síla tohoto zabezpečení je velmi velká.
- Prolomení tohoto druhu ochrany je velmi obtížné.
- Funkčnost a spolehlivost je výborná.

Samozřejmě i toto zabezpečení má své negativní vlastnosti, jako jsou:

- Někdy těžká zapamatovatelnost hesla.
- Velmi nízká rychlost odemykání.

Jelikož tento způsob zabezpečení se umístil na prvním místě a je tedy nejlepším z ostatních způsobů zabezpečení, je potřeba si ho dále analyzovat a zjistit jeho silné a slabé stránky. Proto bude dále analyzováno v další kapitole pomocí SWOT analýzy.

5.4 SWOT analýza pro zabezpečení heslem

Jelikož v předchozí kapitole vyšlo díky multikriteriálnímu hodnocení, že nejlepším druhem zabezpečení obrazovky proti vniknutí cizí osoby je zabezpečení pomocí hesla, tak je potřeba si tento druh zabezpečení více rozebrat a dále analyzovat. Pro analýzu byla vybrána metoda SWOT.

Samotná SWOT analýza je rozdělena na interní a externí faktory a také na pozitivní a negativní faktory.

Dále zde jsou vytvořeny čtyři kvadranty, v nichž jsou vypsány silné stránky, slabé stránky, příležitosti a hrozby.

Obr. 11 - SWOT analýza [vlastní]

Postup:

U silných stránek a příležitostí byla použita kladná stupnice od 1 do 5, kde 5 znamená nejvyšší spokojenost a 1 nejnižší spokojenost.

U slabých stránek a hrozeb byla použita záporná stupnice od -1 (nejnižší nespokojenost) až -5 (nejvyšší nespokojenost).

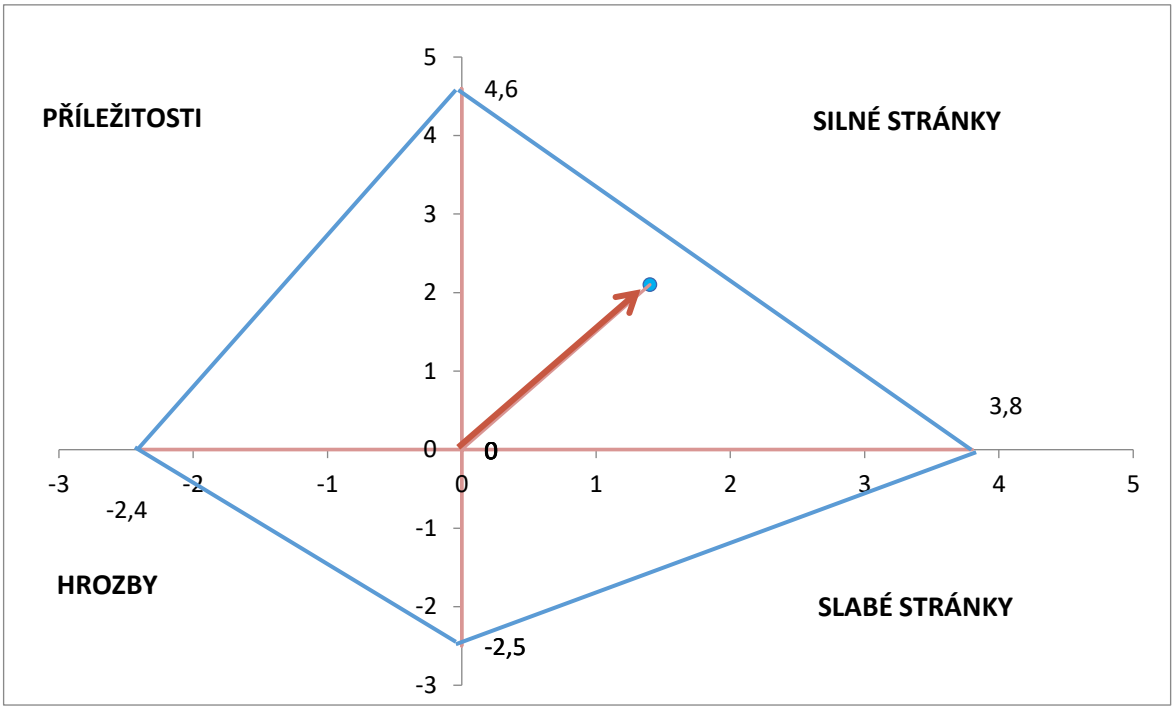
Ke každé silné a slabé stránce, hrozbám a příležitostem se přiřadí váha od 0 do 1. Čím důležitější stránka je, tím výší koeficient se přiřadí. Součet vah v každé části se musí rovnat 1.

Dále:

- Se vynásobí hodnota váhy s hodnocením.
- U každé položky vynásobené hodnoty se sečte:
  1. Interní část SWOT analýzy (slabé a silné stránky)
  2. Externí část SWOT analýzy (příležitosti a hrozby)

Tab. 9 - Hodnocení výsledků SWOT analýzy [vlastní]

Silné stránky	**Váha**	**Hodnocení**	**Součin**
Síla zabezpečení	0,4	2	0,8
Malá pravděpodobnost zapamatování cizí osobou	0,3	5	1,5
Zabránění dalšího zadávání po pěti pokusech	0,3	5	1,5
Součet			**3,8**
Slabé stránky			
Těžší na zapamatování	0,6	-2	-1,2
Velká pravděpodobnost chyby při zadávání	0,2	-3	-0,6
Potřeba delšího času na zadání hesla	0,2	-3	-0,6
Součet			**-2,4**
Příležitosti			
Variabilita při volbě hesla	0,1	1	0,1
Možnost vytvoření velmi silného hesla	0,4	5	2
Možnost častého měnění hesla	0,5	5	2,5
Součet			**4,6**
Hrozby			
Možnost zapomnění hesla	0,5	-2	-1
Možnost poznání hesla díky mastným otiskům	0,5	-3	-1,5
Součet			**-2,5**
Interní		**1,4**	
Externí		**2,1**	
Celkem		**3,5**	



Obr. 12 - Graf výsledku SWOT analýzy [vlastní]

Ve výsledku jde vidět, že tento způsob zabezpečení má hodně silných stránek, ale nejlépe si tento druh zabezpečení vede z hlediska příležitostí, které jednoznačně znázorňují dobrou kvalitu tohoto druhu ochrany.

Slabé stránky nám ukazují, že zabezpečení heslem je poměrně složité a zdlouhavé. To je ovšem ekvivalentní ke kvalitě tohoto zabezpečení.

Mezi příležitosti patří poměrně dobrá variabilita při volbě hesla, to znamená, že může za heslo být zvoleno, jakkoliv složité a dlouhé heslo, tedy za předpokladu splnění základních požadavků, a to alespoň čtyři znaky, z nichž aspoň jeden musí být písmeno.

Jak je napsáno výše, jedná se o poměrně dobré zabezpečení, to dokazuje nízký počet hrozeb. Navíc tyto hrozby jsou možné jen za určitých podmínek. Zapomenutí hesla si můžeme pojistit, tak že si někam heslo napíšeme a možnost poznat heslo podle otisků prstů je možné jen pokud se jedná o jednoduché heslo.

5.5 Návrhy pro zlepšení aktuálního stavu

Níže budou vypsány možné návrhy, jak zlepšit aktuální stav kvality tohoto druhu zabezpečení, a to především eliminací možných hrozeb, které byly zmínění výše ve SWOT analýze.

5.5.1 Zabránění zapomenutí hesla

Existuje několik způsobů, jak by se dalo zabránit zapomenutí hesla. Zvolené heslo si můžeme například uložit do databáze KeePass Password Safe, což je název pro správce hesel používaný pro Microsoft Windows. Přístup do databáze je chráněn hlavním heslem, souborem s klíčem nebo pomocí Master Key (hlavní heslo + soubor s klíčem). Další možností, jak si lépe zapamatovat heslo je používat hesla, která souvisí s prostředím, ve kterém se pohybujeme. To znamená, že by bylo vhodné používat slova, která nás napadnou při pohledu na nějaký objekt, který denně potkáváme. Toto heslo je lepší pro jistou zkombinovat s několika čísly, či speciálními znaky. Takové heslo si mnohem lépe zapamatujeme a pokud ne, stačí si pouze pamatovat s jakým objektem je heslo spojeno a na zbytek se už dá vzpomenout. [31]

5.5.2 Vznik viditelných stop na obrazovce

Z hlediska bezpečnosti je tento jev velice nebezpečný a může způsobit, že útočník rychle zjistí naše heslo. Jedním z nejlepších způsobů, jak zabránit vzniku stop na displeji je, že si budeme obrazovku co nejčastěji čistit. Po vyčištění je prakticky nemožné poznat naše heslo. Je ale samozřejmé, že nebudeme obrazovku utírat po každém použití. Čištění je nejlepší provést ve chvíli, kdy víme, že zařízení nebudeme delší dobu používat, či jestli zařízení někde nenecháme položené.

Obr. 13 - Viditelné stopy na obrazovce [27]

5.6 Analýza přístupu uživatelů mobilních zařízení k bezpečnosti osobních údajů

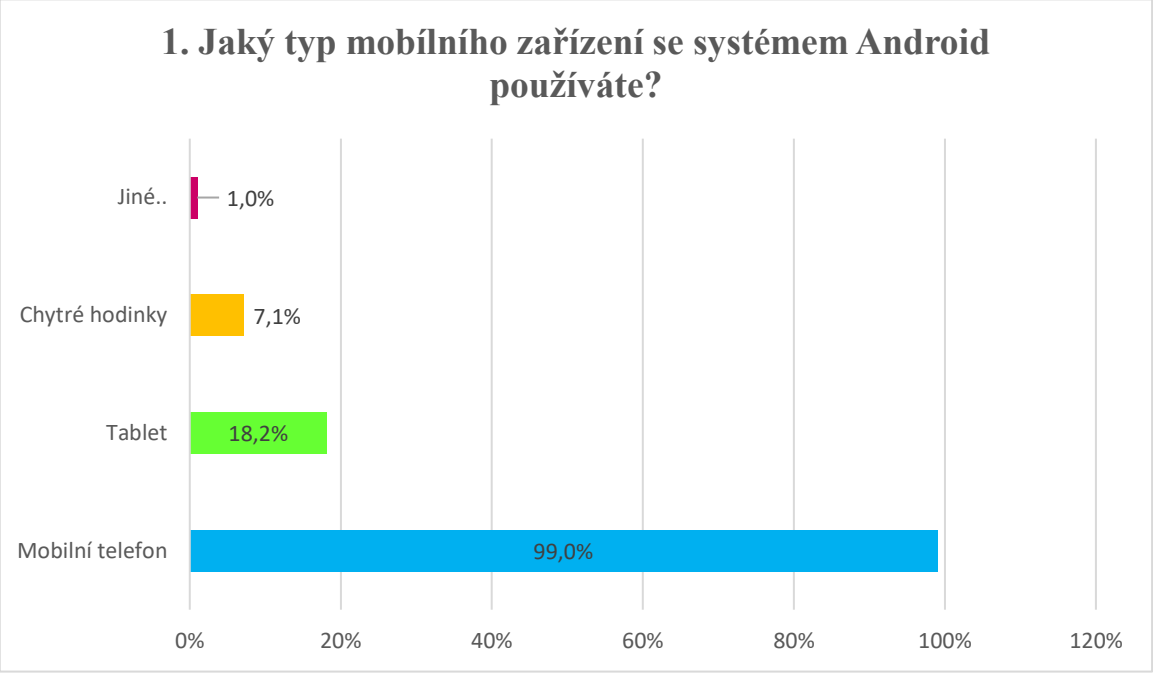
Součástí praktické části je i dotazník. Tento dotazník, byl vytvořen s cílem analyzovat přístup majitelů mobilních zařízení se systémem Android, k bezpečnosti jejich osobních dat a informací umístěných v paměti zařízení.

