Služby pro okamžité zasílání zpráv v kontextu datové bezpečnosti

Bc. Jana Líčeníková

Diplomová práce
2024

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: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jana Líčeníková**
Osobní číslo:	**L22372**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Služby pro okamžité zasílání zpráv v kontextu datové bezpečnosti**

Zásady pro vypracování

1. Zpracujte literární rešerši z domácích i zahraničních zdrojů.
2. Zhodnoťte historický i současný stav služeb pro okamžité zasílání zpráv.
3. Analyzujte rizika spojená s datovou bezpečností.
4. Navrhněte případná doporučení, opatření ke zlepšení stávajícího stavu.

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

Seznam doporučené literatury:

1. ALI, Al-Rahim a Saad Najim ALSAAD. Instant messaging security and privacy secure instant messenger design. *IOP Conference Series: Materials Science and Engineering* [PDF]. 2020, 881(1) [cit. 2023-10-22]. ISSN 1757-8981. Dostupné z: doi: 10.1088/1757-899X/881/1/012117.
2. KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. *CyberSecurity.* Praha: CZ.NIC, 2019. ISBN 978-80--88168-31-7.
3. OPPLIGER, Rolf. *Secure Messaging on the Internet.* Boston: Artech House, 2014. ISBN 978-1-60807-717-5.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Pavel Tomášek, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2023**
Termín odevzdání diplomové práce: **26. dubna 2024**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou 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 Univerzita Tomáše Bati 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 – diplomovou 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 diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 26. 4. 2024

Jméno a příjmení studenta: Bc. Jana Líčeníková

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá problematikou služeb pro okamžité zasílání zpráv v kontextu datové bezpečnosti. V teoretické části práce je provedena rešerše a jsou uvedena základní teoretická východiska dané problematiky. Praktická část se věnuje identifikaci a analýze hrozeb a rizik spojených s datovou bezpečností. V závěru práce jsou na základě zjištěných informací vyhodnoceny aplikace, které vynikají nad ostatními z hlediska bezpečnosti a jsou navržena příslušná doporučení a opatření pro uživatele a pro zlepšení stávajícího stavu.

Klíčová slova: datová bezpečnost, koncové šifrování, kybernetická bezpečnost, služby pro okamžité zasílání zpráv

ABSTRACT

The diploma thesis deals with the issue of instant messaging services in the context of data security. In the theoretical part of the thesis, research is carried out and the basic theoretical starting points of the given issue are presented. The practical part is devoted to the identification and analysis of threats and risks associated with data security. At the end of the work, based on the information found, the applications that stand out from the others in terms of security are evaluated and relevant recommendations and measures are proposed for the users and for improving the current situation.

Keywords: cyber security, data security, end-to-end encrypting, instant messaging

Ráda bych poděkovala panu Ing. Pavlu Tomáškovi, Ph.D. za poskytnutí odborného vedení a cenných rad k obsahu této diplomové práce. Dále bych také chtěla poděkovat mé rodině a kamarádům za podporu po celou dobu studia.

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

OBSAH

ÚVOD

V současné době se svět neustále mění a jedním z nejvýraznějších motorů těchto změn je bezpochyby internet. Tato globální síť, která k nám přišla v posledních dekádách 20. století, způsobila revoluci v mnoha aspektech našich životů. S příchodem internetu se dramaticky změnil způsob, jakým vyhledáváme informace, jak se učíme nové věci a jak si organizujeme svůj osobní i profesní život. A jak se internet vyvíjí, roste s ním i naše závislost na široké škále digitálních služeb, které nám tento nástroj nabízí.

Jedním ze základních pilířů digitálního věku jsou komunikační platformy. Díky nim můžeme v reálném čase komunikovat s lidmi z celého světa, ať už jde o osobní zprávy, videohovory nebo sdílení obsahu. Tyto platformy, jako jsou sociální sítě, emaily nebo aplikace pro instant messaging se staly neodmyslitelnou součástí našich profesních i osobních životů. Umožňují nám sdílet informace rychle a efektivně, což v mnoha případech znamená značnou úsporu času a energie.

Nicméně, jak se naše závislost na těchto digitálních službách zvyšuje, objevují se i nové výzvy a rizika. Jednou z největších obav je otázka bezpečnosti. Každý den jsme svědky zpráv o hackerských útocích, únicích dat a dalších bezpečnostních incidentech, které mohou mít devastující dopady na jednotlivce i firmy. To je důvod, proč je nesmírně důležité, aby byla digitální bezpečnost brána vážně jak na individuální, tak na korporátní úrovni.

V této digitální éře, kde se zprávy a informace šíří rychlostí světla, je třeba klást velký důraz na ochranu našich osobních údajů a soukromí. Existují různé metody a nástroje, jak chránit naše digitální identity, jako jsou silná hesla, dvoufázové ověření, šifrování dat a pravidelné aktualizace softwaru. Tyto postupy by měly být běžnou součástí našeho digitálního života, pokud chceme minimalizovat rizika spojená s online aktivitami.

Tato diplomová práce se zaměřuje na problematikou datové bezpečnosti v kontextu komunikačních aplikací pro okamžité odesílání zpráv. Poskytuje pohled na různé aspekty zabezpečení těchto aplikací, analyzuje rizika a hrozby spojená s jejich používáním a navrhuje doporučení k ochraně uživatelských dat a soukromí.

Práce se soustředí na rozbor osmi chatovacích aplikací, konkrétně na WhatsApp, WeChat, Facebook Messenger, Telegram, Skype Signal, Instagram a Jami, a zkoumá jejich bezpečnostní opatření, způsoby šifrování dat a postupy pro ochranu uživatelských informací.

V závěru práce jsou shrnuty klíčové závěry a doporučení pro bezpečné používání komunikačních nástrojů a jsou vyhodnoceny aplikace, které z hlediska bezpečnosti nad ostatními vynikají. Diplomová práce přináší přehledné a ucelené informace pro každého, kdo se zajímá o ochranu svých osobních dat a soukromí v digitálním prostředí chatovacích platforem.

CÍL PRÁCE A POUŽITÉ METODY

Cílem diplomové práce je zpracovat analýzu pro problematiku služeb pro okamžité zasílání zpráv s důrazem na identifikaci a hodnocení rizik spojených s používám těchto komunikačních platforem. Na základě získaných dat navrhnout a doporučit opatření, která povedou ke zvýšení úrovně bezpečnosti na komunikačních platformách.

K dosažení tohoto cíle byly vypracovány dílčí cíle. Byla zpracována literární rešerše a zhodnocen historický a současný stav služeb pro okamžité zasílání zpráv, která slouží jako základ pro zpracování analyticko-empirické a aplikační části práce.

V praktické analyticko-empirické části byla analyzována rizika spojená s datovou bezpečností. To zahrnuje implementaci koncového šifrování v chatovacích aplikacích a dále také hrozby jako je phishing, malware, úniky citlivých informací nebo útoky na soukromí uživatelů. Na základě této analýzy bylo cílem navrhnout případná doporučení a opatření ke zlepšení stávajícího stavu.

Použité výzkumné metody

Pro zpracování této diplomové práce bylo využito několik odborných metod. Jedná se zejména o metodologii sběru informací ze spektra české a zahraniční literatury, včetně knih a odborných článků, s cílem získat komplexní povědomí o problematice služeb pro okamžité zasílání zpráv. Následují také další aplikované vědecké metody:

- Analýza – provádění rozboru a posouzení rizik a hrozeb spojených s datovou bezpečností.
- Deskripce – čili sběr informací a jejich následná aplikace.
- Komparace – zahrnuje porovnání jednotlivých služeb pro okamžité zasílání zpráv.
- Literární rešerše – shromáždění a přehled odborných literárních zdrojů z české a zahraniční literatury, které se týkají dané problematiku.
- Popis – popsání teoretických východisek nezbytných pro vstup a pochopení dané problematiky.
- Syntéza – vyhodnocení a spojení jednotlivých prvků do konečného celku.

I. TEORETICKÁ ČÁST

1 DEFINICE SLUŽEB PRO OKAMŽITÉ ZASÍLÁNÍ ZPRÁV

Rozvoj moderních technologií a digitalizace společnosti přinesly do našeho každodenního života nové formy komunikace, z nichž jednou z nejrozšířenějších jsou služby pro okamžité odesílání zpráv. Tyto platformy umožňují uživatelům rychlý a pohodlný způsob komunikace a možnost okamžitého spojení s přáteli, rodinou i kolegy, což z nich činí důležitý nástroj pro komunikaci a spolupráci.

Rapidní nárůst oblíbenosti komunikačních aplikací však také přinesl nové bezpečnostní hrozby a obavy týkající se ochrany osobních údajů uživatelů. S nárůstem počtu uživatelů a objemu přenášených dat se tyto platformy staly atraktivními cíli pro různé formy kybernetických útoků. (Ali, Alsaad, 2020)

Služby pro okamžité zasílání zpráv (anglicky *Instant Messaging* - IM) jsou populární komunikační platformy, které umožňují dvěma či více uživatelům posílat a přijímat textové zprávy v reálném čase nehledě na to, kde se právě tyto osoby nacházejí nebo jaké zařízení používají. Tyto služby nabízejí rychlou a efektivní komunikaci a jsou široce používány jak v osobní, tak v pracovní sféře. (James, 2023)

Uživatelé mohou sledovat aktuální přítomnost svých přátel v síti. To znamená, že mají možnost vidět, kteří z jejich přátel jsou v daném okamžiku také připojeni a online. Tato funkce umožňuje uživatelům zjistit, kdo je momentálně aktivní na síti a k dispozici pro komunikaci. Tím se poskytuje prostor pro okamžitou interakci mezi dvěma přáteli, či kolegy. (Chábera et al., 2016)

Mezi nejpopulárnější služby pro zasílání zpráv dnes patří například WhatsApp, Facebook Messenger, Instagram, Skype, X (dříve Twitter), Snapchat a další. Jsou mezi sebou různě propojeny a tím umožňují svým uživatelům nahrávat, upravovat a sdílet různá média. Všechny tyto IM mají v současné době více než 100 milionů aktivních uživatelů. (Sayer, 2015)

K jejich výhodám se řadí okamžitost, jelikož zprávy jsou doručovány téměř okamžitě, což usnadňuje rychlou komunikaci na dálku. Dále také umožňují uživatelům sdílení fotografií, hlasových zpráv, videí, emotikonů či jiných souborů. Mohou se v nich vytvářet skupinové chaty, které usnadňují komunikaci ve vícečlenných týmech nebo mezi přáteli. Většina služeb vyžaduje pouze připojení k internetu, což umožňuje snížit náklady na komunikaci, hlavně v mezinárodním měřítku. A jsou také k dispozici na různých platformách jako mobilní telefony, počítače, tablety atd., tudíž poskytují flexibilitu v používání. Navíc povolují

uživatelům vyhledávání v historii zpráv, aktualizaci osobních statusů, vypínání a zapínání upozornění na zprávy neboli notifikací. Dále též blokaci, kterou uživatelé eliminují jakékoli nechtěné či nevyžádaní zprávy. (James, 2023)

Najde se také několik nevýhod, které se pojí s těmito službami. V první řadě je to závislost zařízení na internetu, jelikož pro používání je nezbytné připojení k internetu, a to může být nevýhodné v oblastech s omezeným přístupem k síti. Existují i bezpečnostní rizika spojená se zneužitím účtu. Hackeři se mohou nabourat do účtu uživatele a získat tak nad ním kontrolu. U některých služeb se také mohou vyskytnout bezpečnostní otázky, zejména pokud jde o ochranu soukromí a bezpečnost dat uživatelů. Dále také mohou okamžité notifikace způsobit rušení při obvyklých činnostech nebo narušení soukromí. V některých případech může být zase snadné přehlédnout důležité informace mezi nadměrným množstvím zpráv. A v neposlední řadě také touha být neustále online může vést k nadužívání, což narušuje soukromý život uživatelů a způsobuje jim problémy jak v pracovní tak osobní oblasti. (James, 2023)

Zásadním problémem pro uživatele se také může stát vytvoření si závislosti na chatovacích aplikacích. Uživatelé, kteří často tráví hodiny denně na těchto aplikacích, mohou postupně ztrácet osobní kontakt s rodinou a přáteli a tím i veškeré sociální interakce mimo digitální prostředí. Pokud se uživatelé příliš spoléhají na chatovací aplikace, existuje riziko, že se uzavřou do světa virtuálních vztahů a izolují se od reálného světa kolem nich. Tento vzorec může vést k obtížím při navazování nových vztahů a udržováním stávajících mimo online prostředí.

Komunikační platformy pro okamžité odesílání zpráv tedy poskytují rychlou a pohodlnou cestu k interakci s ostatními, ačkoli s sebou nesou i určitá bezpečnostní a jiná rizika. Jejich využívání je doprovázeno obavami o ztrátu soukromí a bezpečnosti dat. Je důležité, aby uživatelé byli obezřetní a přijímali opatření k minimalizaci těchto rizik.

1.1 Historický vývoj

Počátek prvních předchůdců IM služeb sahá do 19. století. Do té doby byla komunikace mezi lidmi omezena převážně na osobní setkání a příležitosti ke kontaktu s okolním světem byly taktéž omezené. S postupným rozvojem tisku a elektronických médií však začala komunikační krajina měnit svůj charakter. V roce 1844 byla v USA zprovozněna první telegrafická linka spojující Baltimore a Washington. Tento průlom znamenal rychlejší tok

zasílaných a přijímaných zpráv, což mělo vliv na komunikační možnosti a tím umožnilo lidem komunikovat na větší vzdálenosti. (Hanson, 2020)

Další z historicky významných forem okamžité komunikace na dálku představuje e-mail (anglická zkratka pro *Electronic Mail*), který uživatelům umožňuje posílat a přijímat zprávy prostřednictvím elektronických zařízení připojených k internetu. Tato forma komunikace nahrazuje tradiční fyzickou poštu a poskytuje rychlé a efektivní přenosy textových zpráv, dokumentů, fotografii, obrázků a dalších multimediálních obsahů. Princip e-mailu spočívá ve vytváření elektronických zpráv, které jsou odesílány z jednoho elektronického zařízení na druhé prostřednictvím e-mailových adres. Tyto adresy fungují jako jedinečné identifikátory, které umožňují přesné směrování zpráv k určenému příjemci. (Oppliger, 2014)

Historie e-mailu sahá do 60. let 20. století, kdy americké ministerstvo obrany vyvinulo síť nazvanou ARPANET, která propojovala výzkumníky. E-mail byl vytvořen jako komunikační prostředek na Arpanetu v roce 1971 počítačovým inženýrem Rayem Tomlinsonem za využití symbolu „@“, aby oddělil uživatelské jméno od názvu počítače a nejdříve měl sloužit pro vojenské a vládní účely. Zanedlouho se začal využívat k propojení vědeckých a akademických institucí. V 80. letech 20. století byly vytvořeny první komerční e-mailové služby, čímž se e-mail stal přístupným pro širší veřejnost a s rozvojem osobních počítačů a nástupem internetu do domácností se e-mail stal běžnou součástí každodenního života. Ve Spojených státech Amerických se poprvé v roce 1996 poslalo více e-mailů než fyzických dopisů. (The First E-mail Message of Ray Tomlinson, 2023)

Tato forma komunikace sice zefektivnila textové přenosy, ale stále se nejednalo o formu komunikace v reálném čase. To se změnilo na počátku 90. let 20. století, kdy izraelská společnost Mirabilis spustila ICQ (*I Seek You*), tedy vůbec první software pro okamžité zasílání zpráv. ICQ přineslo revoluční možnost uživatelům, a to komunikovat v reálném čase pomocí posílání textových zpráv. Každý uživatel ICQ disponoval jedinečným identifikačním číslem, které mu umožňovalo přihlásit se do sítě. Uživatel viděl seznam ostatních uživatelů, kteří byli právě připojení a také mohl posílat zprávy i v době, kdy byl offline, tedy v době, kdy nebyl připojen k internetu. ICQ si velmi rychle získalo popularitu v USA a určitou dobu mělo významnou roli v oblasti IM. Postupem času a s nástupem dalších komunikačních platforem však jeho popularita klesla. I přesto je ICQ považováno za průkopníka v oblasti okamžité komunikace na internetu. (James, 2023)

1.2 Současnost

V průběhu posledních dvou dekád došlo k výraznému posunu v oblasti komunikace prostřednictvím instant messaging. Na počátku nového tisíciletí dominovala na poli IM aplikace ICQ, která se stala ikonickou platformou pro okamžitou komunikaci. Nicméně v rychlým rozvojem technologií v oblasti mobilních zařízení a internetu začaly na trh vstupovat další a další populární aplikace pro okamžité zprávy jako je Facebook a později Facebook Messenger, Skype, WhatsApp, Instagram, Telegram a mnoho dalších a tím vznikla nová generace sociálních médií.

Tento vývoj reflektuje nejen dynamiku digitálního prostředí, ale také změnu preferencí uživatelů a potřeb ve společnosti. Uživatelé dnes očekávají komunikační platformy, které nejen umožňují rychlou výměnu zpráv, ale také nabízejí široké spektrum funkcí, jako jsou videohovory, sdílení multimediálního obsahu a skupinové konverzace.

Příkladem toho je Instagram, který původně sloužil primárně ke sdílení fotografií, ale s postupem času integroval prvky okamžité komunikace a dnes funguje jako komplexní platforma pro komunikaci mezi uživateli.

Tento trend ukazuje na neustálý rozvoj komunikačních nástrojů, které ovlivňují způsob, jakým lidé interagují ve svém každodenním životě. S nástupem nových technologií a aplikací se očekává další inovace a změny, které budou přizpůsobeny potřebám moderní společnosti.

1.3 Alternativy k chatovacím aplikacím

Je důležité zmínit, že existuje několik alternativ k instant messagingu, které nabízejí různé přístupy ke komunikaci a interakci.

V první řadě jde o e-mailové služby, kdy e-mail je klasickou formou elektronické komunikace, která umožňuje uživatelům posílat zprávy a soubory v textovém formátu. Na rozdíl od komunikačních platforem jsou e-emaily asynchronní, což znamená, že účastníci nemusí být online ve stejnou dobu, aby komunikovali.

Další možností jsou telefonní hovory, které jsou tradičním způsobem komunikace a umožňují uživatelům mluvit s ostatními v reálném čase. Lze také komunikovat skrze sociální média, kde uživatelé mohou sdílet fotografie, videa, statusy a další obsah. Sociální sítě také mohou sloužit jako prostředek komunikace s přáteli, rodinou i veřejností. Dále lze též využívat diskusní fóra, která umožňují uživatelům diskutovat o různých tématech a sdílet

své názory a zkušenosti. Tato forma komunikace je obvykle asynchronní, stejně jako e-mail, a umožňuje uživatelům vyjadřovat své myšlenky podrobněji.

Nelze opomenout SMS (*Short Message Service*), což je jedna z nejstarších forem textové komunikace pomocí mobilních telefonů. Tato služba umožňuje uživatelům posílat krátké textové zprávy mezi mobilními telefony, aniž by bylo nutné používat internetové připojení. SMS zprávy jsou omezené na určitý počet znaků (obvykle 160), což je důvod, proč jsou vhodné pro krátké a rychlé zprávy. Přestože SMS nenabízí takové funkce jako instant messaging aplikace jako jsou skupinové chaty a sdílení souborů, stále je považována za spolehlivý a široce používaný způsob komunikace, zejména tam, kde není k dispozici internetové připojení nebo kde uživatelé preferují jednoduchost a přímou komunikaci. SMS je stále běžně používána pro různé účely, jako jsou osobní zprávy, upozornění od služeb a firem, bankovní transakce nebo ověřovací kódy pro dvoufaktorové ověření.

2 PŘEHLED POPULÁRNÍCH SLUŽEB DANÉ KATEGORIE

V digitalizované době sehrává okamžitá komunikace zásadní úlohu při propojování lidí po celém světě. S rozvojem internetu a mobilních technologií se objevilo mnoho aplikací, které umožňují rychlou a efektivní komunikaci mezi jednotlivci i skupinami. Služby pro okamžité zasílání zpráv se staly nepostradatelným prvkem každodenního života, umožňující rychlou a efektivní výměnu informací. Tyto služby nabízejí široké spektrum funkcí, včetně textových zpráv, hlasových zpráv a videohovorů a sdílení médií.

Tyto aplikace přinášejí jedinečné funkce, které vyhovují různým potřebám uživatelů po celém světě, ať už jde o osobní neformální chaty nebo důležité pracovní konference. Výběr správné aplikace závisí na specifických požadavcích a preferencích jednotlivce, ale jedno je jisté – v dnešní digitalizované době jsou možnosti téměř neomezené. Zde je uveden přehled chatovacích aplikací, skrze které je možné v dnešní době komunikovat.

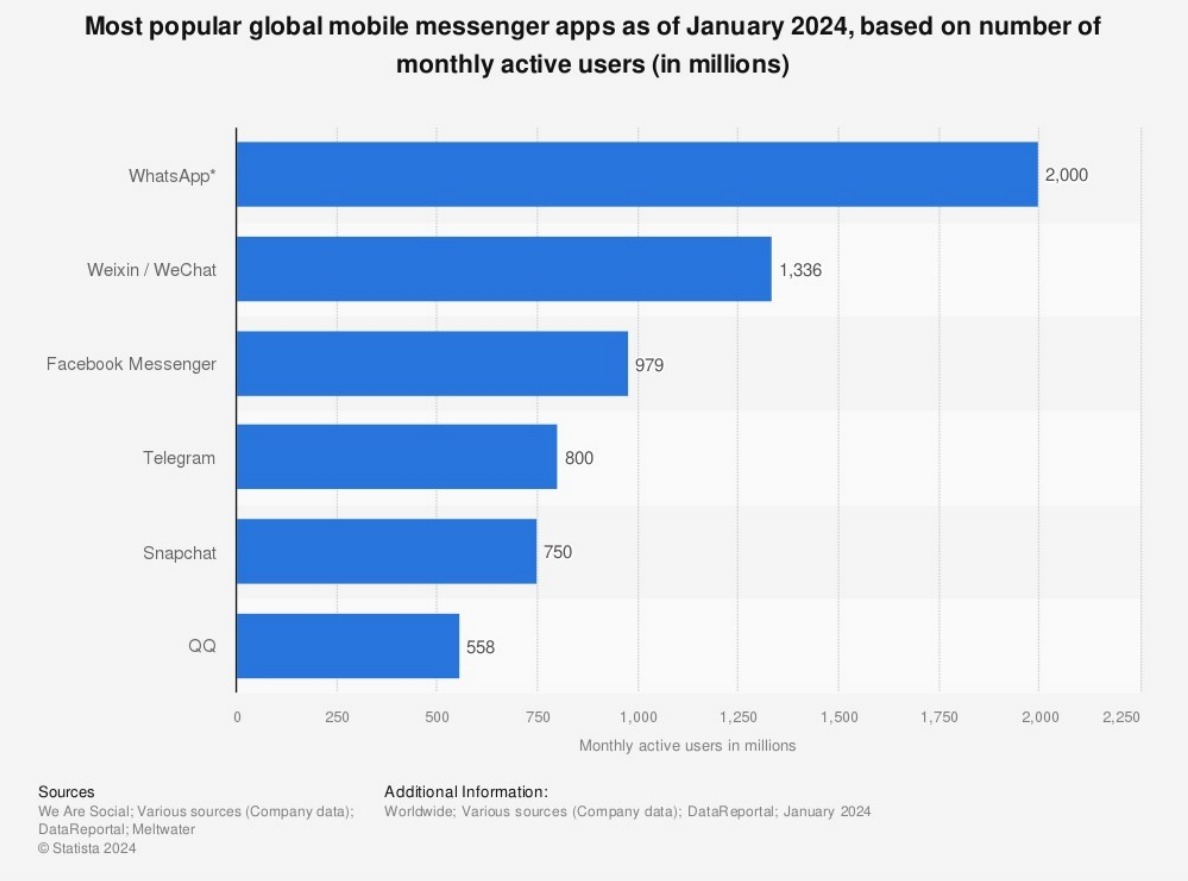
- **Adium** – Aplikace k zasílání zpráv pro operační systém macOS.
- **Apple iMessage** – Služba pro okamžitou komunikaci, která je k dispozici pro uživatele zařízení Apple, jako jsou iPhone, iPad a Mac. Umožňuje posílat textové zprávy, obrázky, videa a audiozáznamy, a to jak mezi zařízeními Apple, tak i na mobilní čísla prostřednictvím SMS.
- **Discord** – Aplikace primárně určená pro hlasovou komunikaci během online her, Discord také poskytuje textové chaty a možnost sdílet média. Je populární mezi hráči i komunitami s různými zájmy.
- **Dust** – Umožňuje posílat textové zprávy, fotky a videa s funkcemi, které poskytují automatické mazání zpráv po určité době.
- **Element Messenger** – Umožňuje uživatelům vytvářet vlastní chatovací servery a komunikovat pomocí textových zpráv, hlasových a videohovorů a sdílení souborů.
- **Facebook Messenger** – Skrze něj mohou uživatelé posílat zprávy a volat přátelům ze sociální sítě Facebook. Nabízí také rozšířené funkce, jako jsou skupinové videohovory a možnost sdílet různá média.
- **Google Messages** – Aplikace pro SMS a MMS zprávy vyvinutá společností Google pro operační systém Android. Kromě běžných textových zpráv umožňuje posílat obrázky, videa, GIFy a vytvářet skupinové konverzace.

- **Hangouts** – Umožňuje posílat textové zprávy, provádět hlasové a videohovory a sdílet média.
- **Instagram** – Umožňuje uživatelům posílat textové zprávy a sdílet média s ostatními uživateli.
- **Jami** – Poskytuje textové zprávy, hlasové a videohovory a sdílení souborů, a to bez centrálního serveru.
- **Kakao Talk** – Uživatelé mohou skrze něj posílat textové zprávy, hlasové zprávy, obrázky, videa, GIFy, sdílet polohu a vytvářet skupinové konverzace a videohovory.
- **Kik Messenger** – Umožňuje posílat textové zprávy, sdílet média a připojovat se k různým chatovacím skupinám.
- **LINE** – Aplikace populární v Asii, která nabízí širokou škálu funkcí včetně posílání zpráv, hlasových a videohovorů, sdílení médií a provádění plateb.
- **Microsoft Teams** – Aplikace určená pro pracovní komunikaci a spolupráci, která kombinuje textové chaty, videohovory, sdílení souborů a integrované nástroje pro projektový management.
- **Reddit** – Známý spíše jako platforma pro diskusi a sdílení obsahu, Reddit také umožňuje uživatelům komunikovat pomocí textových zpráv v rámci různých komunit.
- **Session** – Umožňuje posílat textové zprávy, hlasové a videohovory.
- **Signal** – Platforma, která nabízí textové zprávy, hlasové a videohovory.
- **SimpleX** – Umožňuje posílat textové zprávy, soubory a vytvářet skupinové konverzace.
- **Siskin** – Aplikace, která umožňuje posílat textové zprávy, soubory, hlasové a videohovory.
- **Skype** – Umožňuje posílat textové zprávy, provádět hlasové a videohovory, sdílet soubory a obrazovky a vytvářet skupinové chaty. Skype je rozšířen mezi uživateli, kteří potřebují komunikovat i v pracovním prostředí.
- **Slack** – Zaměřen na pracovní komunikaci a spolupráci v týmech, Slack poskytuje textové chaty, sdílení souborů a integrované nástroje pro správu projektů.