Samotný dotazník byl vytvořený přes on-line platformu pro tvorbu dotazníků Survio. Jeho vyplňování probíhalo on-line, a to právě díky této službě. Tento dotazník byl distribuován pomocí sociálních sítí. Respondentem mohl být kdokoliv, kdo měl zájem tento dotazník vyplnit a zároveň byl majitelem mobilního zařízení se systémem Android.

Respondenty byly pouze uživatelé mobilních zařízení se systémem Android, aby bylo získáno, co nejvíce reálných odpovědí.

Dotazník se skládá z deseti otázek, na které se odpovídá buď výběrem jedné z odpovědí, nebo výběrem více možných odpovědí. Poslední otázka slouží pro zjištění, jak uživatelé mobilních zařízení hodnotí bezpečnost vlastních mobilních telefonů, tabletů či jiných zařízení.

Ne tento dotazník odpovídalo 99 respondentů ze 99 možných.

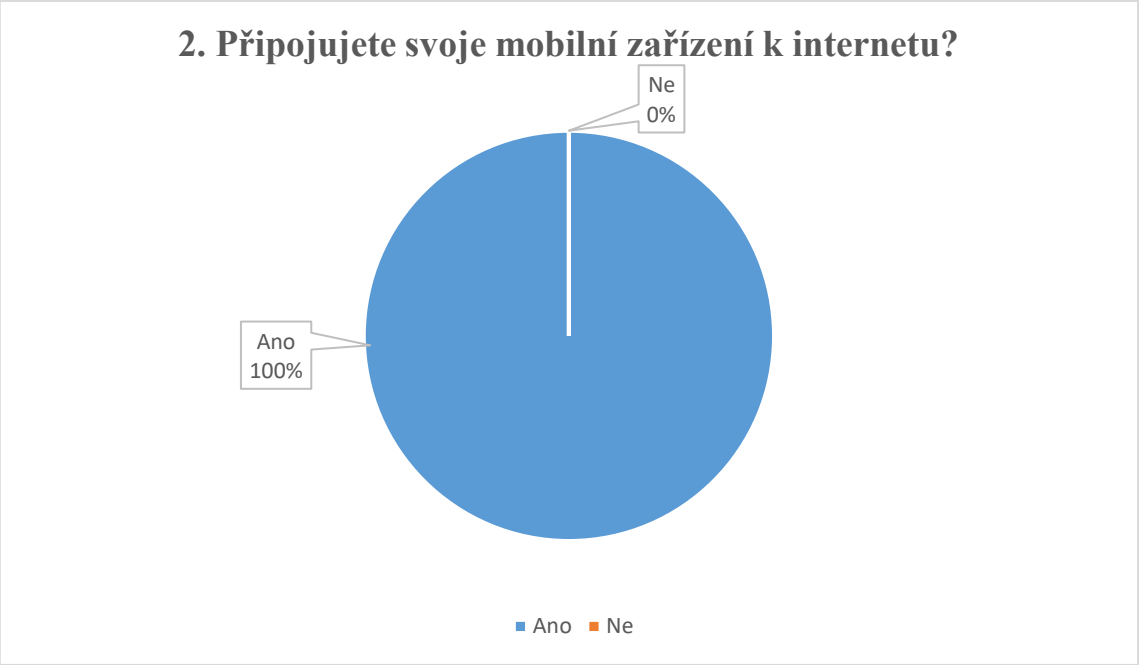


Obr. 14 - Graf odpovědí na otázku č. 1 [vlastní]

První otázka slouží pro základní zjištění, jaká zařízení uživatelé systému Android používají. Z celkového počtu 99 respondentů, 98 používá mobilní telefon. Tento počet tvoří tedy 99 %

dotázaných. Tablet využívá 18 tázaných. Chytré hodinky využívá už jen 7 uživatelů a jeden z respondentů uvedl, že využívá chytrý náramek.

Díky této otázce bylo zjištěno, že skoro každý z respondentů používá mobilní telefon. Důležitější je ale informace, že někteří uživatelé používají nejen mobilní telefon, ale i tablet, či chytré hodinky.

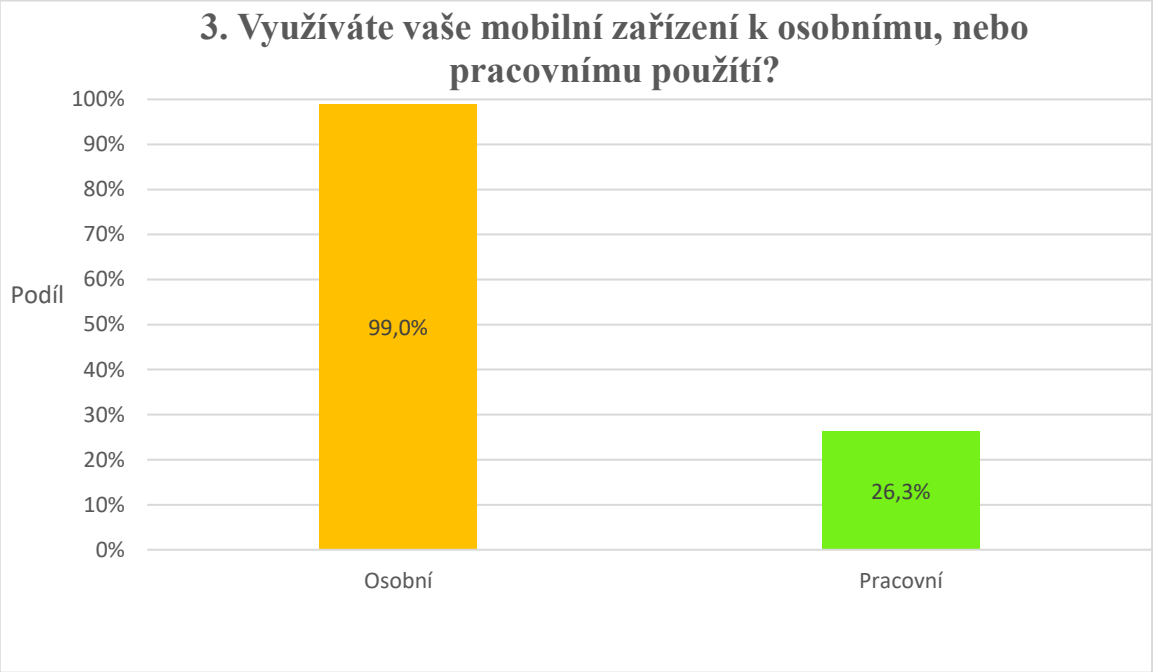


Obr. 15 - Graf odpovědí na otázku č. 2 [vlastní]

Tato otázka pouze dokazuje skutečnost, že 100 % z dotázaných majitelů mobilních zařízení se systémem Android připojuje k internetu svá chytrá zařízení. Každé zařízení je tím pádem vystaveno možným hrozbám, spojených se zneužitím, či odcizením osobních údajů či informací prostřednictvím internetu. Kdyby například mobilní telefon nebyl připojován k internetu, bylo by eliminováno riziko odcizení osobních údajů ze zařízení pomocí většiny technik sociálního inženýrství. Zároveň by bylo velice obtížné do tohoto zařízení importovat škodlivý software.

Z toho nám vychází, že mobilní zařízení, které není připojeno k internetu, je velice bezpečné a osobní údaje, jsou v tomto zařízení naprosto v pořádku než právě v zařízení, které je připojeno k internetu. Skutečnost je ale taková, že mobilní zařízení, jsou v dnešní době již vyráběna pro to, aby byla připojována k internetu. A podle výsledků z dotazníku, je lehké dokázat tu skutečnost, že každé moderní mobilní zařízení je připojováno k internetu. Mohou sa-

možřejmě existovat výjimky, ale jelikož z 99 dotázaných, všichni své zařízení připojují k internetu, bude tuto výjimku tvořit velice malý počet majitelů mobilních zařízení se systémem Android v celém světě.



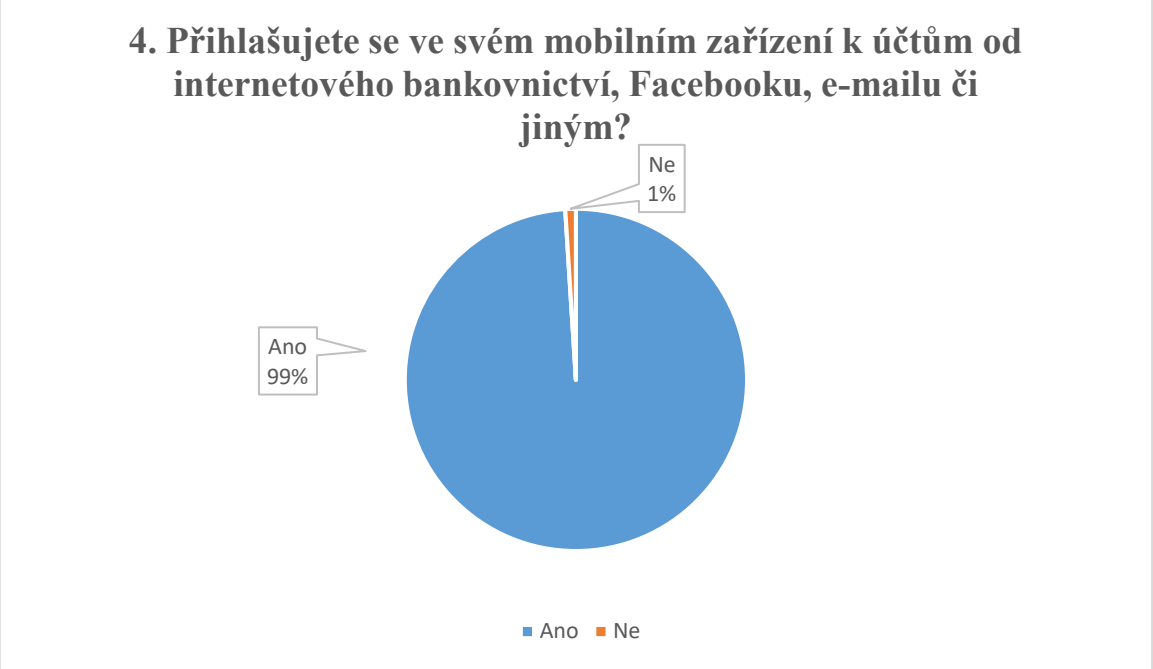
Obr. 16 - Graf odpovědí na otázku č. 3 [vlastní]

Díky této otázce bylo zjištěno, kolik lidí přibližně využívá svoje mobilní zařízení pro osobní použití a kolik pro pracovní. Rozdíl mezi těmito dvěma způsoby využití z hlediska bezpečnosti informací je především ten, že zařízení využívaná pro osobní využití mohou potenciálně ohrozit pouze majitele zařízení, případně jeho blízké. Zatím co zařízení využívána k pracovnímu použití mohou způsobit únik informací o celé firmě, či organizaci. Z hlediska možného uniku informací je tedy využívání mobilních zařízení pro pracovní využití mnohem rizikovější.