- **Snapchat** – Aplikace zaměřená zejména na sdílení fotografií a videí s možností přidání různých filtrů a efektů. Nabízí také chatování a možnost vytvářet příběhy pro sdílení s ostatními uživateli.
- **Telegram** – Nabízí šifrované textové zprávy, hlasové a videohovory, sdílení souborů a vytváření skupinových chatů.
- **Threeema** – Nabízí možnost posílat textové zprávy, volat a sdílet soubory.
- **Viber** – Aplikace, která umožňuje posílat textové zprávy, provádět hlasové a videohovory a sdílet média. Nabízí také možnost vytvářet skupinové chaty a volat na telefony mimo aplikaci za výhodných podmínek.
- **WhatsApp** – Umožňuje posílat textové zprávy, hlasové a videohovory, sdílet soubory a média a vytvářet skupinové chaty. Je k dispozici na různých platformách.
- **WeChat / Weixin** – Populární IM aplikace v Číně, která kombinuje funkce sociální sítě, platební brány a komunikační platformy. Umožňuje posílat zprávy, volat, sdílet média a provádět platby.
- **Wickr Me** – Umožňuje posílat šifrované textové zprávy, obrázky, videa a soubory.
- **Wire** – Nabízí textové zprávy, hlasové a videohovory a sdílení souborů.
- **X, dříve Twitter** – Sociální síť, která umožňuje uživatelům posílat krátké textové zprávy nazývané "tweety". Tyto zprávy mohou být veřejné nebo sdíleny pouze mezi vybranými uživateli. X slouží k okamžité komunikaci, sdílení informací a interakci s ostatními uživateli.
- **ZOOM** – Primárně známý jako platforma pro videohovory, ZOOM také nabízí možnost posílat textové zprávy a sdílet soubory. Je často využíván pro online setkání a vzdělávání.

Každá z výše uvedených aplikací disponuje specifickými funkcemi a vlastnostmi, které oslovují různé skupiny uživatelů. Přinášejí různé přístupy k tomu, jak mohou lidé komunikovat a sdílet informace v digitálním světe a to od jednoduchého posílání zpráv po komplexní týmovou spolupráci. Přestože se jejich funkcionality mohou lišit, všechny však sdílejí základní cíl, a to je usnadnění komunikace mezi lidmi bez ohledu na jejich geografickou polohu.

Na Obrázku 1 je zobrazen přehled, který znázorňuje, které mobilní aplikace pro okamžité zasílání zpráv jsou na celosvětové úrovni nejpopulárnější podle aktivních uživatelů. Tento graf odráží situaci za měsíc leden 2024. Co do počtu uživatelů těmto platformám vévodí aplikace WhatsApp se dvěma miliardami aktivních uživatelů. Na druhé příčce je WeChat s více než 1,3 miliardami uživatelů. Třetí příčku uzavírá Facebook Messenger s 980 miliony uživatelů.



Obrázek 1: Nejpopulárnější mobilní služby pro okamžité zasílání zpráv podle aktivních uživatelů za měsíc leden 2024 (Statista, 2024)

Uvedená statistika pochází z databáze Statista a nabízí aktuální statistické údaje a srovnání v širokém spektru témat. Vzniká z kombinace různých veřejně dostupných i vlastních zdrojů dat, včetně průzkumů, výzkumných studií, veřejných zpráv a analýz provedených týmy expertů. Tyto informace jsou pak zpracovány a prezentovány ve formě grafů, tabulek a reportů, které poskytují uživatelům přehledné a aktuální informace o různých tématech a trzích. Zhruba 25% celkových dat v databázi Statista pochází z volně dostupných zdrojů online, jako je Světová banka a Americký úřad pro sčítání lidu, který slouží jako hlavní zdroj

kvalitních dat o občanech a ekonomice země. Data jsou kombinována tak, aby zahrnula obsáhlou škálu témat. (Statista, 2024)

Je důležité zdůraznit, že uvedenou statistiku do jisté míry ovlivňuje fakt, že v Číně nejsou dostupné populární komunikační platformy jako je WhatsApp, Facebook Messenger, Telegram, Signal a Instagram. Čína jakožto komunistická země omezuje svobodu projevu svých občanů a internetovou cenzurou redukuje tok a šíření jakýchkoli informací, které jsou v rozporu s jejími vlastními názory a ideologií. Avšak má k tomu i ekonomické důvody, protože cenzurou zahraničních aplikací Čína propaguje domácí internetové a technologické společnosti. Z toho důvodu se tak obyvatelé Číny spoléhají na domácí služby, které jsou podrobeny přísné kontrole a regulaci ze strany čínských úřadů jako je chatovací aplikace WeChat, která se nachází na druhé příčce nejpopulárnějších mobilních služeb pro okamžité odesílání zpráv podle aktivních uživatelů. (Binns, 2023)

Následující přehled se zaměřuje na osm chatovacích aplikací. Čtyři z nich jsou mezi nejpopulárnějšími aplikacemi podle počtu uživatelů, tudíž ovládají digitální komunikační prostředí a proto byly zahrnuty do této práce a jde o WhatsApp, WeChat, Facebook Messenger a Telegram. K nim byl přidán Instagram, který patří do portfolia společnosti Meta (stejně jako WhatsApp a Facebook Messenger). Dále je zahnut Skype, který je populární mezi uživateli komunikující v pracovním prostředí a i dvě méně známe služby Signal a Jami, které však vynikají svým zabezpečením a ochranou soukromí uživatelů. Všechny uvedené aplikace jsou zároveň pro uživatele dostupné zdarma. Tyto aplikace byly také vybrány z důvodu, že nabízejí možnost koncového šifrování, ať už v základním nastavení nebo je zde alespoň možnost ho zapnout. Ovšem toto zabezpečení se netýká aplikace WeChat, která jak již bylo zmíněno, podléhá kontrole čínských úřadů.

2.1 WhatsApp

WhatsApp je mobilní aplikace jejíž prostřednictvím lze zasílat zprávy, uskutečňovat hovory a sdílet multimediální obsah. WhatsApp byl spuštěn v roce 2009 a založili jej Brian Acton a Jan Koum, kteří chtěli vytvořit prostředek pro komunikaci, který by byl jednoduchý, rychlý a bezplatný. Původně byla aplikace zaměřena na textové zprávy, ale postupem času byly přidávány nové funkce, včetně hlasových hovorů, videokonferencí a dalších inovací. V roce 2014 aplikaci koupil Facebook, nyní Meta Platforms, Inc. Výhodou WhatsAppu je nezávislost na sociálních sítích. K používání stačí uživatelům pouze telefonní číslo.

WhatsApp je dostupný pro Android, Microsoft Windows, iOS, macOS i Linux. (Posílejte soukromé zprávy, 2024)

2.2 WeChat / Weixin

WeChat, vyvinutý čínskou společností Tencent v roce 2011, je jednou z nejpopulárnějších komunikačních aplikací v Číně, kde je známý pod názvem Weixin. Získal si mezinárodní uživatelskou základnu a jeho popularita spočívá v širokém spektru funkcí, které přesahují běžné komunikační platformy. WeChat kombinuje jak prvky sociální sítě, tak i chatovací platformy jako jsou textové a hlasové zprávy, videohovory a sdílení fotografií. Dále se využívá k provádění plateb, k online nakupování či rezervacím. Aplikace je dostupná pro Android, Microsoft Windows, iOS, macOS i Linux. (Binns, 2023)

Nutno dodat, že WeChat podléhá kontrole čínské vlády a cenzuře obsahu. To znamená, že veškerá komunikace a sdílený obsah skrze tuto platformu může být sledován a kontrolován čínskými úřady. Dále je nutné počítat i s tím, že WeChat uplatňuje cenzuru obsahu podle politických a sociálních směrnic stanovených čínskou vládou, což omezuje svobodu projevu uživatelů a jejich možnost přístupu k nezávislým informacím.

2.3 Facebook Messenger

Messenger je aplikace vyvinutá společností Facebook, Inc. a nyní ji vlastní společnost Meta Platforms, Inc. Slouží k posílání textových a hlasových zpráv, videohovorů, sdílení fotografií, videí, souborů a také k vytváření skupinových konverzací. Byla spuštěna v srpnu 2011 a nahradila Facebook Chat. V současné době mohou uživatelé používat Messenger, aniž by měli účet na Facebooku, jak tomu bylo v minulosti. Dnes stačí pouze zadat telefonní číslo. (Moreau, 2021)

Kromě toho, že je Messenger textovací aplikací, lze na něm zasílat i různé emotikony, nálepky a GIFy. Zahrnuje také funkci, kdy aplikace indikuje, pokud osoba na druhé straně chatu právě píše zprávu, údaj o potvrzení o přečtení, údaj o času, kdy byla zpráva odeslána a další údaj, kdy si příjemce přečetl poslední zprávu. V roce 2019 Messenger aktivoval možnost mazání zpráv z konverzace. Dříve bylo možné smazat z chatu zprávy jen pro odesílatele, ale v současné době Messenger disponuje funkcí smazat zprávy jak pro odesílatele, tak pro příjemce. Aplikace je dostupná pro Android, Microsoft Windows, iOS, macOS i Lunux. (Moreau, 2021)

2.4 Telegram

Aplikace Telegram byla poprvé uvedena v roce 2013 americkou společností Digital Fortress, za kterou stojí Pavel Durov, zakladatel ruské sociální sítě VKontakte. V současné době sídlí společnosti v Dubaji, jelikož kvůli sporům s ruskými úřady ohledně poskytování přístupu k uživatelským datům opustila svou základnu v Rusku. Telegram je komunikační aplikace, která klade důraz na rychlost a bezpečnost. Pro identifikaci uživatelů využívá stejně jako WhatsApp jejich telefonní číslo. Tato platforma je dostupná pro Android, Microsoft Windows, iOS, macOS i Linux. Uživatelé mohou používat Telegram na všech svých zařízeních současně, protože zprávy se synchronizují. Vedle textových zpráv umožňuje Telegram také posílat hlasové zprávy, dokumenty, fotografie, videa a sdílet aktuální polohu. (Telegram FAQ, 2024)

2.5 Instagram

Instagram je online sociální médium a platforma pro sdílení fotografií a krátkých videí. Aplikace byla spuštěna v roce 2010 a stáli za ní zakladatelé Kevin Systrom a Mike Krieger. Nyní ji vlastní společnost Meta Platforms, Inc., mateřská společnost Facebooku a je tudíž propojen s Facebookem a platformou X (dříve Twitter). Jsou zde dvě možnosti, jak mohou uživatelé sdílet svůj obsah, a to buď trvale ve svém „feedu“ nebo formou „stories“, které zmizí za 24 hodin. Uživatelé se mohou navzájem kontaktovat skrze soukromé zprávy, kam lze zasílat fotografie a videa a také mizející fotografie a videa, která slouží jen pro jednorázové zobrazení a poté nenávratně zmizí. Aplikace je dostupná pro Android, Microsoft Windows, iOS, macOS i Linux. (Eldridge, 2024)

2.6 Skype

Skype je komunikační platforma, která umožňuje uživatelům komunikovat prostřednictvím hovorů, videohovorů, textových zpráv a sdílením souborů. Skype byl spuštěn v roce 2003 a získal velkou popularitu díky své schopnosti poskytovat bezplatné hovory mezi uživateli, a to bez ohledu na to, kde se zrovna nacházejí. V současné době Skype vlastní společnost Microsoft, která jej koupila v roce 2010. Aplikace je dostupná pro Android, Microsoft Windows, iOS, macOS i Linux. (What is Skype?, 2024)

2.7 Signal

Signal je bezpečná a šifrovaná platforma pro okamžité zasílání zpráv, která klade důraz na ochranu soukromí uživatelů. Byla spuštěna v roce 2014 a nabízí širokou škálu funkcí, včetně textových zpráv, hlasových hovorů a videohovorů, sdílení fotografií a vytváření zabezpečených skupinových chatů. Signal vyniká svým důrazem na šifrování konverzací, které je založeno na open-source protokolu Signal. V aplikaci Signal nejsou žádné reklamy a tato platforma je dostupná pro Android, Microsoft Windows, iOS, macOS i Linux. (Proč používat službu Signal?, 2024)

2.8 Jami

Jami, dříve známý jako Ring a SFLphone, je komunikační aplikace zavedená v roce 2016. Tato platforma nabízí širokou škálu funkcí, včetně textových zpráv, hlasových zpráv a videohovorů, přenosu souborů a videokonferencí. Co Jami odlišuje od jiných aplikací je jeho základní technologie, která klade důraz na ochranu soukromí uživatelů a uživatel nepotřebuje k vytvoření účtu zadávat jakékoliv osobní údaje. Jami se vyznačuje jednoduchým rozhraním a poskytuje uživatelům možnost svobodné komunikace bez ohledu na to, zda jde o posílání zpráv, videohovory nebo sdílení souborů. Původně byl zaměřen na operační systém Linux, ale v současné době je dostupný i pro Microsoft Windows, MacOS, iOS a Android. (Sdílejte svobodně a soukromě, 2024)

2.9 Sumarizace charakteristik komunikačních aplikací

WhatsApp se dvěma miliardami aktivních uživatelů patří mezi nejpopulárnější komunikační platformy. Nabízí široké spektrum funkcí, včetně textových zpráv, hlasových hovorů a videokonferencí a je nezávislý na sociálních sítích. Facebook Messenger nabízí velmi obdobné služby jako WhatsApp a je mezi uživateli populární, což dokazuje i počet aktivních uživatelů, kterých je téměř jedna miliarda. Další aplikace Instagram slouží hlavně jako platforma pro sdílení fotografií a videí, ale také poskytuje možnost komunikace prostřednictvím soukromých zpráv. Všechny zmíněné aplikace patří do stáje společnosti Meta Platforms, Inc.

WeChat je populární platforma v Číně, která svými funkcemi přesahuje jiná komunikační média, avšak podléhá vládní kontrole a cenzuře. Telegram klade důraz na rychlost a bezpečnost a s 800 miliony aktivních uživatelů také patří k populárním komunikačním

platformám. Stejně tak platformy Signal, a Jami si zakládají na ochraně soukromí uživatelů a zabezpečení komunikace.

Poslední aplikace Skype je dlouholetým hráčem v oblasti digitální komunikace. Je schopen poskytovat stabilní a kvalitní videohovory a hovory a tím se stal oblíbenou volbou pro obchodní schůzky nebo rodinné hovory. I přes nástup novějších komunikačních platforem zůstává Skype populární volbou pro mnoho uživatelů díky své spolehlivosti, široké dostupnosti a integrovaným funkcím.

3 DATOVÁ BEZPEČNOST

V současné době, kdy jsou chatovací aplikace tak rozšířené a využívané téměř každým z nás, je třeba si uvědomit, že s jejich rostoucí popularitou přicházejí i nové výzvy a rizika. Je zajímavé sledovat, jak se tento digitální fenomén vyvíjí a adaptuje na potřeby moderního uživatele.

Předchozí kapitola se zabývala popisem existujících chatovacích aplikací a jejich funkcí, které nám tyto technologie nabízejí. Následující kapitola se však zaměřuje na méně viditelnou, avšak stejně důležitou tematiku a to datovou bezpečnost.

Jak se chatovací aplikace stávají stále více všudypřítomnými, je nezbytné zamyslet se nad bezpečnostními aspekty, které s sebou tato digitální propojení nesou. Kybernetické hrozby mohou mít různou podobu, od malwaru až po zneužití osobních dat. Pochopení základních principů ochrany soukromí a datové bezpečnosti by mělo být považováno za nezbytnou součást digitální gramotnosti každého jedince. Bez takového porozumění se uživatelé mohou snadno stát terčem kybernetických útoků, které mohou mít devastující dopady nejen na digitální, ale i reálné životy. Pochopení základních principů datové bezpečnosti by mělo být považováno za nezbytnou součást digitální gramotnosti každého jedince.

Datová bezpečnost představuje klíčový prvek v digitálním prostředí, jehož hlavním cílem je zajistit ochranu informací a dat před neoprávněným přístupem, ztrátou, poškozením, zneužitím nebo krádeží. V kontextu datové bezpečnosti je nezbytné identifikovat citlivá data a specifikovat, jakým způsobem by s nimi mělo být zacházeno. To obnáší definování oprávnění pro přístup k datům a stanovení postupů pro bezpečné sdílení informací. Součástí strategie na ochranu dat je také systematické zálohování a obnovení informací s ohledem na neočekávané události, jako jsou havárie systémů, počítačové útoky nebo přírodní katastrofy. (Kolouch et al., 2019)

Je tedy důležité definovat si několik základních pojmů, které souvisí s datovou bezpečností.

3.1 Kyberprostor

Kyberprostor (anglicky *Cyberspace*) se používá k označení virtuální reality v počítačovém světě. Je to elektronické médium, které slouží k usnadnění online komunikace. Termín kyberprostor může být použit pro označení jakéhokoli systému s výraznou uživatelskou základnou nebo pro systém s dobře navrženým uživatelským rozhraním. Zjednodušeně lze konstatovat, že kyberprostor zahrnuje celý internet. (Rouse, 2023)

Tato virtuální realita je úzce propojená s materiální podstatou, což znamená, že je závislá na technologiích existujících ve skutečném světě. Kyberprostor představuje nehmotné médium, které využívá prvky z reálného světa, jako jsou jednotlivé počítačové systémy a cloudová úložiště a kde se také odehrávají různé digitální aktivity, včetně komunikace, obchodu, zábavy či výzkumu. Propojení s materiálním prostředím umožňuje kyberprostoru adaptovat se na změny a poškození. Nicméně pokud všechny jeho součásti úplně selžou, může to vést k nevratnému poškození nebo zániku kyberprostoru jako entity. (Ning, 2022)

Zásadní charakteristikou kyberprostoru je schopnost jednotlivých uživatelů internetové sítě rychle a snadno komunikovat a sdílet soubory prostřednictvím služeb pro okamžité zasílání zpráv. Dále také hrát online hry a v neposlední řadě provádět platební transakce. (Rouse, 2023)

V souvislosti s kyberprostorem se vyskytují tři hlavní segmenty, a to Surface Web, Deep Web a Dark Web. Surface Web je takzvaný povrchový web, který představuje veřejně přístupnou část internetu, kterou lze procházet pomocí běžných webových prohlížečů, jako jsou například Google, YouTube a Seznam. (Kolouch, 2016)

Deep Web neboli hluboký web zahrnuje část internetu, která není veřejně dostupná. Patří sem například vědecké práce, finanční záznamy, vládní dokumenty nebo další online služby, které vyžadují přihlášení. Tato část internetu není automaticky viditelná a přístupná pro každého. (Kolouch, 2016)

Poslední vrstvou je Dark Web, tedy temný web, a představuje záměrně skrytou část internetu, která je nepřístupná pro běžné uživatele. Je známý svou schopností uchovávat anonymitou ale často slouží nejen k nelegálním aktivitám, ale rovněž poskytuje možnost svobodné komunikace bez omezení. Uživatelé musí použít speciální software, aby na něj mohli přistupovat. (Kolouch, 2016)

3.1.1 Kybernetické riziko

Představuje potenciální hrozbu, které organizace nebo jednotlivec čelí v digitálním prostředí v důsledku možného útoku, zneužití nebo neoprávněného přístupu k informacím či datům, Jedná se o možnost, že kybernetický útok může mít negativní dopad na bezpečnost, integritu nebo dostupnost digitálních systémů a dat. (Kolouch et al., 2019)

3.1.2 Aktivum

V oblasti kybernetické bezpečnosti je aktivum vnímáno jako cokoliv, co má pro organizaci hodnotu a co by mohlo být vystaveno kybernetickému riziku. Tato aktiva zahrnují informace, data, hardware (počítače, servery) software, sítě, zařízení a další prvky, které jsou klíčové pro bezproblémový chod organizace. Za aktivum lze také považovat faktory, které ovlivňují funkčnost a dostupnost systému. Patří sem také reputace a dobré jméno organizace a lidé (uživatelé) s jejich znalostmi a zkušenostmi. (Kolouch et al., 2019)

3.1.3 Zranitelnost

Zranitelnost označuje slabiny či nedostatečné zabezpečení softwaru nebo aktiv, která mohou být zneužita útočníky. Příčiny zranitelnosti jsou různorodé a mohou zahrnovat lidské chyby, technické nedostatky nebo vnější faktory jako je vyšší moc. Zranitelnosti lze rozdělit na dvě kategorie a to jako opravené a neopravené, kdy opravené jsou ty, na které již výrobce vydal aktualizaci nebo zabezpečení. Naopak neopravené zranitelnosti jsou takové, které jsou známy výrobci, ale dosud nebyla provedena jejich oprava. (Kolouch et al., 2019)

3.2 Kyberkriminalita

Kyberkriminalita, také označovaná jako počítačová nebo IT kriminalita, představuje označení pro trestné činy, které jsou spáchány v kyberprostoru. Tyto činy zahrnují širokou škálu aktivit, včetně podvodů, krádeží identity, kyberšikany, poškozování dat nebo počítačových systémů. Jsou to nelegální činy, které využívají informační a komunikační technologie k dosažení svých cílů. (Shaw, 2020)

Kyberkriminalita reprezentuje škodlivé aktivity, kdy se kyberzločinci zaměřují především na oblasti jako bankovní nebo e-mailové účty. V prvním případě je jejich cílem získání hesel a informací nutných k neoprávněnému přístupu k bankovním účtům, čímž dochází k odčerpání finančních prostředků obětí. Druhá oblast kyberkriminality zahrnuje krádeže osobních dat uživatelů a shromažďování kontaktů pro spam a další nelegální aktivity, což vede k ohrožení soukromí a bezpečnosti jednotlivců. (Co je kyberkriminalita, 2022)

Zločinci v kyberprostoru se neomezují pouze na tyto aktivity. Mohou se také dopouštět vydírání, kdy využívají získané informace k vydírání obětí za účelem finančního zisku nebo jiných výhod. Dalším závažným prvkem kyberkriminality je sabotáž firemních serverů, což může mít zásadní následky pro podniky, ať už jde o ztrátu dat nebo narušení obchodních operací. Zároveň mohou zločinci jednat z osobních důvodů, včetně pomsty vůči konkrétním

osobám či subjektům, což dodává kyberkriminalitě rozměr osobního konfliktu. (Co je kyberkriminalita, 2022)

3.3 Kybernetické hrozby

Kybernetické hrozby, známé také jako hrozby kybernetické bezpečnosti, představují různé formy možných škodlivých pokusů o narušení počítačových systémů. Cílem těchto útoků je neoprávněný přístup k datům, narušení IT systémů nebo únik informací. (Co jsou kybernetické hrozby, 2023)

Zdroje kybernetických hrozeb jsou v první řadě záměrné, kdy útočník směřuje k úmyslnému poškození nebo smazání dat, fyzickému poškození počítačového systému nebo krádeži dat a informací. Druhou kategorií jsou hrozby způsobené nedbalostí, což zahrnuje neúmyslné smazání dat, fyzické poškození počítačového systému v důsledku náhodného pádu nebo poškození dat na základě nevědomosti uživatele. Dalším zdrojem hrozeb jsou technické chyby, včetně chyb softwaru nebo hardwaru, které mohou být využity k neoprávněnému přístupu nebo poškození dat. Tato kategorie zahrnuje i hrozby způsobené vyšší mocí, jako jsou neplánované výpadky napájení, přírodní katastrofy a požáry, které mohou způsobit ztrátu nebo nefunkčnost systémů. (Kolouch et al., 2019)

Útoky jsou iniciovány buď jednotlivci, nebo různými subjekty. Mezi těmito subjekty mohou být teroristické skupiny, zločinecké organizace, hackeři ale nespokojení zaměstnanci nebo firemní špioni uvnitř organizace. (Co jsou kybernetické hrozby, 2023)

Škodlivé útoky mají různé motivace a mohou vážně ohrozit bezpečnost a integritu digitálního prostředí. Pokud kybernetická hrozba vychází z úmyslného jednání člověka, lze do motivace zařadit získání finančního prospěchu, kdy útočníci mohou být motivování touhou po získání peněz prostřednictvím nelegálních aktivit, jako jsou krádeže bankovních údajů a vydírání. Další motivací je získání konkurenční převahy, kdy podniky mohou chtít získat výhodu nad konkurencí tím, že budou schopny získat citlivé a strategické informace o svých soupeřích, což jim umožňuje dosáhnout lepší pozice na trhu. Někteří hackeři mohou být motivování snahou předvést své schopnosti a získat uznání ve světě kybernetické bezpečnosti. Tato motivace vede k různým formám útoků, které mají za cíl demonstrovat jejich technické dovednosti. I odplata může být dalším důvodem kybernetických útoků. Útočníci mohou jednat odvetně za dřívější události, buď na osobní úrovni, nebo motivované nějakým konfliktem či sporem. Nakonec i nespokojení zaměstnanci nebo další vnitřní aktéři

mohou být motivováni neplněním povinností nebo nespokojeností se svou pozicí. (Kolouch et al., 2019)

Existuje mnoho různých typů kybernetických hrozeb, které mohou ohrozit bezpečnost digitálního prostředí. Tyto hrozby lze rozdělit do několika hlavních kategorií:

3.3.1 Sociální inženýrství

Sociální inženýrství představuje specifický typ kybernetického útoku, který se zaměřuje na manipulaci a získávání důvěry obětí. Jeho hlavním cílem je získání citlivých informací, neoprávněný přístup k systémům nebo provedení jiných nežádoucích akcí. Na rozdíl od technicky orientovaných útoků se sociální inženýrství spoléhá na psychologické techniky a sociální interakce. Tato strategie využívá lidské důvěřivosti, nevědomosti nebo přílišné důvěrnosti a je spojena s různými formami podvodů, kde útočníci využívají emocionálních reakcí svých obětí k dosažení svých záměrů. (Sociální inženýrství, 2016)

3.3.2 Phishing

Typickým příkladem sociálního inženýrství je phishing, což představuje strategii, při které se útočníci zaměřují na uživatele prostřednictvím podvodných e-mailů, klamavých webových stránek nebo sociálních sítí. Cílem těchto útoků je získat citlivé informace jako jsou hesla nebo údaje z platebních karet. Útočníci se snaží vytvořit iluzi důvěryhodné komunikace nebo webové stránky, aby uživatele nalákali k poskytnutí svých citlivých dat tím, že je uživatel na těchto podvodných stránkách vyplní. Tento druh útoku je často maskován za legitimní komunikaci od bank, firem nebo jiných známých institucí, což zvyšuje pravděpodobnost, že oběť bude oklamána.