Podle počtu responzí a následného grafu počtu odpovědí je možné vidět, že z 99 uživatelů využívá své mobilní zařízení pro pracovní použití jen 26 respondentů. Samozřejmě v některých profesích je využívání mobilních zařízení nepotřebné, ale skutečnost je taková, že mobilní zařízení jsou čím dál více využívané v různých profesích, a dokonce se zvyšuje i počet profesí, které jsou na mobilních zařízeních závislé. Se vzrůstajícím počtem těchto závislých profesí roste i pravděpodobnost úniku důležitých interních informací z různých subjektů.

Dalo by se tedy čekat zvýšení počtu útoků na různé firmy a na jejich interní údaje a informace. Na toto riziko je potřeba odpovědět, a to celkově zlepšením ochrany těchto interních údajů a informací právě zlepšením zabezpečení mobilních zařízení se systémem Android.

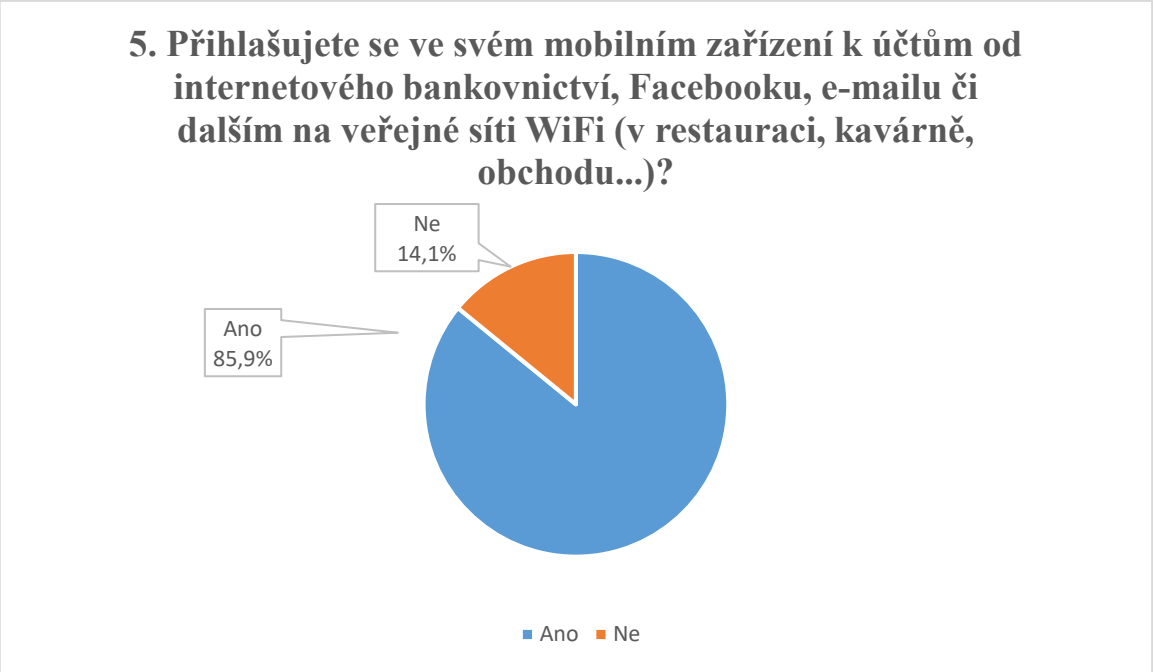
To nejjednodušší, co se dá proti tomuto riziku dělat je, že se zvýší povědomí o této problematice a všechny zaměstnanci budou seznámeni s tímto možným rizikem. Právě techniky sociálního inženýrství vycházejí z nevědomosti a nepozornosti uživatelů mobilních zařízení, a proto stačí pouze, aby člověk věděl, že ho může někdo podvést a ukrást důležité informace, za které může právě tento člověk zodpovídat.



Obr. 17 - Graf odpovědí na otázku č. 4 [vlastní]

Na výsledky předchozí otázky, týkající se počtu připojovaných mobilních zařízení, navazuje tato otázka. Slouží společně s následující otázkou ke zjištění, zda se připojují uživatele mobilních zařízení se systémem Android k různým účtům jako je účet na Facebooku, e-mailu anebo internetového bankovnictví. Z výsledků této otázky bude vycházet několik dalších otázek z celého dotazníků.

Výsledky této otázky jsou celkem jednoznačné. 98 z 99 respondentů připojuje své zařízení k různým účtům. Samotné připojování těchto mobilních zařízení k těmto účtům, není tak velké riziko. Záleží ovšem, kde se k těmto účtům připojujeme. Zda je to veřejná síť anebo domácí síť. Rozdíl mezi těmito dvěma druhy připojení bude vysvětleno v následující otázce.



Obr. 18 - Graf odpovědí na otázku č. 5 [vlastní]

V předchozí otázce bylo zjištěno, že 98 z 99 respondentů připojuje své zařízení k různým účtům.

Tato otázka sloužila ke zjištění, kolik z těchto lidí připojuje svá zařízení k různým účtům na veřejných místech, jako jsou kavárny restaurace anebo bary. Ze znění otázky můžeme vydedukovat, že právě připojování k účtům na veřejných sítích je mnohem nebezpečnější.

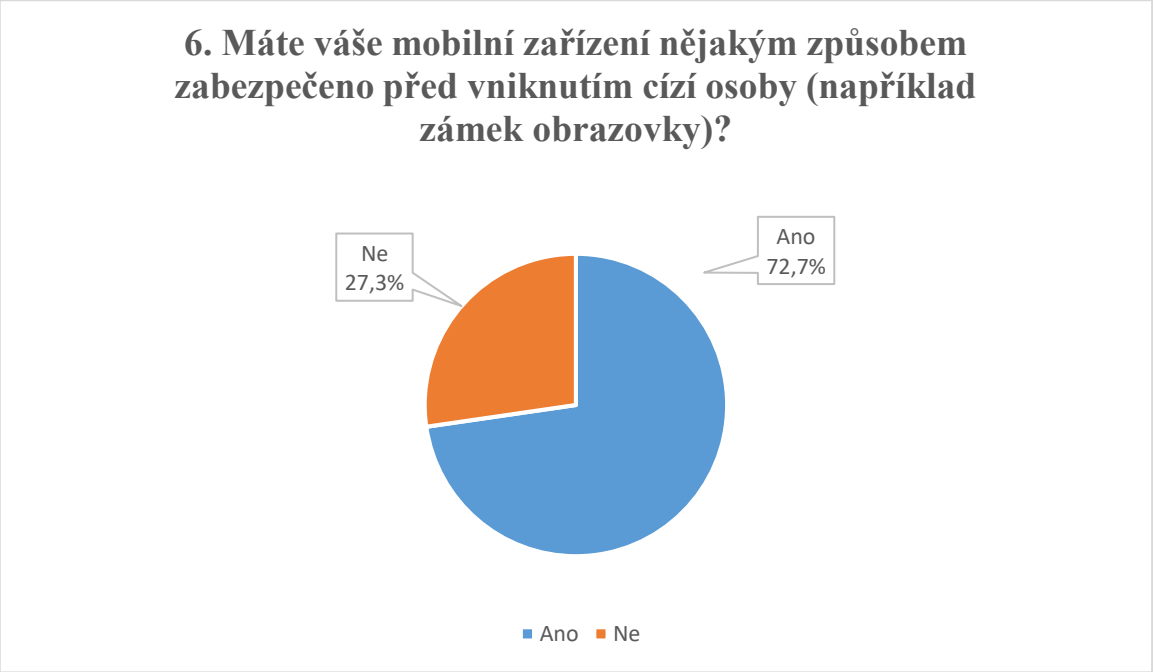
Na veřejné Wi-Fi platí, že každé připojené zařízení může teoreticky patřit útočníkovi, který odposlouchává vaše zařízení a sleduje data šířená Wi-Fi sítí. Na veřejné síti je mnohdy přístup k internetu zdarma, ovšem je otázkou, jestli riziko, kterému se uživatel vystavuje, stojí za to. Data se v rámci Wi-Fi sítě šíří vzduchem a pro zkušenější uživatele není až takový problém odposlouchávat přenášená data mezi uživatelovým zařízením a routerem. Samozřejmě to není tak, že je ke každé volně přístupné Wi-Fi připojen i nějaký útočník, který odposlouchává data, nicméně ta šance tu je, jelikož uživatelé připojení k veřejně přístupné Wi-Fi síti jsou jednoduchým cílem útoku. Naštěstí je v dnešní době většina komunikace s důležitými servery jako Gmail, Seznam, Facebook atd. zabezpečená (skrz protokol HTTPS), ale představte si situaci, kdy se na veřejné Wi-Fi síti připojíte k serveru, který šifrované spojení nepoužívá a kde používáte stejné heslo, jaké používáte i ke svému e-mailu. Útočník může takové heslo odposlechnout a pak už jen vyzkoušet, jestli se s ním náhodou nedostane do vaší e-mailové schránky. Tím získá přístup k vaší digitální identitě, neboť s pomocí vašeho

e-mailu může ovládat všechny služby, do nichž jste se pomocí tohoto e-mailu registrovali. [16]

Dalším způsobem, jakým může být ohrožen uživatel mobilního zařízení přihlašujícího se k různým účtům na veřejné síti je, že si útočníci na nějakém veřejném místě zřídí vlastní otevřenou Wi-Fi síť, která slouží výhradně k útokům na uživatele. Název sítě může evokovat, že jde o oficiální službu poskytovanou např. provozovatelem letiště, kavárny nebo obchodního centra. Uživatel se tedy domnívá, že se přihlašuje na Wi-Fi patřící například kavárně, ve skutečnosti je to ale síť patřící útočníkovy. Dojde tedy přihlášení uživatele přímo na síť útočníka a ten už jen sleduje pohyb uživatele mobilního zařízení na internetu. Tím útočník získá všechny hesla k různým účtům a velké množství osobních informací. [17]

Proto je důležité dávat si pozor na veřejných sítích na své osobní informace a hesla od různých účtů. Mohou být kdykoliv zneužity, a to bez vědomí samotného majitele mobilního zařízení.