Do phishingu se také řadí **spear phishing**. Jde o precizní a sofistikovaný podvod, při kterém je oběť útoku po delší dobu systematicky sledována s cílem získat o ní co nejvíce osobních informací. Útočníci čerpají z různých dostupných zdrojů, jako jsou profily na sociálních sítích, osobní webové stránky nebo účast oběti na konkrétní akci. Získaná data pak slouží k vytvoření autentického a přesvědčivého obsahu e-mailu nebo zprávy, která je na míru přizpůsobena konkrétní oběti. Tímto způsobem se zvyšuje pravděpodobnost, že se oběť „chytí“, protože komunikace je utvořena tak, aby byla co nejvíce personalizovaná.

Pro tento typ podvodu se často využívají sociální sítě a IM. Jde o situace, kdy útočníci pošlou oběti odkazy na nebezpečný software právě prostřednictvím těchto komunikačních sítí jako je Messenger, Facebook atd. (Phishing - stále aktuální hrozba, 2015)

3.3.3 Malware

Malware je zkratka pro škodlivý software (anglicky *Malicious Software*) a představuje různé formy kybernetických hrozeb, včetně virů, trojských koní, ransomware a spyware. Při těchto útocích pachatelé získávají kontrolu nad zařízením oběti útoku, jako jsou počítače, mobilní zařízení, tablety atd. Toto může vést k poškození, odcizení nebo vymazání dat, sledování aktivit uživatelů, uzamčení souborů a následnému požadování výkupného. (What is malware?, 2024)

3.3.4 DoS, DDoS útoky

Hrozby distribuovaného odmítnutí služby (anglicky *Denial of Service* a *Distributed Denial of Service*) jsou útoky, při kterých jsou cílené webové stránky nebo online služby v jednu chvíli zahlcovány velkým množstvím požadavků, což způsobuje nedostupnost pro běžné uživatele. (Nejzávažnější kybernetické hrozby v EU, 2024)

Funguje to tak, že útočník si vytvoří vzdálenou kontrolu nad několika zařízeními pomocí malwaru, čímž vytvoří síť botů. Následně, bez vědomí vlastníků těchto zařízení, útočník využívá tuto botnet síť k masivnímu útoku na konkrétní webovou stránku. Výsledkem je, že tato webová stránka se stává nedostupnou. (Bhattacharyya, Kalita, 2016)

3.4 Triáda CIA

Triáda CIA je jedním ze základních pilířů v oblasti informační bezpečnosti a definuje tři klíčové aspekty, které by měly být chráněny v rámci jakéhokoli informačního systému a dat. Tato triáda zahrnuje tři složky a to důvěrnost, integritu a dostupnost.

Princip důvěrnosti (anglicky *Confidentiality*) je zaměřen na udržení informací v tajnosti. Zároveň to znamená, že se informace mají udržet nedostupné pro neoprávnění osoby. Hlavním cílem tohoto principu je zabezpečit, že pouze osoby s oprávněním mají přístup k citlivým datům. Pro zajištění důvěrnosti se využívají různé metody jako je šifrování dat, ověřování totožnosti uživatelů (autentizace) a striktní správa přístupových práv. Tímto způsobem je zajištěno, že citlivé informace zůstanou nepřístupné pro neoprávněné subjekty a budou chráněny před neoprávněným přístupem či zneužitím. (Daimi, 2018)

Princip integrity (anglicky *Integrity*) se zaměřuje na udržení přesnosti a neporušenosti dat. Znamená to, že data zůstávají nedotčená a neměnná a jsou uživateli doručena v původním stavu beze změn nebo úprav. Cílem tohoto principu je zajistit, že data zůstanou neporušena po celou dobu své existence. Pro zajištění integrity dat se používají různé metody. Jedním

z běžných postupů je používání digitálních podpisů, které slouží k ověření autentičnosti a původu dat. Tímto způsobem lze garantovat, že data nebyla pozměněna bez povolení. Další používanou technikou jsou kontrolní součty, které umožňují ověřit, zda se data změnila od okamžiku svého vytvoření. (Daimi, 2018)

Princip dostupnosti (anglicky *Availability*) zaručuje, že data budou kdykoliv dostupná pro oprávněné uživatele, kteří je potřebují. Hlavním cílem je umožnit oprávněným uživatelům bezproblémový přístup k datům bez omezení. K dosažení této dostupnosti je nezbytné přijmout opatření, která minimalizují výpadky systémů. To zahrnuje implementaci zálohování dat pro případ výpadků, vytváření redundance v infrastruktuře a pravidelnou údržbu systémů. Tímto způsobem se předchází či odolává možným útokům, jako jsou DoS (*Denial of Service*), které by mohly omezením přístupu k datům narušit běžný chod systému. (Daimi, 2018)

Triáda CIA slouží k ochraně zásadních aspektů dat v informačních systémech. Principy důvěrnosti, integrity a dostupnosti společně tvoří klíčový rámec pro udržení bezpečnosti informací. Spojením těchto principů se vytváří efektivní ochrana proti různým hrozbám a nebezpečím, což zásadně přispívá k celkové bezpečnosti IT systémů.

3.5 Traffic Light Protocol

Sdílení informací je zásadní, ale stejně důležité je chránit citlivá data. Proto byl v roce 2000 vytvořen protokol TLP (*Traffic Light Protocol*) což je standardní systém klasifikace a sdílení citlivých informací mezi organizacemi a jednotlivci. Tento protokol umožňuje bezpečnou a efektivní výměnu informací v rámci různých subjektů a zároveň poskytuje jasná pravidla pro ochranu těchto informací. (Roccia, 2023)

TLP definuje čtyři úrovně klasifikace citlivosti informací:

Červená (TLP: RED) – Červené informace jsou extrémně citlivé a mohou být sdíleny pouze s omezeným okruhem důvěryhodných adresátů, kteří mají nezbytnou potřebu znalostí. Tyto informace mohou obsahovat kritické a nebezpečné údaje, jejichž zneužití by mohlo mít závažné následky.

Oranžová (TLP: AMBER) – Oranžová klasifikace označuje informace, které mohou být sdíleny pouze s omezeným okruhem adresátů, kteří mají legitimní potřebu znalosti. Tato klasifikace může obsahovat omezené množství citlivých údajů a jejich neopatrné sdílení by mohlo negativně ovlivnit bezpečnost.

Zelená (TLP: GREEN) – Informace označené jako zelené jsou považovány za omezeně citlivé a mohou být bezpečně sdíleny v rámci určité komunity ale ne skrze veřejně přístupné kanály. Tyto informace nesmí být zveřejněny mimo komunitu.

Bílá (TLP: CLEAR) – Bílá klasifikace znamená, že informace nejsou klasifikovány podle TLP a mohou být volně sdíleny bez omezení. Tyto informace obvykle neohrožují bezpečnost, integritu nebo dostupnost systémů. (Roccia, 2023)

Cílem Traffic Light Protocolu je zlepšit spolupráci a sdílení informací mezi organizacemi a jednotlivci a zároveň chránit citlivá data před neoprávněným přístupem a zneužitím. TLP poskytuje jednoduchý a srozumitelný systém klasifikace, který usnadňuje správu a ochranu citlivých informací tím, že poskytuje jasný rámec pro určení, jaké informace lze sdílet a s kým. To pomáhá lépe reagovat na kybernetické hrozby a účinněji spolupracovat při ochraně před kybernetickými útoky a zneužitím dat.

3.6 Kybernetická bezpečnostní událost

Kybernetická bezpečnostní událost je širší kategorií, která zahrnuje všechny možné situace nebo jevy, které by mohly mít bezpečnostní následky, ačkoliv v danou chvíli nebylo zaznamenáno žádné konkrétní ohrožení bezpečnosti informací, tedy důvěrnosti, integrity nebo dostupnosti. Může se jednat o různé situace, jako například ztráta vstupní karty nebo detekci potenciálně nebezpečného provozu na síti jako je malware. Lze tedy říci, že se jedná o existenci hrozby, která nemusí být reálná. (Řešení bezpečnostních událostí a incidentů s využitím SOC a IRT, 2022)

3.7 Kybernetický bezpečnostní incident

V případě kybernetického bezpečnostního incidentu jde o situaci, kdy už skutečně dojde k narušení bezpečnosti informací. To zahrnuje konkrétní události, jako je neoprávněný přístup k systému, únik citlivých informací nebo útok na systém, který má za následek porušení integrity informací. Incidenty představují akce nebo události, během nichž je ohrožena kybernetická bezpečnost a dochází k reálným následkům na bezpečnostní úrovni. Tyto incidenty mohou ovlivnit běžný chod systému a vyžadovat okamžitou reakci k jejich řešení. (Řešení bezpečnostních událostí a incidentů s využitím SOC a IRT, 2022)

3.8 Legislativa v oblasti kybernetické bezpečnosti

V České republice je vrcholným správním orgánem v oblasti kybernetické a informační bezpečnosti Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Jeho působnost zahrnuje problematiku kybernetické bezpečnosti, včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Vznikl v roce 2021 a sídlí v Brně. (NÚKIB a legislativa, 2021)

Zákonem, který u nás upravuje kybernetickou bezpečnost je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů. Zákon v České republice vstoupil v platnost 29. srpna 2014 s účinností od 1. ledna 2015 a od tohoto data jsou jeho ustanovení právně závazná. (ČESKO, 2014)

Tento zákon definuje důležité pojmy a principy v oblasti kybernetické bezpečnosti, stanovuje povinnosti pro poskytovatele kybernetických služeb a další aktéry. Také stanovuje opatření pro ochranu kybernetického prostoru. Hlavním úkolem tohoto zákona je zajistit odpovídající úroveň kybernetické bezpečnosti v České republice a chránit kritickou informační infrastrukturu. (ČESKO, 2014)

3.9 Vyhlášky Národního úřadu pro kybernetickou bezpečnost

Vyhlášky Národního úřadu pro kybernetickou bezpečnost slouží k upřesnění a implementaci právních předpisů v oblasti kybernetické bezpečnosti. Tyto vyhlášky jsou vydávány v souladu s platnými zákony a směrnicemi a mají za cíl poskytnout detailní pravidla, postupy a požadavky které jsou potřebné k zajištění kybernetické bezpečnosti v různých oblastech.

Vyhláška Národního úřadu pro kybernetickou bezpečnost č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby se týká kritérií pro identifikaci provozovatele základní služby a byla zveřejněna 15. prosince 2017 ve Sbírce zákonů České republiky. Tuto vyhlášku připravil Národní úřad pro kybernetickou a informační bezpečnost ve spolupráci s odborným sektorem. Jejím cílem je implementovat požadavky Směrnice Evropského parlamentu a Rady (EU) 2016/1148, známé jako Směrnice NIS, která stanovuje opatření pro zajištění vysoké úrovně bezpečnosti sítí a informačních systémů v Evropské unii. Tato vyhláška specifikuje kritéria pro určení provozovatelů základních služeb a definuje míru významnosti narušení těchto služeb v kontextu zabezpečení společenských a ekonomických aktivit, jak je uvedeno v § 22a odst. 1 zákona o kybernetické bezpečnosti. Vyhláška nabyla účinnosti od 1. února 2018. (Legislativa KB, 2024)

Vyhláška Národního úřadu pro kybernetickou bezpečnost č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu obsahuje požadavky a specifické podmínky, které musí poskytovatelé cloudových služeb splňovat pro zápis do katalogu cloud computingu. To zahrnuje technické a organizační požadavky týkající se bezpečnosti dat, dostupnosti služeb, ochrany soukromí a dalších aspektů cloudového prostředí. Dále také postup pro zápis do katalogu cloud computingu, včetně dokumentace a informací, které musí poskytovatelé předložit pro hodnocení jejich služeb. Upravuje podmínky pro provoz a údržbu katalogu cloud computingu a způsob zveřejňování informací o zapsaných poskytovatelích. Vyhláška vstoupila v platnost 1. září 2021. (ČESKO, 2021)

Vyhláška Národního úřadu pro kybernetickou bezpečnost č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci vstoupila v platnost dne 1. září 2021 a obsahuje specifikaci bezpečnostních úrovní pro využívání cloudových služeb, které mají orgány veřejné moci dodržovat. Tato kritéria zahrnují technické, organizační a právní požadavky týkající se zabezpečení dat, dostupnosti služeb, správy identit, řízení přístupu a dalších aspektů. Zahrnuje také postup pro hodnocení a ověření dodržování bezpečnostních úrovní orgány veřejné moci při využívání cloudových služeb a způsob zveřejňování informací o dodržování bezpečnostních úrovní a monitoring jejich dodržování. (ČESKO, 2021)

Vyhláška Národního úřadu pro kybernetickou bezpečnost č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu vymezuje povinnosti a požadavky, které musí orgány veřejné moci dodržovat při využívání cloudových služeb. Jedním z hlavních aspektů této vyhlášky je stanovení bezpečnostních opatření, která mají být přijata pro ochranu dat a informací orgánů veřejné moci uložených v cloudovém prostředí. Dále stanovuje postupy pro hodnocení a ověření dodržování bezpečnostních pravidel a způsob zveřejňování informací o bezpečnosti cloudových služeb využívaných orgány veřejné moci. Cílem této vyhlášky je zajistit, aby orgány veřejné moci správně a odpovědně využívaly cloud computing s důrazem na ochranu citlivých dat a informací a minimalizaci rizik spojených s jejich ukládáním a zpracováním v cloudovém prostředí. (ČESKO, 2023)

3.10 Směrnice NIS a NIS 2

Evropská unie se také zabývá bezpečností na úrovní sítí a informačních systémů v členských státech EU a proto vydala směrnici NIS (*Network and Information Security*). Jde o dokument

s názvem **Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii** a je to legislativní nástroj Evropské unie zaměřený na zlepšení kybernetické bezpečnosti v členských státech. Cílem této směrnice je posílit odolnost Evropské unie proti kybernetickým hrozbám a zvýšit úroveň ochrany sítí a informací v klíčových odvětvích a institucích. (ČESKO, 2016)

Směrnice NIS stanovuje minimální požadavky na kybernetickou bezpečnost, které musí členské státy zavést a dodržovat. Tyto požadavky se týkají hlavně kritické infrastruktury a klíčových služeb, jako jsou energetika, doprava, bankovnictví a zdravotnictví. Podle směrnice musí tyto subjekty přijmout opatření k prevenci a reakci na kybernetické incidenty a zajistit dostatečnou úroveň ochrany svých sítí a informací. (ČESKO, 2016)

Dalším důležitým prvkem směrnice NIS je zavedení mechanismů spolupráce a výměny informací mezi členskými státy a evropskými institucemi. To má za cíl posílit schopnost rychle reagovat na kybernetické hrozby a koordinovat společné akce v případě krizových situací. (ČESKO, 2016)

Implementace směrnice NIS přináší výzvy, ale také příležitosti pro zlepšení kybernetické bezpečnosti a posílení ochrany dat v rámci EU. Přispívá k vytvoření společného evropského přístupu k řešení kybernetických hrozeb a posiluje spolupráci mezi členskými státy a dalšími relevantními subjekty. Směrnice NIS tak představuje důležitý krok směrem k zajištění odolnosti a bezpečnosti digitálního prostoru v Evropské unii v době neustále se zvyšujícího počtu kybernetických hrozeb a incidentů. (ČESKO, 2016)

Směrnice NIS byla přijata Evropským parlamentem a Radou Evropské unie v roce 2016 a členské státy měly povinnost transponovat její ustanovení do své vnitrostátní legislativy do května 2018. Od té doby byla směrnice doplněna dalšími právními předpisy, jako je Nařízení o kybernetické bezpečnosti (EU) 2019/881, které rozšiřuje rozsah směrnice NIS na další subjekty a posiluje spolupráci mezi členskými státy v oblasti kybernetické bezpečnosti.

(ČESKO, 2016)

Nicméně Evropská Unie vydala další dokument s názvem **Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148**. Jde o směrnici NIS 2 a jedná se o právní nástroj Evropské unie, který posiluje kybernetickou

bezpečnost a ochranu sítí a informací v rámci členských států. Jedná se o revizi původní směrnice NIS, která byla schválena v roce 2016, a která má za cíl reagovat na nové a rostoucí výzvy v oblasti kybernetických hrozeb a digitální bezpečnosti. (ČESKO, 2022)

Směrnice NIS 2 se zaměřuje na posílení odolnosti digitální infrastruktury, veřejných služeb a digitálních služeb v EU prostřednictvím stanovení přísnějších požadavků na kybernetickou bezpečnost. Zahrnuje nové povinnosti pro provozovatele kritických infrastruktur a digitálních služeb, včetně rozšířených požadavků na zabezpečení sítí a informačních systémů, hlášení kybernetických incidentů a spolupráci s národními bezpečnostními orgány. Nejdůležitější změnou směrnice NIS 2 je rozšíření rozsahu subjektů, na které se vztahuje. Tato směrnice má být transponována do vnitrostátního práva do 17. října 2024.

(ČESKO, 2022)

3.11 Vyhlášky Národního bezpečnostního úřadu

Národní bezpečnostní úřad (NBÚ) je orgánem moci výkonné a byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, účinný od 1. srpna 1998. NBÚ má ve své pravomoci ochranu utajovaných informací a hodnocení bezpečnostní způsobilosti. Výkon pravomocí NBÚ se řídí v souladu se Zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Kontrolu nad činností NBÚ provádí Poslanecká sněmovna Parlamentu České Republiky prostřednictvím zvláštního kontrolního orgánu a to Stálé komise pro kontrolu činností NBÚ. Tento orgán také vydává vyhlášky, které se týkají kybernetické bezpečnosti. (Národní bezpečnostní úřad, 2024)

Vyhláška Národního bezpečnostního úřadu č. 316/2014 Sb., o kybernetické bezpečnosti se zaměřuje na problematiku kybernetické bezpečnosti a upravuje konkrétní opatření a pravidla týkající se ochrany informačních systémů a dat. Tato vyhláška stanovuje požadavky pro informační systémy, které spadají do kategorie kritické informační infrastruktury, včetně komunikačních systémů, významných informačních systémů a systémů poskytovatelů digitálních služeb. Tato vyhláška upravuje obsah a formát bezpečnostní dokumentace, rozsah bezpečnostních opatření, klasifikace a ohodnocení kybernetických bezpečnostních incidentů, procesy hlášení těchto incidentů a postupy pro reaktivní opatření. Také specifikuje náležitosti oznámení o provedení reaktivních opatření a formát kontaktních údajů. Zároveň stanovuje postupy pro likvidaci dat, provozních údajů a informací v souladu s bezpečnostními normami. (Legislativa KB, 2024)

Vyhláška Národního bezpečnostního úřadu č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích obsahuje specifikaci významných informačních systémů, jejich definující kritéria a postupy pro jejich hodnocení. Tato kritéria mohou zahrnovat například dopad na kritické infrastruktury, citlivost dat, počet uživatelů nebo oblast působnosti systému. Cílem této vyhlášky je poskytnout jasný rámec pro identifikaci a hodnocení informačních systémů, které jsou klíčové z hlediska kybernetické bezpečnosti. (ČESKO, 2014)

V roce 2020 byla schválena novela vyhlášky, která má za cíl upřesnit kritéria pro stanovení, zda je daný informační systém považován za významný. Novela rozděluje účinnost změněného znění vyhlášky do tří fází, přičemž první fáze vstoupila v platnost 1. ledna 2021, druhá fáze 1. ledna 2022 a třetí fáze nabyla účinnosti 1. ledna 2023. (Legislativa KB, 2024)

3.12 Ochrana dat v digitálním prostředí

Datová bezpečnost je důležitým prvkem v digitálním světě, kde se informace stávají stále cennějšími aktivy. Současná digitální éra s sebou přináší nové výzvy a rizika, která jsou spojena s kyberprostorem a kybernetickými hrozbami. Kybernetické riziko, aktivum a zranitelnost jsou klíčovými pojmy, které ovlivňují bezpečnost datových systémů.

Mezi nejvýznamnější formy kybernetických hrozeb patří kyberkriminalita, která zahrnuje různé techniky jako je sociální inženýrství, phishing, malware a DDoS útoky. Tyto hrozby ohrožují důvěrnost, integritu a dostupnost datových systémů a mohou mít značný dopad na organizace i jednotlivce.

V rámci ochrany datových systémů je důležité chápat koncept triády CIA, který zdůrazňuje důležitost zachování důvěrnosti, integrity a dostupnosti dat a s tím související Traffic Light Protocol, který utváří rámec pro klasifikaci citlivých informací. A dále se také kybernetické bezpečnostní události a incidenty se stávají stále častějšími a organizace musí být připraveny na jejich řízení a řešení.

V České republice hraje klíčovou roli v monitorování kybernetických hrozeb a poskytování odborného poradenství a podpory Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Legislativa je dalším důležitým prvkem, který stanovuje povinnosti a zodpovědnosti v oblasti kybernetické bezpečnosti.

Lze tedy konstatovat, že efektivní ochrana datových systémů vyžaduje komplexní přístup zahrnující technická opatření, provozní postupy, školení zaměstnanců a spolupráci s kybernetickými autoritami a regulátory.

4 TECHNOLOGIE ZAJIŠŤUJÍCÍ DATOVOU BEZPEČNOST V KOMUNIKAČNÍCH APLIKACÍCH

Zajištění datové bezpečnosti v prostřední služeb pro okamžité zasílání zpráv je podstatným aspektem pro zachování soukromí a ochranu informací v digitálním světě. Existuje několik klíčových technologií a opatření, které jsou nezbytné pro efektivní zabezpečení dat a k zaručení ochrany citlivých informací v komunikačních platformách. Je důležité si uvědomit, že ochrana dat není pouze otázkou technologie, ale také správného nastavení procesů a osvěty uživatelů. Informovanost uživatelů o rizicích spojených s IM komunikací hraje zásadní roli v zajištění bezpečnosti komunikace a ti by měli být vedeni k tomu, aby přijímali správné bezpečnostní praktiky, Tato kapitola se zaměřuje na několik nejdůležitějších technologií a strategií, které jsou nezbytné pro efektivní zabezpečení přenosu dat a soukromí uživatelů.

4.1 Symetrické a asymetrické šifrování

Symetrické a asymetrické šifrování jsou základními pilíři v oblasti kryptografie, která se zabývá zabezpečením a šifrováním dat. Kryptografie studuje metody zabezpečení komunikace a uchovávání dat pomocí matematických a algoritmických postupů, a to jak pro ochranu před neoprávněným přístupem, tak i pro zajištění důvěrnosti a integrity dat. (Menezes et al., 2018)

Symetrické šifrování využívá jeden společný klíč jak pro šifrování, tak dešifrování dat. Tento klíč musí být sdílen mezi odesílatelem a příjemcem předem, aby mohli úspěšně komunikovat. Princip fungování symetrického šifrování spočívá v tom, že data jsou zašifrována pomocí tohoto společného klíče na straně odesílatele a poté dešifrována na straně příjemce. Příklady symetrických šifrovacích algoritmů zahrnují AES (*Advanced Encryption Standard*) a DES (*Data Encryption Standard*). Symetrické šifrování je často rychlejší než asymetrické, ale vyžaduje důvěrnou výměnu klíčů mezi komunikujícími stranami. (Banoth, Regar, 2023)

Na rozdíl od symetrického šifrování, asymetrické šifrování používá dvojici klíčů - veřejný a privátní. Veřejný klíč je sdílen otevřeně a slouží k šifrování dat, zatímco privátní klíč je držen tajně a slouží k jejich dešifrování. Odesílatel může použít veřejný klíč příjemce k šifrování zprávy, kterou poté příjemce dešifruje pomocí svého privátního klíče. Tato asymetrická struktura umožňuje bezpečnou výměnu šifrovacích klíčů bez potřeby sdílení tajného klíče.

Asymetrické šifrování je pomalejší než symetrické, ale nabízí vyšší úroveň bezpečnosti díky oddělení veřejného a privátního klíče. (Banoth, Regar, 2023)

4.2 End-to-end šifrování

Koncové šifrováním, známé také jako end-to-end šifrování (anglicky *end-to-end encryption* – E2EE), se zaměřuje na ochranu výměny dat mezi zařízeními. Princip koncového šifrování spočívá v tom, že zpráva je zašifrovaná na koncovém bodě odesílatele a až poté je dešifrována na koncovém bodě příjemce. To znamená, že nikdo jiný mimo odesílatele a příjemce nemá schopnost číst obsah těchto zpráv a to včetně poskytovatele služby, kterou uživatelé používají k odesílání a přijímání zpráv. (Koncové šifrování – co to je a proč jej používat?, 2023)

Koncové šifrování se tímto liší od tradičních šifrovacích postupů, které se zaměřují na ochranu dat při přenosu a to tím, že data nejsou nikdy dešifrována na serveru. Bezpečnost na úrovni zařízení skrze koncové šifrování je dosažena pomocí jedinečného páru veřejného a privátního klíče. Tyto klíče jsou generovány při vytváření nového účtu. Když tedy poté uživatel zahájí komunikaci, protokoly koncového šifrování vygenerují jedinečný pár těchto šifrovacích klíčů a stažením veřejného klíče příjemce, který je uložen na serveru, jsou data zašifrována na koncovém bodě odesílatele. Veřejný klíč může být sdílen se všemi uživateli, zatímco privátní klíč zůstává k dispozici pouze na zařízení jednotlivce. Tento privátní klíč tak slouží k dešifrování dat a tím se vytváří bezpečný komunikační kanál, který chrání citlivé informace. Uchováním uživatelova privátního kryptografického klíče na jeho koncovém bodě tudíž nejsou nikdy klíče dostupné na serveru. Server tedy nemůže získat přístup k dešifrovacím klíčům a tím pádem ani nemůže dešifrovat data, což znamená, že ani zločinci ani třetí strany tak nemohou data vidět. (Berlove, 2024)

Koncepce end-to-end šifrování existuje již dlouho, ale získala na významu s rozvojem a nárůstem digitální komunikace a technologickým pokrokem. V počátcích nového tisíciletí se objevily návrhy na zavedení koncového šifrování pro internetovou komunikaci, avšak tyto koncepty byly v raných fázích vývoje a nebyly plně vypracované. Změna nastala, když Edward Snowden odhalil informace o špionáži, sledování telefonů a elektronické komunikace. Po těchto odhaleních začala veřejnost požadovat implementaci koncového šifrování v komunikačních službách. (Oppliger, 2020)

Koncové šifrování představuje klíčový nástroj pro zajištění ochrany soukromí a bezpečnosti uživatelů v digitálním prostředí. Tato metoda umožňuje uživatelům udržovat kontrolu nad

přístupem k jejich komunikaci a zajišťuje, že pouze zamýšlení příjemci mají možnost číst obsah zpráv. Využívání koncového šifrování poskytuje efektivní obranu proti různým formám kybernetických útoků, včetně phishingových útoků nebo úniků dat. Tato technologie rovněž uživatelům umožňuje komunikovat bez obav o sledování jejich zpráv ze strany vlády nebo dalších třetích stran, což posiluje svobodu projevu a podporuje demokracii. Využívání koncového šifrování tak tedy celkově poskytuje uživatelům vyšší úroveň kontroly, ochrany a bezpečnosti během digitální komunikace. (Koncové šifrování – co to je a proč jej používat?, 2023)