Samozřejmě existují různé způsoby, jak se chránit před útočníky na těchto veřejných sítích, ale ten nejjednodušší je právě zvýšit povědomí o této problematice a hlavně, být si vědomí možného napadení.



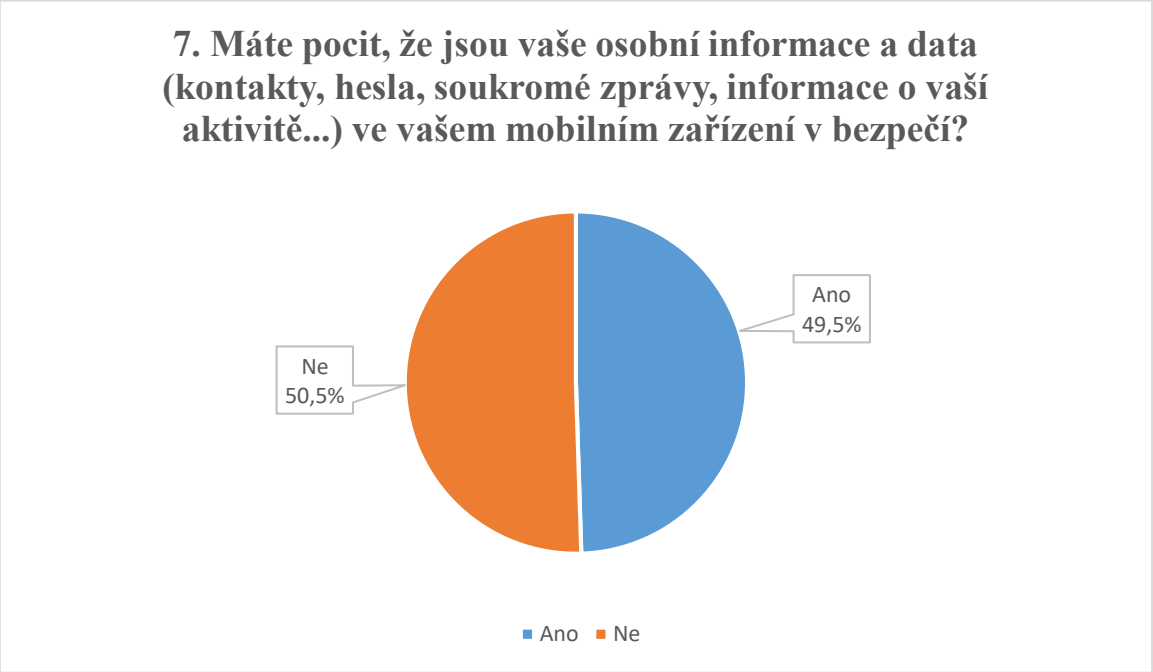
Obr. 19 - Graf odpovědí na otázku č. 6 [vlastní]

V případě, že uživatel nepřipojuje své zařízení k internetu, či se nepřipojuje k různým účtům, může být i tak stále napaden a jeho osobní údaje mohou být opět jednoduše odcizeny. Tyto

způsoby napadení se již ale nevyhnou přímého kontaktu útočníka s cílovým mobilním zařízením. To znamená, že útočník například ukradne někomu jeho mobilní telefon a přímo začne vyhledávat informace a údaje, které potřebuje. Pokud nemáme mobilní zařízení nějakým způsobem zabezpečené proti vniknutí cizí osoby, je tak pro útočníka nesmírně jednoduché získat potřebné informace a v jeho cestě za získáním těchto informací nestojí žádná překážka.

V případě, že má majitel mobilní zařízení zabezpečeno proti vniknutí cizí osoby, ztíží tím cestu útočníkovi, při jeho pokusu odcizit osobní údaje a informace. I tak ale není uživatel naprosto v bezpečí. Útočníci zde využívají například různých chyb v zabezpečení, jednotlivých verzí operačního systému Android, nebo přímím sledováním uživatele při odemykání jeho mobilního zařízení.

Porovnání jednotlivých způsobů zabezpečení obrazovky bylo analyzováno v předchozí kapitole pomocí multikriteriálního hodnocení a SWOT analýzy.



Obr. 20 - Graf odpovědí na otázku č. 7 [vlastní]

Následující otázky slouží už jen pro zjištění, jak uživatelé mobilních zařízení se systémem Android hodnotí bezpečnost těchto zařízení a celkově systému Android, a to především z hlediska bezpečnosti informací. Jde taky o zjištění, zdali si jsou majitelé mobilních zařízení se systémem Android vědomi možných rizik. Protože právě seznámení s možnými riziky je nejlepším řešením, jak se chránit před možnými útoky.

Na otázku, zda se mají uživatelé mobilních zařízení se systémem Android pocit, že jsou jejich osobní informace a data (kontakty, hesla, soukromé zprávy, informace o vaší aktivitě...) v jejich mobilních zařízeních v bezpečí, odpovídalo opět 99 respondentů. Výsledky této otázky jsou velice vyrovnané. 49 respondentů si myslí, že jsou jejich osobní informace v zařízení v bezpeční a 50 respondentů mají pocit, že ne.

V podstatě by se dalo říct, že 50 respondentů má pocit, že jsou jejich osobní informace v nebezpečí. Tím pádem, jsou si vědomi nějakého možného rizika, které může jejich mobilní zařízení postihnout. Otázkou už je jen, zda tito uživatelé znají přesně, jakým způsobem mohou být napadeni, či mají jen zdánlivý pocit možného rizika, ale nezná jeho přesnou podobu.

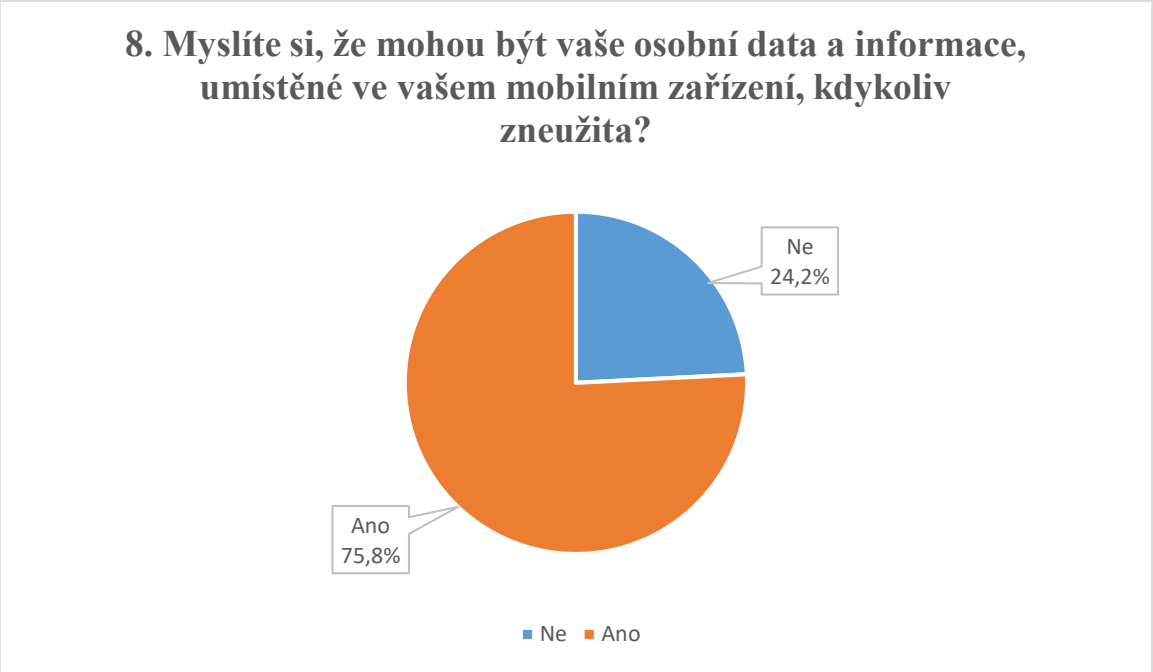
Otázkou zůstává 49 respondentů, kteří mají pocit, že jsou jejich osobní informace v zařízení v bezpečí. Může se jednat o uživatele, kteří mají povědomí o možným riziku, ale podnikají dostatečné kroky pro zabezpečení jejich informací a tím pádem se cítí v bezpečí, anebo si možné riziko vůbec neuvědomují a tím pádem nepodnikají žádné kroky pro eliminaci možného napadení jejich zařízení útočníkem.

Je potřeba tedy posoudit, jaká kategorie uživatelů odpovídajících na tuto otázku je více v nebezpečí z hlediska bezpečnosti informací uložených v jejich zařízení. Mohlo by se jednat o respondenty odpovídající na otázku pozitivně, tedy odpovědí Ano.

To především z několika důvodů:

- Tito uživatelé si nejsou vůbec vědomi možného rizika.
- Jsou si vědomi možného rizika, ale nepřipouští si ho.
- Nejsou si vědomi velkého množství osobních informací umístěných v jejích zařízení, které může být odcizeno.

Ovšem jak bylo zmíněno výše, může se jednat o uživatele, kteří podnikají dostatek kroků, pro eliminaci pravděpodobnosti možnosti napadení jejich mobilního zařízení útočníkem.



Obr. 21 - Graf odpovědí na otázku č. 8 [vlastní]

V této otázce bylo zjištěno, že i když podle předchozí otázky si 49 uživatelů myslí, že jsou jejich osobní informace v bezpečí, tak podle této otázky si už někteří uživatele ze zmíněných 49 myslí, že mohou být kdykoliv jejich údaje zneužity. Pokud si uživatel myslí, že nejsou jeho údaje v bezpečí, je velmi pravděpodobné, že si bude myslet, že mohou být jeho údaje také kdykoliv zneužity. Pokud si, ale uživatel myslí, že jsou jeho údaje v bezpečí, ale zároveň si myslí, že mohou být kdykoliv zneužity, znamená to, že buď:

- Uživatel má povědomí o možném riziku, dává mu ale velice malou váhu, která ho nepřesvědčí o tom, že jsou jeho údaje v nebezpečí.
- Uživatel nedává svým osobním údajům příliš vysokou váhu a nebojí se jejich odcizení a zneužití.