Hlavních důvodů pro využívání koncového šifrování je tedy hned několik. V první řadě je to ochrana soukromí uživatelů, která udržuje komunikaci v utajení. Tato funkce je zásadní pro osoby pracující s citlivými informacemi, jako jsou například novináři. Kromě toho koncové šifrování zvyšuje bezpečnost uživatelů tím, že chrání komunikaci před hackerskými útoky prostřednictvím nečitelnosti zpráv, mimo odesílatele a příjemce. Použití koncového šifrování zvyšuje důvěryhodnost služeb a aplikací, které tuto technologii implementují, protože uživatelé mají jistotu šifrování komunikace. V některých zemích platí zákony, které umožňují vládám získat přístup k elektronické komunikaci a vyžadují po poskytovatelích těchto služeb, aby jim přístup ke zprávám svých uživatelů dovolili. Koncové šifrování pak slouží jako nástroj k zajištění ochrany soukromí uživatelů před těmito zásahy. Dále je také většina aplikací využívajících koncové šifrování open-source. Znamená to, že mají otevřený zdrojový kód a ten je přístupný veřejnosti. Tato transparentnost tedy poskytuje odborníkům z celého světa možnost zkoumat a analyzovat bezpečnost aplikace a identifikovat případné nedostatky v programovém kódu. (Koncové šifrování – co to je a proč jej používat?, 2023)

Co se týče IM služeb, WhatsApp možnost koncového šifrování používá již od roku 2016. Společnost Meta, pod kterou spadá aplikace Messenger, začala zavádět end-to-end šifrování pro osobní zprávy a hovory až v roce 2023. I když zapnout koncové šifrování v Messengeru bylo možné již od roku 2016, týkalo se to jen tajných konverzací, na které měl uživatel možnost v chatu přepnout. (Meta zavádí end-to-end šifrování pro osobní zprávy a hovory na Messengeru a Facebooku, 2023)

4.3 Autentizace

Autentizace je proces ověření identity uživatele, systému nebo zařízení, který slouží k potvrzení, že osoba, počítačový systém nebo jiné zařízení je skutečně tím, za co se vydává. Autentizace zajišťuje bezpečnost digitálních systémů a dat tím, že zamezuje neoprávněnému

přístupu k danému účtu nebo komunikaci. Existují různé metody autentizace, včetně uživatelských jmen a hesel, biometrických prvků (otisky prstů nebo rozpoznání obličeje) a dvoufaktorová autentizace, kde je vyžadována kombinace dvou na sobě nezávislých prvků pro ověření. (Whitman, Mattord, 2014)

K ověřování pravosti se používají tři základní autentizační faktory. V prvním je uživatel ověřen na základě něčeho, co zná. Může jít o heslo nebo jiný autentizační kód, jako například PIN. Ve druhém podle něčeho, co uživatel má či vlastní. Do této kategorie patří čipová karta, mobilní zařízení pro generování jednorázových kódů či fyzický klíč. Třetí autentizace je založená na individuálních vlastnostech každého uživatele, tedy na biometrii, kam spadají otisky prstů, rozpoznání obličeje, hlasové rozpoznávání nebo skenování oční duhovky. (Whitman, Mattord, 2014)

V rámci IM služeb hraje autentizace zásadní roli pro zajištění bezpečnosti a ověření identit uživatelů. V současné době již většina chytrých mobilních telefonů podporuje biometrické prvky autentizace, jako je rozpoznání obličejů či čtečku otisků prstů k ověření identity uživatele. Pokud těmito faktory některá mobilní zařízení nedisponují, po uživateli požadují alespoň zadání PIN kódu pro vstup do zařízení. Po odemčení zařízení má tedy uživatel možnost vstupu do IM aplikací, které má ve svém mobilu nainstalované. Tady už pouze stačí otevřít aplikaci, která již nevyžaduje další přihlašování, protože většina uživatelů se po každém jednotlivém použití těchto platforem neodhlašuje. Jde tedy o poměrně bezpečnou technologii, protože biometrické prvky se nedají tak lehce odcizit.

Co se týče stolních počítačů nebo notebooků, tak v dnešní době již také některá zařízení disponují čtečkou otisků prstů. Dovolím si ale říci, že většina ještě spoléhá na zadávání uživatelského jména a hesla jak při přihlašování do svého počítačového účtu, tak při následném přihlašování do IM služeb skrze webový prohlížeč. Tady už je úroveň bezpečnosti nižší, jelikož došlo a dochází k úniku hesel uživatelů a jejich následným zneužitím v internetovém prostředí.

4.4 Autorizace

S autentizací se pojí termín autorizace. Je to následný krok, který řídí proces udělování oprávnění nebo povolení konkrétnímu subjektu (uživateli, systému nebo aplikaci) pro provádění určitých akcí nebo přístup k určitým informacím a funkcím. Poté, co je uživatel autentizován, autorizační systém rozhoduje, které akce může uživatel provádět. Toto rozhodnutí je založeno na předchozích definovaných oprávněních, rolích nebo pravidlech v

systému. Příklady autorizace zahrnují určení, kteří uživatelé mají přístup k určitým souborům, úrovně oprávnění pro různé role v organizaci nebo schválení konkrétních transakcí. (Whitman, Mattord, 2014)

4.5 Aktualizace

Aktualizace operačních systémů a aplikací pro okamžitou komunikaci jsou klíčové z hlediska zajištění bezpečnosti. Tyto aktualizace zahrnují opravy známých bezpečnostních chyb a zranitelností. Bez pravidelných aktualizací může zůstat systém nechráněný proti novým hrozbám, což zvyšuje riziko útoků a zneužití. Neaktualizovaný software může být cílem různých typů útoků a právě jeho aktualizace brání zneužívání těchto slabých míst a zvyšují odolnost systému proti útokům. Aktualizace také mohou obsahovat vylepšení soukromí a bezpečnosti dat, čímž mohou mít uživatelé větší kontrolu nad tím, jak jsou jejich osobní údaje zpracovávány a uchovávány. (Pět důvodů, proč aktualizovat software, 2019)

4.6 Firewall

Firewall je bezpečnostní zařízení nebo software, který slouží k ochraně počítačové sítě před nežádoucím a potenciálně škodlivým provozem. Jeho hlavním úkolem je filtrovat a řídit komunikaci mezi různými částmi sítě nebo mezi sítí a vnějším prostředím, jako je internet. Firewall chrání sítě před různými bezpečnostními hrozbami, tudíž zabraňuje neoprávněnému přístupu útočníků, monitoruje síťovou aktivitu a implementuje pravidla pro bezpečný datový přenos. Stejně tak může zabránit nechtěné odchozí komunikaci, což je důležité například v případě, kdy se počítač infikovaný škodlivým softwarem (malware) pokouší připojit k botnetové síti. Firewall je důležité pravidelně aktualizovat, aby byla zajištěna maximální úroveň ochrany. (Firewall, 2024)

4.7 Ochrana před phishingem

Phishing je kybernetický útok, při kterém se podvodník snaží vylákat z oběti citlivé informace prostřednictvím e-mailů nebo zpráv jako například hesla, údaje o platebních kartách, rodná čísla nebo čísla bankovních účtů. Útočník se často vydává za důvěryhodný zdroj, například banku, vládu nebo známou společnost a žádá oběť, aby mu poskytla své citlivé údaje. V minulosti byly phishingové zprávy často psány v angličtině, ale v dnešní době se běžně setkáváme se zprávami psané bezchybnou češtinou. (Phishing, 2024)

Aby se uživatelé nestali oběťmi tohoto podvodného jednání, je důležité znát typické znaky phishingu. Mezi ně patří hrozby a naléhavost, kdy se útočníci snaží zapůsobit na oběť například tvrzením, že účet bude zablokován a tím ji přimět rychle reagovat. Dále jsou to neshodné e-mailové domény. To znamená, že se falešné e-maily snaží vydávat za komunikaci od známých společností, jako je například banka, ale e-mailové domény v odeslané adrese se neshodují s oficiálními doménami těchto společností. (Ochrana před útoky phishing, 2024)

Dalším znakem phishingových pokusů mohou být až příliš výhodné nabídky nebo dobré zprávy. Jedná se o zprávy s informacemi o mnohamilionovém dědictví od vzdáleného příbuzného ze zahraničí nebo služby a zboží za nesmyslně výhodnou cenu. Podvodné zprávy mohou obsahovat i přílohy nebo odkazy, které by mohli odkazovat na falešné webové stránky. V tomto případě se doporučuje myší najet na odkaz, ale neklikat na něj, a zobrazí se nám skutečná adresa. (Phishing, 2024)

V roce 2023 zaznamenala nezisková organizace APWG (*Anti-Phishing Working Group*), specializující se na analýzu phishingových útoků, téměř 5 milionů incidentů. Tento výsledek představuje rekordně nejvyšší počet phishingových útoků. Koncem roku 2023 také došlo k výraznému nárůstu útoků zaměřených na sociální média, což představovalo 42,8 % všech phishingových útoků. (Phishing Activity Trends Reports, 2023)

Tyto skutečnosti ukazují, že phishing je rozšířenou a neustále se vyvíjející kybernetickou hrozbou. Obrat k česky psaným zprávám a zdokonalení techniky podvodníků ukazuje na neustálou snahu se přizpůsobit a oklamat uživatele. Identifikace klíčových znaků phishingu je nezbytná pro ochranu před tímto typem podvodů. Rekordní počet phishingových útoků za rok 2023 zdůrazňuje naléhavou potřebu informovanosti a opatrnosti při interakci s e-maily a zprávami. Rovněž stoupající podíl útoků zaměřených na sociální sítě signalizuje posun kybernetických hrozeb směrem k moderním komunikačním kanálům. Uživatelé by měli zůstat obezřetní a využívat bezpečnostních opatření k minimalizaci rizika podvodů a zneužití citlivých informací.

5 ZÁVĚREČNÁ KAPITOLA TEORETICKÉ ČÁSTI

Služby pro okamžité zasílání zpráv jsou důležitým prvkem současné digitální komunikace, které přinášejí mnoho výhod, ale současně s sebou nesou i určitá rizika v oblasti datové bezpečnosti. Je nezbytné, aby uživatelé byli obezřetní a přijímali opatření k ochraně svých dat a správně reagovali na kybernetické hrozby. Také je podstatné, aby se uživatelé zajímali o zabezpečení komunikačních aplikací, které využívají

V teoretické části byly definovány služby pro okamžité zasílání zpráv spolu s jejich výhodami a nevýhodami, abychom porozuměli jejich vlivu na současnou digitální komunikaci. Dále byl poskytnut přehled služeb této kategorie, skrze které lze komunikovat, a bylo představeno osm aplikací, kterým se tato práce věnuje, a to WhatsApp, WeChat, Facebook Messenger, Telegram, Instagram, Skype, Signal a Jami spolu s jejich charakteristikami a funkcemi.

Další část byla zaměřena na důležité koncepty datové bezpečnosti jako je kyberprostor, kybernetická rizika a hrozby, kterým jsou organizace i jednotlivci vystaveni, jako jsou phishing, malware a další. Byl vysvětlen pojem triáda CIA, který představuje základní principy zabezpečení dat a to konkrétně důvěrnost, integritu a dostupnost. Byl diskutován Traffic Light Protocol, který slouží k označování a sdílení citlivých informací s cílem zlepšit spolupráci mezi organizacemi a jednotlivci a současně chránit citlivá data před neoprávněným přístupem a zneužitím. Byla zmíněna role Národního úřadu pro kybernetickou a informační bezpečnost a legislativní opatření v oblasti kybernetické bezpečnosti, která mají za cíl posílit ochranu dat. Následně byly předestřeny technologie a opatření, která se využívají k zaručení ochrany citlivých informací v instant messaging komunikaci jako je symetrické a asymetrické šifrování, koncové šifrování, autentizace, autorizace či firewall.

II. PRAKTICKÁ ČÁST

6 PRINCIP FUNGOVÁNÍ JEDNOTLIVÝCH APLIKACÍ

Princip fungování chatovacích aplikací je základním kamenem jejich úspěchu a uživatelského přijetí. Obecně fungování chatovacích aplikací spočívá v poskytování uživatelům prostředků pro komunikaci v reálném čase pomocí textových, hlasových, video nebo multimediálních zpráv. Tato kapitola se zaměřuje na přehled a porozumění mechanismům, prostřednictvím kterých tyto aplikace umožňují uživatelům komunikaci a interakci. Jsou uvedeny klíčové služby, které tyto aplikace nabízí, údaj, které jsou požadovány pro registraci, dále také zda fungují jako sociální sítě či jaké mají zabezpečení.

6.1 WhatsApp

Aplikace WhatsApp poskytuje prostředek pro rychlou a bezpečnou komunikaci mezi uživateli a umožňuje posílat textové, hlasové a video zprávy jednotlivcům i skupinám. Uživatelům také umožňuje sdílet fotografie, videa a soubory s jejich kontakty.

Registrace: Uživatelé se zaregistrují pomocí svého telefonního čísla a následně se přihlásí do aplikace. WhatsApp používá ověření dvoufaktorovým kódem pro zvýšení bezpečnosti účtu. Aplikace synchronizuje kontakty ze zařízení uživatele a vytváří seznam přátel, kteří jsou také registrovaní na WhatsApp.

Platforma pro komunikaci: Uživatelé mohou komunikovat s těmito přáteli prostřednictvím textových zpráv, hlasových a videohovorů, sdílení multimediálních souborů a dalších funkcí.