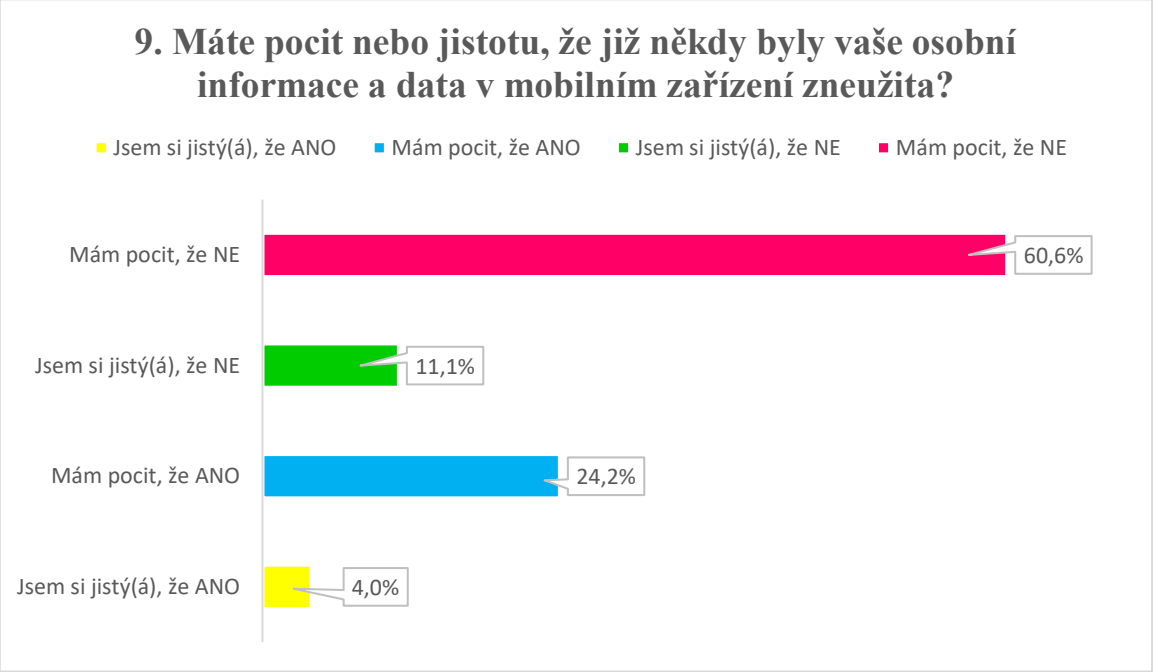
Ve výsledku 75 respondentů si myslí, že mohu být jejich osobní data a informace kdykoliv zneužita. Což vypovídá o poměrně dobré informovanosti uživatelů mobilních zařízení se

systémem Android v oblasti bezpečnosti informací a osobních údajů uložených v jejich zařízení.

24 respondentů má pocit, že jejich osobní údaje nemohou být kdykoliv zneužity. Opět to může znamenat, že jsou tito uživatelé dobře informovaní a dostatečně seznámeni s problematikou ochrany osobních údajů a informací umístěných ve vlastních mobilních zařízeních. To by znamenalo, že ví přesně, kdy mohou nebo nemohou být napadeni.

Existuje ale i možnost, že tito respondenti si nejsou vůbec vědomi možné hrozby, a proto si myslí, že jsou jejich osobní údaje a informace v bezpečí. Nicméně je těchto lidí méně, což je z hlediska znalosti možných rizik v oblasti bezpečnosti informací dobré.

Více lidí si myslí, že mohou být jejich údaje zneužity, a právě vědomí těchto uživatelů o možném riziku je to nejdůležitější pro snížení pravděpodobnosti napadení mobilního zařízení útočníkem s cílem odcizit naše osobní údaje a informace.



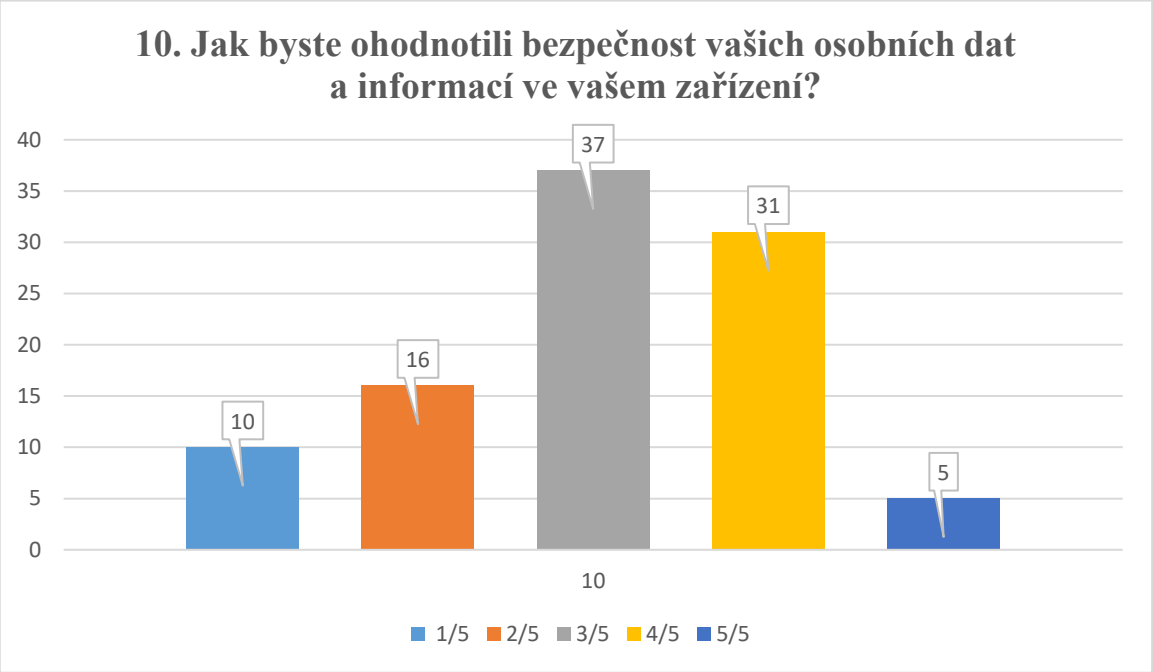
Obr. 22 - Graf odpovědí na otázku č. 9 [vlastní]

Tato otázka je z hlediska získání co nejvíce informací o vztahu uživatelů mobilních zařízení se systémem Android, jedna z nejdůležitějších. Jde zde o zjištění, zda si jsou respondenti jistí, nebo zda mají pocit, že byly jejich osobní údaje zneužity. Podle grafu výsledků otázky jde vidět, že jistotu má pouze jeden uživatel z 99 tázaných. Což dokazuje, že i když se možná některý z uživatelů stal obětí útočníka a byly mu zneužity osobní údaje, není si touto možnou skutečností jistý.

60 respondentů má pocit, že jejich osobní informace nikdy nebyly zneužity. Jistotu má ovšem jen 11 odpovídajících.

Z výsledů je také zajímavé sledovat fakt, že 24 respondentů z 99 si myslí, že byly jejich údaje zneužity, ale nejsou si jistí. To dokazuje, že určití uživatele mají povědomí o možném riziku, a dokonce si myslí, že se byli již postiženi tímto rizikem. Je ale poměrně těžké dokázat tuto skutečnost, a proto má tak málo uživatelů jistotu, že byly jejich údaje zneužity.

Opět je ale důležité zdůraznit, že informovanost v oblasti ochrany osobních údajů a znalost způsobu, jak se chránit před možným útokem je na nízké úrovni.



Obr. 23 - Graf odpovědí na otázku č. 10 [vlastní]

Tato otázka sloužila pouze pro zjištění celkového dojmu z bezpečnosti osobních údajů, uživatelů mobilních zařízení se systémem Android. Respondenti odpovídali na tuto otázku formou hodnocení. Jedna hvězda znamenala, že jsou uživatelovi osobní údaje v nebezpečí a pět hvězd znamenalo, že jsou podle názoru uživatele, jeho osobní informace v bezpečí.

Pokud se ale podíváme na jednotlivé odpovědi, tak i přes neutrální výsledek, je vidět, že například 5 respondentů má pocit, že jsou jejich údaje naprosto v bezpečí, a naopak proti tomu, má 10 respondentů pocit, že jsou jejich údaje v nebezpečí.

Více uživatelů jsou, ale v oblasti ochrany osobních údajů a informací více optimističtí a hodnotí bezpečnost těchto informací v zařízeních se systémem Android spíše kladně.

Výsledek, jak jde vidět, je neutrální. Uživatelé nemají v průměru naprostý pocit bezpečí, ale ani naprosto pocit ohrožení.

Z výše uvedených hodnocení je možné udělat celkový průměr. Ten vyšel 3,1. Výsledek, jak jde vidět, je neutrální. Uživatelé nemají v průměru naprostý pocit bezpečí, ale ani naprosto pocit ohrožení.

Celkové vyhodnocení dotazníku

Díky tomuto dotazníku bylo zjištěno velké množství reálných informací. Na otázky odpovídali běžní uživatelé mobilních zařízení se systémem Android. Bylo tak díky tomu dosaženo co nejreálnějších a přesně vypovídajících výsledků, díky kterým je možné lépe poznat vztah uživatelů mobilních zařízení se systémem Android k bezpečnosti osobních informací a údajů umístěných v těchto zařízeních.

Konečně by se tedy tento vztah uživatelů dal popsat, tak že malé povědomí mezi těmito uživateli existuje. Někdo tomuto povědomí dává větší váhu a někdo menší. Vyskytují se zde i ale případy, kdy někteří uživatelé nemají absolutně žádné povědomí o možném riziku odcizení osobních údajů přímo z jejich zařízení.

Nejjednodušším řešením problému nízkého povědomí o možném riziku odcizení a zneužití osobních informací je právě zlepšení informovanosti, a hlavně seznámení s těmito možnými riziky.

Jak bylo napsáno výše, pravděpodobnost výskytu rizika nejlépe eliminujeme zvýšením povědomím o tomto riziku a seznámením s možnými cestami, jakými mohou být uživatelé napadeni. Pokud nebude uživatel mobilního zařízení seznámen s tím, že může být například na veřejné síti velice lehce napaden a tím může být jeho digitální identita odcizena, nebude schopný se tomuto riziku bránit a v nejhorším případě u takového uživatele dojde k odcizení osobních údajů, a to bez jakéhokoliv vědomí.

Zvýšení povědomí o této problematice a názorným ukázním možných cest přístupu útočníka k osobním informacím je právě jedním z cílů této práce. A právě takovým způsobem se může zlepšit bezpečnost mobilních zařízení a osobních údajů umístěných v paměti těchto přístrojů.

5.7 Doporučení pro zlepšení zabezpečení

V této části práci bude vypsáno a vysvětleno několik tipů pro uživatele mobilních zařízení se systémem Android, jak zvýšit bezpečnost jejich zařízení. Na začátku jsou vypsány obecné doporučení pro zlepšení bezpečnosti mobilních zařízení, dále se doporučení bude týkat možného zabránění napadení škodlivým softwarem. Na závěr bude vypsáno několik tipů, jak poznat škodlivou aplikaci na Google Play.

5.7.1 Obecné tipy pro lepší zabezpečení zařízení

Existuje několik možných a jednoduchých kroků, díky kterým se z našeho mobilního zařízení může stát více bezpečnější přístroj u kterého se už uživatel nebude muset bát ztráty osobních dat a informací.

Zálohování a synchronizace dát

Velká většina uživatelů pravidelně nezálohuje svá data. V dnešní době se dá o data přijít kdykoliv. Zálohování se může zdát časově náročné a zastrašující, ale vůbec to tak není.

Odborníci doporučují pravidlo 3-2-1 na zálohování:

- tři kopie dokumentů,
- dvě lokálně (na různých zařízeních)
- a jedna mimo lokality.

Pro velký počet lidí to znamená mít původní data uložená v počítači, zálohu na externím pevném disku a další data uložená na cloudu. S takovým systémem je velmi nepravděpodobné, že se ztratí všechny údaje v případě, že bude zařízení ztraceno nebo poškozeno. [19]

Vypínaní automatického připojení na Wi-Fi, Bluetooth

Poslední radou při zabezpečení mobilního operačního systému je zvýšená pozornost při připojování k nezajištěným sítím. Velká většina uživatelů zapomíná po práci s mobilním zařízením vypínat Wi-Fi a může se stát, že se zařízení připojí k nezabezpečené síti. Většina těchto sítí sice nebezpečná být nemusí, ale může se stát, že se útočník velmi lehko pomocí nezajištěného připojení dostane k citlivým informacím. Pokud už se uživatel chce připojit na takto nezabezpečenou síť, doporučuje se nepracovat s citlivými údaji. [28]

Ochrana proti krádeží a ztrátě mobilního zařízení

Doporučeným krokem před ztrátou nebo krádeží mobilního zařízení jsou programy třetích stran s funkcemi Anti-Theft. Tyto programy dokáží pomocí GPS zjistit stav zařízení, jeho poslední známou polohu, poslední navštívené stránky. Dokáže odesílat fotografie z předního a zadního fotoaparátu, a dokonce má možnost poslat zprávu při špatně zadaném hesle nebo neznámé SIM kartě s informacemi o ní.

Pravidelná aktualizace operačního systému a aplikací

Aktualizace softwaru v operačním systému Android je velmi jednoduchá a stačí k tomu pouze připojení na internet. Služba Google Play se automaticky postará o to, aby byla v zařízení nainstalována aktuální verze softwaru. Samozřejmě se přímo v aplikaci dá nastavit způsob automatické aktualizace, případně její vypnutí. Tuto možnost se však nedoporučuje z důvodu zabezpečení zařízení. Mnohé ze zastaralých aplikací mohou obsahovat chyby nebo škodlivý software, což může vést ke zpomalení nebo úplnému neúčinnost zařízení. [30]

Co se týče pravidelné aktualizace operačního systému a bezpečnostních aktualizace je to, co se operačního systému týká, horší. Z důvodu rychlého vydávání novějších a novějších verzí operačního systému dochází ke ztrátě podpory pro starší verze. Také dost záleží na výrobci daného zařízení, který by měl dodržovat nasazování opravných aktualizací na zařízení. [30]

5.7.2 Ochrana proti škodlivému softwaru

Níže jsou vypsány tipy a rady díky kterým je možné předcházet riziku vniknutí škodlivého softwaru do mobilního zařízení. Tyto tipy a doporučení se budou týkat nejznámějším a nejrozšířenějším škodlivým softwarům.

Ochrana proti virům a červům

Pro ochranu zařízení proti virům se používá antivirový software, který slouží jako pomyslná brána mezi zařízením a internetem. Antivirový program, při stahování souborů nebo aplikací z internetu a před jejich uložením do zařízení, vyhledává danou aplikaci a zajistí, že se virus do zařízení nedostane. Také je dobré dbát na to, aby byl dán antivirový program, operační systém a různé další programy pravidelně aktualizovány, protože nové hrozby z internetu se objevují denně. V tomto případě se dají použít i bezpečnostní balíky firewall, které jsou určeny pro zabránění neoprávněného přístupu do nebo ze soukromé sítě. [29]

Ochrana proti Trojskému koni

V této souvislosti je první a nejlepší možností ochrany proti trojskému koni nikdy neotevírat přílohy e-mailu nebo spustit program, pokud si uživatel není jistý, z jakého zdroje pochází. Tyto typy virů jsou nyní rozšířeny nejméně, protože jejich funkce se postupem času nemění. Proto na jejich detekci a odstranění postačí antivirový program.[29]

Ochrana proti Spyware a Adware

Možná nejdůležitějším krokem v zabránění infikování zařízení spywarem je mít nainstalovaný nástroj, který dokáže detekovat a zabránit instalací škodlivého kódu do zařízení. Většina antivirových programů je účinná při identifikaci různých typů Spywaru, ale nemusí rozpoznat všechny jeho varianty. Dobrým řešením je mít nainstalovaný kromě antivirového softwaru i software pro detekci Spywaru. [29]

Spyware se do zařízení často dostává při návštěvě infikovaných nebo škodlivých webových stránek. Proto by měl být uživatel opatrný při klikání na odkazy webových stránek z neznámých zdrojů. Kromě toho je dobré stahovat programy pouze z důvěryhodných webových stránek. [29]

Je třeba dbát zvýšené pozornosti při zobrazení nežádoucího nebo náhodného upozornění a neklikat na tlačítko "Souhlasím" nebo "OK", čímž se uzavře kontextové okno. Ve skutečnosti se do zařízení nainstaluje škodlivý software. Namísto toho je dobré toto okno zavřít.

Aktualizace webového prohlížeče může také pomoci zabránit instalací Spywaru. Většina prohlížečů dokáže upozornit na škodlivé programy a navrhnout bezpečný postup v případě možné infikace.

Ochrana proti Phishingu

Výrazné snížení šance na to stát se obětí útoku typu Phishing, je být opatrný při online prohlížení a kontrole e-mailů. Je dobré neklikat na odkazy v e-mailu, pokud si uživatel není jistý, zda se jedná o autentický zdroj. Pokud má uživatel pochybnosti, je vhodné otevřít nové okno prohlížeče a zadat adresu URL do adresního řádku. [1]

Také je potřeba dávat si pozor na e-maily vyžadující důvěrné informace, zejména pokud se jedná o osobní údaje nebo bankovní informace. Legitimní organizace včetně banky, totiž nikdy nebudou požadovat citlivé informace prostřednictvím e-mailu.

Velmi mnoho e-mailů sloužících phisingu je velmi snadné rozeznat. E-maily se od těch pravých odlišují množstvím slov, velkými a malými písmeny, a vykřičníky. Mohou také obsahovat neosobní pozdrav nebo nepravděpodobný obsah.

Druhou důležitou věcí je věnovat pozornost zkráceným linkem, zejména na sociálních médiích. Útočníci často používají tyto služby na to, aby si uživatel myslel, že kliknul na legitimní odkaz, ale ve skutečnosti je neúmyslně nasměrovaný na falešnou stránku. Tyto falešné stránky jsou používány na ukradení zadaných osobních dat. [1]

Uživatel by měl vždy, pokud je to možné, používat bezpečnou webovou stránku, kterou chce prohledávat, a to hlavně při odesílání citlivých informací jako jsou osobní údaje.

Nikdy by neměl používat veřejné, nezabezpečené Wi-Fi na prohlížení bankovnictví, nakupování nebo zadávání osobních údajů. Pokud je to možné, je třeba použít internet od operátora.

Ochrana proti Ransomware

Samozřejmě nejlepší ochranou proti Ransomware je, že uživatel nebude vůbec ohrožen útokem. Dalším účinným krokem může být, zálohovat si všechny své data ať už na externí jednotky USB, nebo na cloudových uložištích. [1]

Pokud už se tedy staneme obětí útoku, útočník logicky nebude mít co ukrást, protože všechny soubory s osobními informacemi budeme mít na externím uložišti, které nebude připojeno k zařízení. [1]

5.7.3 Tipy, jak poznat potenciálně škodlivou aplikaci v Obchodě Play

Aplikace jsou jedním z nejčastějších zdrojů infekce operačního systému škodlivým softwarem. Proto nejlepším možným řešením, jak instalovat aplikace do zařízení, je přes obchod Google Play. Při instalaci aplikace je dobré dbát zvýšené pozornosti z důvodu možného stažení nechtěné aplikace, protože Google Play obsahuje ohromné množství různých aplikací, a ne všechny jsou bezpečné. K větší bezpečnosti má dopomoci i aplikace Google Play Protect, která je přímo instalována k aplikací Google Play a pravidelně kontroluje aplikace a zařízení, a hledá stopy po malwaru, proto je dobré tuto funkci povolit v nastavení aplikace. Také pomáhá sledovat hodnocení a recenze aplikace. V případě jejího nahlášení jako škodlivého softwaru více uživateli se Google touto aplikací začne zabývat. [21]

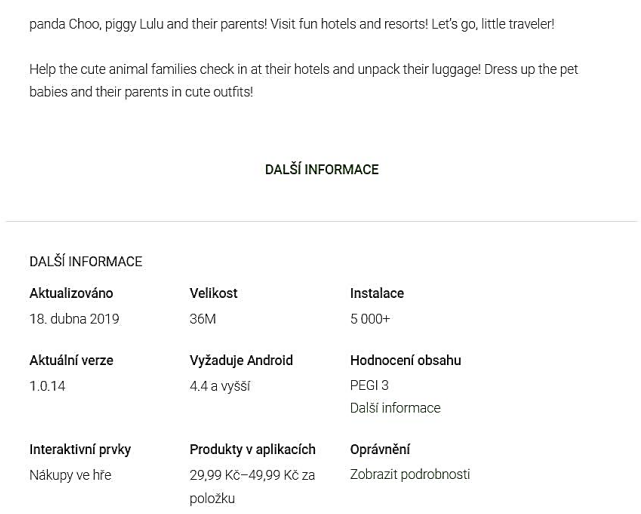
V Obchodě Play jsou stovky tisíc aplikací, které jsou sice automaticky kontrolovány na přítomnost některých známých škodlivých komponent, nicméně to nemusí být zdaleka dostačující. Na rozdíl od Apple App Store nejsou programy před publikací schvalovány tak přísně, takže zjednodušeně řečeno do Obchodu Play může nahrát aplikaci skoro kdokoli. Existuje několik tipů, jak poznat takovou škodlivou aplikaci.[21]

Hodnocení aplikace

Vcelku dobrým měřítkem kvality by mělo být hodnocení aplikace, pohybující se na stupnici od 1 (nejhorší) do 5 (nejlepší). Většinou se dá celkem dobře dedukovat, že program, který má od uživatelů špatnou známku (3,0 a méně) nejspíš nenaplní naše představy a velmi pravděpodobně nefunguje tak, jak má. [21]

Bohužel to neplatí pro aplikace s velmi vysokým hodnocením. V tomto směru se totiž někteří autoři uchylují k podvádění. Doporučuje se tedy dívat se na to, kolik uživatelů aplikaci hodnotilo. [21]

Ani to ale není jednoznačným vodítkem – pokud si autor zajistí stovky nebo tisíce kladných hodnocení, nemusíme na první pohled vidět nic podezřelého. Jak jde vidět na obrázku níže Aplikace má přes 5000 instalací a známku 5,0, ale žádné komentáře. To je důvod, proč tuto aplikaci podezřívat. [21]

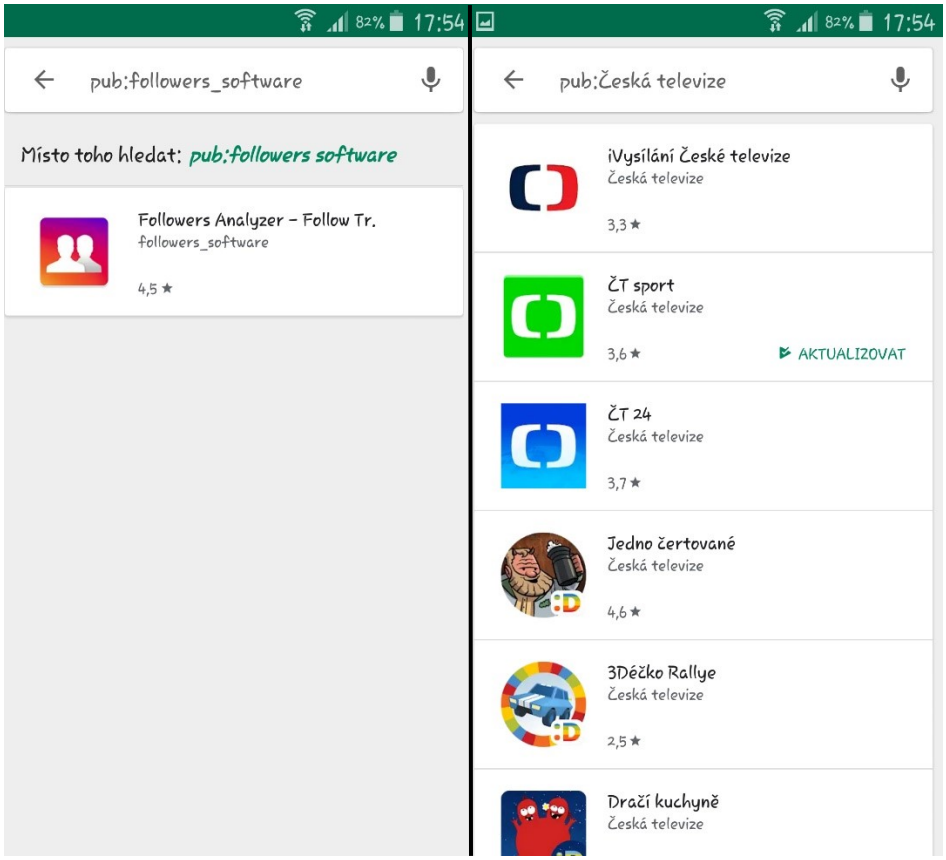


Obr. 24 - Informace o aplikaci [20]

Celkem dobrým pomocníkem mohou být komentáře uživatelů, které u zfalšovaných hodnocení obvykle zcela chybí, nebo jsou převážně negativní. [21]

Prověření autora aplikace

Snahy dostat do Obchodu Play různé podvržené či škodlivé aplikace jsou obvykle realizovány jednorázově, tedy pod jedním účtem bývá vystavena jedna aplikace. Stačí klepnout na jméno vývojáře, pod názvem aplikace je možné vidět, jaké programy v Obchodě Play publikoval. Pokud je pouze jeden, je vhodné mít se na pozoru. [21]



Obr. 25 - Vlevo podezřelý vývojář, vpravo důvěryhodný vývojář [vlastní]

Na obrázku výše jde vidět, že vývojář má jedinou aplikaci, kterou vytvořil, to je možný důvod k pozornosti.

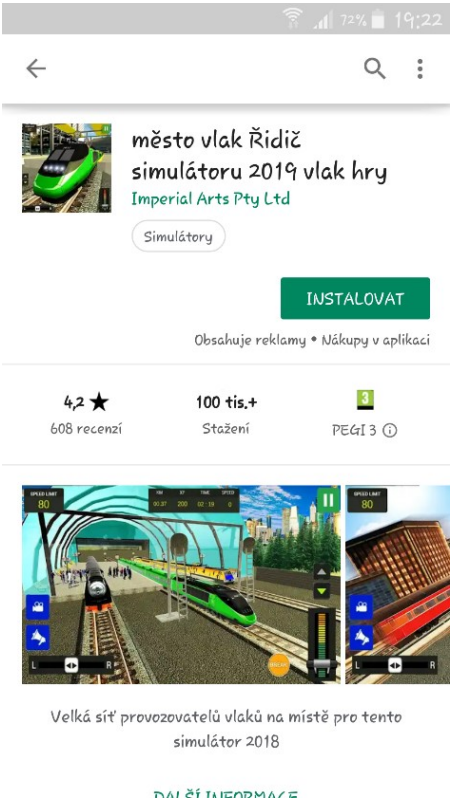
Na tomto obrázku jde vidět, že vývojář má široké portfolio a vydal už velké množství aplikací. V tomto případě, je tedy možné důvěřovat danému vývojáři a v klidu a bez strachu si stáhnout jeho aplikaci.

Další vodítka najdete v dolní části informací o aplikaci v sekci Vývojář. U těch důvěryhodnějších zpravidla najdete odkaz na webové stránky, kde se mnohdy můžete o aplikaci dozvědět víc podrobností. Něco také může vypovídat e-mailová adresa – pokud má autor schránku na Gmailu, je to opět důvod ke zvýšené pozornosti. Důvěryhodná vývojářská studia se většinou netají ani svou fyzickou adresou, ovšem u jednotlivců to není podmínkou. [21]

Pomoci může i zadání jména vývojáře či studia do Googlu. Pokud ho najdete na nějakém vývojářském fóru (např. XDA Developers), je pravděpodobné, že se jedná o někoho, kdo se skutečně zabývá vývojem aplikací, nikoli jen jejich úpravou za účelem integrace nějakého škodlivého kódu. [21]

Rozeznání škodlivé aplikace podle názvu

Poměrně častým společným rysem škodlivých a podvržených aplikací je špatná „lokalizace“ názvu. Zpravidla se jedná o očividné strojové překlady, jako jsou „Slovo Křížovka Připojit – Bez Kříže Česky“, „město vlak Řidič simulátoru 2019 vlaky hry“ či „Motorka závod 2019 Zdarma“.



Obr. 26 - Podezřelý název aplikace

[vlastní]

Pochopitelně kvůli tomu nemusí hned být daná aplikace škodlivá a nemusí to znamenat, že každý automaticky přeložený název je snahou vývojáře infikovat vaše mobilní zařízení škodlivou aplikaci. Solidní autoři však zpravidla hledají lokální dobrovolníky, kteří jim aplikaci včetně popisku přeloží tak, aby se za ni nemuseli stydět. [21]

Rozeznání podle zásad ochrany soukromí

Všechny aplikace musejí mít dle pravidel Obchodu Play uvedené zásady ochrany soukromí. Najdete je jako odkaz v dolní části výpisu v sekci Vývojář. Stačí se podívat, kam odkaz směřuje, a zda podmínky působí důvěryhodným dojmem. Vývojář by zde měl uvést to, jaká data sbírá a jak je zpracovává – pokud vám není lhostejné vaše soukromí, doporučuje se těmto informacím věnovat pozornost. [21]

Sledování požadavků na oprávnění

Stejně tak by se ještě před instalací měli uživatelé podívat na to, k čemu chce aplikace přístup. To se dá zjistit po klepnutí na odkaz Zobrazit podrobnosti v sekci Oprávnění. Většinou stačí použít selský rozum a zamyslet se: potřebuje aplikace, která funguje jako svítilna, přístup k poloze? Takřka jistě nikoli – a to je důvod, proč ji neinstalovat. Vývojáři často vysvětlují, k čemu jaké oprávnění potřebují, ale nebývá to pravidlem. [21]

ZÁVĚR

Citlivá data jako například hesla k různým účtům, telefonní čísla či osobní informace jsou v dnešním světě jednoznačné jednou z nejdůležitějších věcí, co si musí člověk chránit pro svoje bezpečí a jelikož si většina lidí tyto data ukládá na svůj mobilní telefon, je důležité, aby si je také co nejlepším způsobem dokázali ochránit. Jelikož jsou mobilní zařízení tolik využívané a obsahují o každém uživateli obrovské množství informací, je potřeba si tyto údaje chránit. V důsledku jejich odcizení by mohlo dojít k velkým újmám, a to jak po fyzické stránce, tak po psychické. Mezi citlivá data mohou patřit kódy k bankovním účtům, telefonní čísla, či osobní údaje a informace patřící majiteli mobilního zařízení. O takové data by nikdo nechtěl přijít, a proto je potřeba, aby si každý majitel byl vědom ohrožení, které ho může postihnout.

Tato práce se věnuje bezpečnosti osobních dat v mobilních zařízeních, které jsou součástí života mnoha lidí. Definuje hlavní aktiva, které je potřeba v mobilních zařízeních chránit. Dále uvádí, jaké hrozby mohou tyto aktiva ohrozit, a hlavně je popsáno jakým způsobem mohou tyto útoky být provedeny. Nejdůležitější částí práce je analýza bezpečnosti mobilních zařízení se systémem Android, a to za pomoci multikriteriálního hodnocení, SWOT analýzy a dotazníkového šetření. Na konec je také doporučeno, jak co nejlépe svoje mobilní zařízení zabezpečit, a jak zlepšit bezpečnost těchto mobilních zařízení.

Hlavním cílem práce bylo analyzovat a zhodnotit bezpečnost mobilních zařízení operačním systémem Android a navrhnout opatření pro zlepšení bezpečnosti. Cíl bakalářské práce byl splněn.

SEZNAM POUŽITÉ LITERATURY

[1] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[3] BUREŠ, Miroslav, Miroslav RENDA, Michal DOLEŽEL, Peter SVOBODA, Zdeněk GRÖSSL, Martin KOMÁREK, Ondřej MACEK a Radoslav MLYNÁŘ. Efektivní testování softwaru: klíčové otázky pro efektivitu testovacího procesu. Praha: Grada, 2016. Profesionál. ISBN 978-80-247-5594-6.

[4] Bezpečnost. *Ministerstvo vnitra* [online]. Praha [cit. 2019-03-02]. Dostupné z: https://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

[5] Operační systém. *Technická univerzita v Liberci* [online]. Liberec [cit. 2019-03-02]. Dostupné z: http://www.nti.tul.cz/~kolar/os/os.pdf

[6] Kyberprostor. *Techopedia* [online]. Kanada [cit. 2019-03-02]. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace

[7] Osobní údaj. *GDPR* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/osobni-udaje/

[8] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). *NÚKIB* [online]. Brno [cit. 2019-03-02]. Dostupné z: https://nukib.cz/cs/o-nukib/

[9] Znak Androidu. *ITnetwork* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.itnetwork.cz/images/17568/android.png

[10] Podíl OS ve světě. *IDC* [online]. Framingham [cit. 2019-05-04]. Dostupné z: https://www.idc.com/promo/smartphone-market-share/os

[11] Celosvětové porovnání obsazení verzí jednotlivých systému v mobilních zařízení. *Statista* [online]. New York [cit. 2019-03-02]. Dostupné z: http://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide/#daily-20190420-20190420-bar

[12] Google Play Protect. *Google* [online]. Mountain View [cit. 2019-05-04]. Dostupné z: https://support.google.com/googleplay/answer/2812853?hl=cs

[13] Pharming. *Kaspersky* [online]. Moscow [cit. 2019-03-03]. Dostupné z: https://www.kaspersky.com/cz/internet-security-center/definitions/pharming

[14] MALINKA Kamil a PECHO Peter. Evoluční teorie v podání spear phishingu. *CONNECT!*. Brno: Computer Press, s.r.o, 2008, roč. 2008, č. 6, s. 22-23. ISSN 1211-3085

[15] Phishing a Spear-phishing. *Globaldots* [online]. Berlín [cit. 2019-03-03]. Dostupné z: https://www.globaldots.com/wordpress/wp-content/uploads/2017/11/Phishing-and-Spear-Phishing.png

[16] Riziko veřejné Wi-Fi. *Svět Androida* [online]. Praha [cit. 2019-04-01]. Dostupné z: https://www.svetandroida.cz/verejna-wi-fi-vpn/

[17] Veřejné Wi-Fi sítě. *Újezd.net* [online]. Praha [cit. 2019-04-01]. Dostupné z: https://www.ujezd.net/bezpecnost-verejne-wifi

[18] Odemykání pomocí gesta. *Dvojklik* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.dvojklik.cz/odemykani-android-telefonu-pomoci-gesta-neni-tak-bez-pecne-jako-pin-kod

[19] Pravidlo 3-2-1. *Datahelp* [online]. Praha [cit. 2019-04-24]. Dostupné z: https://www.datahelp.cz/clanky/znate-zalohovaci-pravidlo-3---2-1

[20] Informace o aplikaci. *Svět Androida* [online]. Praha [cit. 2019-04-24]. Dostupné z: https://www.svetandroida.cz/media/2019/04/aplikace-ma-pres-5000-instalaci-a-znamku-50-ale-zadne-komentare.jpg

[21]Jak poznat potenciálně škodlivou aplikaci. *Svět Androida* [online]. Praha [cit. 2019-04-24]. Dostupné z: https://www.svetandroida.cz/jak-poznat-skodlivou-aplikaci-android/?utm_source=FB&utm_medium=SvetAndroida.cz&utm_campaign=SNAP%2Bfrom%2BSv%C4%9Bt+Android&fbclid=IwAR2H_R1x0BGo5l8sCcUs9NwEiwOqqtwxM8WGYRvhl0scnkBI32ZdesTHq_s

[22] VPN. *ROOT* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

[23] Poloha uživatele. *Lidovky* [online]. Praha [cit. 2019-04-26]. Dostupné z: https://www.lidovky.cz/relax/zajimavosti/google-uklada-udaje-o-poloze-uzivatelu-i-proti-jejich-vuli.A180814_122341_ln-zajimavosti_ape

[24] Odemčení tváří. *MobileNet* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://mobilenet.cz/clanky/odemknuti-tvari-v-androidu-40-oblafne-fotografie-obliceje-video-7994

[25] Odemykací gesta. *Svět Androida* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.svetandroida.cz/odemykaci-gesta-pruzkum/

[26] Nastavení hesla. *Google* [online]. Mountain View [cit. 2019-05-04]. Dostupné z: https://support.google.com/android/answer/9079129

[27] Viditelné stopy na obrazovce. Newlaunches [online]. New York [cit. 2019-05-04]. Dostupné z: http://www.newlaunches.com/wp-content/uploads/2013/01/Lock-screen-protection-thumb-450x493.jpg

[28] Automatické vypínání Wi-Fi. *Svět androida* [online]. Praha [cit. 2019-04-26]. Dostupné z: https://www.svetandroida.cz/jak-automaticky-vypnout-wi-fi/

[29] Antiviry a viry. *Root* [online]. Praha [cit. 2019-04-26]. Dostupné z: https://www.root.cz/antiviry-viry/

[30] Aktualizace OS. *Android Tip* [online]. Praha [cit. 2019-05-01]. Dostupné z: http://www.androidtip.cz/ptate-se-jak-aktualizovat-android-na-tabletu-telefonu-jednoduchy-navod/

[31] KeePass. *KeePass* [online]. Metzingen [cit. 2019-05-03]. Dostupné z: https://keepass.info

[32] Citlivé osobní údaje. *GDPR* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

[33] GDPR. *Úřad pro ochranu osobních údajů* [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.uoou.cz/gdpr/ds-3938/p1=3938

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GDPR Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)

IDC International Data Corporation

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

OS Operační systém

VPN Virtuální privátní síť (Virtual private network)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Analýza bezpečnosti mobilních zařízení se systémem Android

Dobrý den,

jmenuji se Jakub Němec a studuji na Fakultě logistiky a krizového řízení v Uherském Hradišti a studuji obor Ochrana obyvatelstva. Píši kvalifikační práci na téma Analýza bezpečnosti mobilních zařízení se systémem Android.

Jste-li uživatelem jakéhokoliv mobilního zařízením se systémem Android, věnujte prosím několik minut svého času, pro vyplnění následujícího dotazníku, který se zaměřuje na analýzu bezpečnosti mobilních zařízení se systémem Android a na bezpečnosti osobních informací, uložených v těchto zařízení.

Výsledky tohoto dotazníku mi pomohou k zjištění, jaký vztah mají uživatelé mobilních zařízení se systémem Android k bezpečnosti jejich osobních informací v jejích zařízeních, a zda pociťují nějaké riziko při používání mobilních zařízení.

Děkuji Vám,

Jakub Němec

1. Jaký typ mobílního zařízení se systémem Android používáte?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Mobilní telefon
- ☐ Tablet
- ☐ Chytré hodinky
- ☐ Jiné...

2. Připojujete svoje mobilní zařízení k internetu?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano
- ○ Ne

Obr. 27 – První strana dotazníku [Survio]

3. Využíváte vaše mobilní zařízení k osobnímů, nebo pracovnímu použití?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

☐ Osobní

☐ Pracovní

4. Přihlašujete se ve svém mobilním zařízení k účtům od internetového bankovnictví, Facebooku, emailu či jiným?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano

◯ Ne

5. Přihlašujete se ve svém mobilním zařízení k účtům od internetového bankovnictví, Facebooku, emailu či dalším na veřejné síti WiFi (v restauraci, kavárně, obchodu...)?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano

◯ Ne

6. Máte váše mobilní zařízení nějakým způsobem zabezpečeno před vniknutím cízí osoby (například zámek obrazovky)?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano

◯ Ne

7. Máte pocit, že jsou vaše osobní informace a data (kontakty, hesla, soukromé zprávy, informace o vaší aktivitě...) ve vašem mobilním zařízení v bezpečí?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano

◯ Ne

Obr. 28 – Druhá strana dotazníku [Survio]

8. Myslíte si, že mohou být vaše osobní data a informace, umístěné ve vašem mobilním zařízení, kdykoliv zneužita?

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ Ano
- ◯ Ne

9. Máte pocit nebo jistotu, že již někdy byly vaše osobní informace a data v mobilním zařízení zneužita?

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ Jsem si jistý(á), že ANO
- ◯ Mám pocit, že ANO
- ◯ Jsem si jistý(á), že NE
- ◯ Mám pocit, že NE

10. Jak byste ohodnotili bezpečnost vašich osobních dat a informací ve vašem zařízení?

Nápověda k otázce: *Jedna hvězda - mé informace jsou v nebezpečí. Pět hvězd - mé informace jsou naprosto v bezpečí.*

☆☆☆☆☆ ☐ / 5

Obr. 29 - Třetí strana dotazníku [Survio]

PŘÍLOHA P II: VÝSLEDKY DOTAZNÍKU

Tab. 10 - Podrobnosti k odpovědím na otázku č. 1 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Mobilní telefon	98	99,0 %
Tablet	18	18,2 %
Chytré hodinky	7	7,1 %
Jiné…	1	1,0 %
Jiné…: Chytrý náramek		

Tab. 11 - Podrobnosti k odpovědím na otázku č. 2 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Ano	99	100 %
Ne	0	0 %

Tab. 12 - Podrobnosti k odpovědím na otázku č. 3 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Osobní	98	99 %
Pracovní	26	26,3 %

Tab. 13 - Podrobnosti k odpovědím na otázku č. 4 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Ano	98	99 %
Ne	1	1 %

Tab. 14 - Podrobnosti k odpovědím na otázku č. 5 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Ano	85	85,9 %
Ne	14	14,1 %

Tab. 15 - Podrobnosti k odpovědím na otázku č. 6 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Ano	72	72,7 %
Ne	27	27,3 %

Tab. 16 - Podrobnosti k odpovědím na otázku č. 7 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Ano	49	49,5 %
Ne	50	50,5 %

Tab. 17 - Podrobnosti k odpovědím na otázku č. 8 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Ano	75	75,8 %
Ne	24	24,2 %

Tab. 18 - Podrobnosti k odpovědím na otázku č. 9 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
Jsem si jistý(á), že NE	11	11,1 %
Mám pocit, že NE	60	60,6 %
Mám pocit, že ANO	24	24,2 %
Jsem si jistý(á), že ANO	4	4,0 %

Tab. 19 - Podrobnosti k odpovědím na otázku č. 10 [vlastní]

Možnost odpovědí	*Responzí*	*Podíl*
1/5	10	10,1 %
2/5	16	16,2 %
3/5	37	37,4 %
4/5	31	31,3 %
5/5	5	5,1 %