Sociální síť: WhatsApp nefunguje jako sociální síť.

Bezpečnost: WhatsApp umožňuje uživatelům aktivovat dvoufaktorové ověření, což je další vrstva zabezpečení, která vyžaduje kromě telefonního čísla také heslo nebo PIN kód. WhatsApp dále používá end-to-end šifrování pro zabezpečení komunikace mezi uživateli. Nicméně byl v minulosti vystaven několika bezpečnostním incidentům, které odhalily zranitelnost aplikace. Po bezpečnostních incidentech WhatsApp pravidelně aktualizuje své zabezpečení a implementuje opatření k ochraně uživatelů, aby minimalizoval riziko útoků a zneužití.

Multiplatformita: WhatsApp je k dispozici pro širokou škálu zařízení, včetně chytrých telefonů s operačními systémy Android a iOS a také pro desktopové počítače prostřednictvím webového rozhraní a na operačních systémech Windows a macOS.

Další funkce: WhatsApp ukládá zprávy a multimediální soubory do cloudového úložiště, což umožňuje uživatelům přístup k nim z různých zařízení a zároveň zajišťuje zálohování dat. Také posílá uživateli notifikace o nových zprávách, i když není aktivní.

6.2 WeChat

Princip fungování WeChatu spočívá v poskytování komplexního digitálního ekosystému uživatelům, který zahrnuje komunikaci, sociální sítě, mobilní platby a další funkce. **Registrace:** Uživatelé se zaregistrují pomocí svého telefonního čísla a následně si ověří svůj účet. To zahrnuje přijetí ověřovacího kódu zaslaného prostřednictvím SMS.

Platforma pro komunikaci: WeChat umožňuje uživatelům posílat textové, hlasové a video zprávy jednotlivcům i skupinám. Podporuje multimediální zprávy, což uživatelům umožňuje sdílet fotografie, videa a soubory s jejich kontakty.

Sociální síť: Funguje také jako sociální síť, která umožňuje uživatelům propojit se s přáteli, rodinou a známými. Uživatelé mohou vytvářet osobní profily, sdílet aktualizace a fotografie na svém časovém pásu a interagovat s ostatními uživateli prostřednictvím lajků, komentářů a soukromých zpráv.

Bezpečnost: Aplikace WeChat je provozována čínskou společností. To znamená, že data uživatelů jsou uložena na serverech v Číně a podléhají čínským právním předpisům. Čínská vláda provádí přísnou internetovou cenzuru a monitorování online aktivity občanů a WeChat podléhá těmto opatřením. Komunikace prostřednictvím WeChatu tím pádem může být monitorována a filtrována čínskými úřady. Nicméně WeChat tvrdí, že poskytuje šifrovanou komunikaci, ale detaily o tom, jakým způsobem je šifrování implementováno a jaké bezpečnostní opatření jsou používána, nejsou veřejně známa. Uživatelé by proto měli mít na paměti, že jejich aktivity na platformě mohou být sledovány a že jejich soukromí nemusí být zaručeno.

Multiplatformita: WeChat k dispozici pro různé operační systémy, včetně Androidu, iOS, Windows a macOS a skrze webové rozhraní.

Další funkce: WeChat je integrován s WeChat Pay, službou mobilních plateb, která umožňuje uživatelům platit za zboží a služby přímo v aplikaci. Uživatelé mohou propojit své bankovní účty nebo platební karty s WeChat Pay a provádět platby skenováním QR kódů nebo převodem peněz na ostatní uživatele. Dále nabízí mini programy, což jsou aplikace, které fungují uvnitř ekosystému WeChatu, a které poskytují různé služby a funkce, jako jsou

hry, nakupování, rozvoz jídla, doprava a další, aniž by uživatelé museli stahovat samostatné aplikace. WeChat také poskytuje platformu pro podniky, organizace, celebrity a mediální agentury k vytváření oficiálních účtů. Tyto účty jim umožňují sdílet novinky, aktualizace, akce a další obsah se svými sledujícími.

WeChat se snaží být jedním centrálním místem pro komunikaci, sociální sítě a každodenní transakce. Tím, že integruje různé funkce a služby do jedné aplikace poskytuje uživatelům pohodlí a efektivitu ve svém každodenním životě.

6.3 Facebook Messenger

Princip fungování aplikace Facebook Messenger je navržen tak, aby uživatelům poskytoval snadný a přístupný způsob komunikace s jejich přáteli a rodinou prostřednictvím různých typů zpráv a multimediálního obsahu.

Registrace: Uživatelé se buď přihlásí pomocí svého existujícího účtu na Facebooku, nebo si vytvoří nový účet pomocí své e-mailové adresy nebo telefonního čísla.

Platforma pro komunikaci: Facebook Messenger umožňuje psát textové zprávy, sdílet média, jako jsou fotografie a videa, a také provádět hlasové nebo videohovory.

Sociální síť: I když je spojen s jednou z největších sociálních sítí na světě Facebookem, sám o sobě není plnohodnotnou sociální sítí.

Bezpečnost: Facebook Messenger používá end-to-end šifrování pro zabezpečení obsahu zpráv mezi odesílatelem a příjemcem. Uživatelé mohou nastavit různé bezpečnostní funkce, jako je dvoufaktorové ověřování, aby zvýšili ochranu svého účtu před neoprávněným přístupem. Facebook Messenger byl v minulosti vystaven bezpečnostním incidentům, kdy došlo k únikům dat uživatelů. Po těchto incidentech Facebook Messenger pravidelně aktualizuje svůj software a posiluje ochranná opatření.

Multiplatformita: Facebook Messenger je dostupný na mobilních zařízeních s operačními systémy iOS a Android, což zahrnuje chytré telefony a tablety. Kromě toho je Messenger dostupný i pro desktopové počítače prostřednictvím webového rozhraní a na operačních systémech Windows a macOS.

Další funkce: Nabízí řadu dalších funkcí, včetně možnosti vytvářet skupinové konverzace, sdílet polohu nebo funkci příběhů, kde uživatelé mohou sdílet dočasné příspěvky, které zmizí po 24 hodinách. Aplikace také posílá uživateli notifikace o nových zprávách, i když není aktivní. To umožňuje uživatelům rychle reagovat na nové zprávy.

6.4 Telegram

Telegram poskytuje uživatelům širokou škálu funkcí pro komunikaci a sdílení obsahu, zatímco klade důraz na bezpečnost, soukromí a uživatelskou kontrolu.

Registrace: Uživatelé si vytvoří účet pomocí svého telefonního čísla. Po přihlášení uživatelé vidí seznam svých kontaktů, kteří také používají Telegram. Mohou začít konverzaci s jednotlivými kontakty nebo vytvářet skupinové chaty s více lidmi.

Platforma pro komunikaci: Telegram umožňuje uživatelům posílat textové zprávy, multimediální soubory, hlasové zprávy, soubory a další obsah.

Sociální síť: Telegram je komunikační platforma, jako sociální síť nefunguje.

Bezpečnost: Telegram klade důraz na bezpečnou komunikaci. Kromě end-to-end šifrování nabízí možnost utajených chatů s automatickým mazáním zpráv a možností nastavit samozničení zpráv. Dále také možnost nastavení hesla nebo biometrického ověření pro přístup k aplikaci.

Multiplatformita: Uživatelé mohou používat Telegram na různých mobilních zařízeních a operačních systémech, včetně Androidu a iOS, Kromě toho je Telegram k dispozici i pro desktopové počítače prostřednictvím webového rozhraní a na operačních systémech Windows, macOS a Linux. Veškeré konverzace jsou synchronizovány mezi zařízeními.

Další funkce: Telegram umožňuje uživatelům vytvářet skupinové chaty s až tisíci členy. Tyto skupiny mohou být veřejné nebo soukromé a umožňují diskuzi na různá témata. Uživatelé mohou individuálně nastavit, jak budou dostávat notifikace pro každý chat nebo skupinu. Notifikace lze také vypnout, pokud uživatelé nechtějí být rušeni. Telegram ukládá veškerý obsah, včetně zpráv, médií a souborů, do cloudu, což umožňuje uživatelům přístup ke svým datům z různých zařízení a zajišťuje jejich zálohování a synchronizaci.

6.5 Instagram

Instagram představuje platformu pro sdílení fotografií a videí, která umožňuje uživatelům sdílet osobní profily, sdílet a prohlížet obsah ostatních uživatelů a komunikovat s nimi.

Registrace: Uživatelé si vytvářejí účet na Instagramu tím, že se registrují pomocí své e-mailové adresy nebo telefonního čísla.

Platforma pro komunikaci: Instagram umožňuje uživatelům sdílet fotografie a videa, posílat textové a hlasové zprávy, vytvářet skupinové konverzace a další obsah. Mohou přidávat hashtagy, popisky a označovat další uživatele.

Sociální síť: Instagram umožňuje uživatelům sledovat profily ostatních uživatelů a vidět jejich příspěvky ve svém feedu.

Bezpečnost: Instagram aktuálně neumožňuje automatické použití end-to-end šifrování pro veškerou komunikaci. Ačkoli tato platforma podporuje end-to-end šifrování, uživatelé musí ručně aktivovat tuto funkci a spustit chat s koncovým šifrováním. Tento postup však není standardní a není implementován pro všechny komunikační kanály. Důsledkem je nižší úroveň zabezpečení a důvěry v soukromí uživatelů této aplikace. Dále Instagram umožňuje uživatelům aktivovat dvoufaktorové ověřování, což znamená, že kromě běžného hesla musí poskytnout druhý ověřovací prvek. Tento druhý faktor může být jednorázový kód vygenerovaný mobilní aplikací nebo zaslaný prostřednictvím textové zprávy. Instagram má také mechanismy ochrany soukromí, které umožňují uživatelům nastavit, kdo může vidět jejich příspěvky a kdo je může kontaktovat.

Multiplatformita: Aplikace je k dispozici pro mobilní zařízení s operačními systémy iOS a Android a pro počítače s operačními systémy Windows, macOS a Linux. Uživatelé mohou také přistupovat k Instagramu pomocí webového prohlížeče na svých počítačích.

Další funkce: Uživatelé mohou sledovat ostatní uživatele a být sledováni zpět. Sledování umožňuje uživatelům vidět příspěvky svých přátel a dalších uživatelů ve svém zpravodajském kanálu. Funkce příběhů umožňuje uživatelům sdílet dočasné příspěvky, které zmizí po 24 hodinách. Instagram také poskytuje nástroje pro podnikání, které umožňují prodej produktů a služeb přímo na platformě.

6.6 Skype

Skype je komunikační platforma, která slouží k usnadnění komunikace mezi uživateli prostřednictvím různých funkcí. Tato platforma je často využívána ve firemním prostředí.

Registrace: Uživatelé se mohou registrovat pomocí e-mailové adresy nebo telefonního čísla a vytvořit si osobní účet a poté si přidat kontakty pomocí jejich uživatelských jmen, e-mailových adres nebo telefonních čísel.

Platforma pro komunikaci: Skype se zaměřuje na komunikaci a spolupráci mezi uživateli a týmy a umožňuje uživatelům provádět hlasové a videohovory s ostatními uživateli, posílat textové zprávy a soubory.

Sociální síť: Skype není sociální platformou.

Bezpečnost: Skype neposkytuje end-to-end šifrování pro své standardní konverzace, což je významná mezera v zabezpečení této platformy.

Multiplatformita: Skype je dostupný pro mobilní zařízení s operačními systémy iOS a Android, stejně jako pro počítače s operačními systémy Windows, macOS a Linux.

Další funkce: Skype nabízí další funkce jako sdílení obrazovky, přenos souborů, možnost volání na pevné linky a mobilní čísla, videokonference, nahrávání hovorů a přidávání kreditu pro volání na jiná než Skype čísla.

6.7 Signal

Princip fungování aplikace Signal spočívá v poskytování bezpečné a šifrované platformy pro komunikaci.

Registrace: Uživatelé se registrují pomocí telefonního čísla a vytvořit si účet. Signal nevyžaduje žádné osobní údaje a poskytuje uživatelům možnost zachování anonymity.

Platforma pro komunikaci: Signal umožňuje posílání textových zpráv, hlasových zpráv, fotografií, videí, souborů a videohovorů mezi uživateli.

Sociální síť: Signal je primárně platforma pro soukromou komunikaci mezi jednotlivými uživateli a skupinami. Není považován za sociální síť.

Bezpečnost: Je známý svou vysokou úrovní bezpečnosti a ochrany soukromí. Signal používá pro veškerou komunikaci end-to-end šifrování. Aplikace neprovádí sledování uživatelů ani shromažďování jejich osobních dat.

Multiplatformita: Signal je k dispozici pro mobilní zařízení s operačními systémy iOS a Android, stejně jako pro počítače s operačními systémy Windows, macOS a Linux.

Další funkce: Mezi další funkce patří možnost nastavení automatického mazání zpráv, vytvoření zabezpečených skupin s možností nastavení přístupových práv a zabezpečený přístup k aplikaci pomocí PIN kódu nebo biometrických údajů.

6.8 Jami

Jami slouží jako komplexní platforma pro komunikaci a sociální interakci a zároveň klade důraz na zabezpečení a ochranu soukromí uživatelů.

Registrace: Uživatelé se registrují v aplikaci Jami pomocí své e-mailové adresy nebo telefonního čísla.

Platforma pro komunikaci: Jami umožňuje uživatelům posílat textové zprávy, provádět hlasové a videohovory, sdílet soubory a provádět videohovory.

Sociální síť: Jami slouží jako platforma pro soukromou komunikaci mezi jednotlivými uživateli a skupinami.

Bezpečnost: Jami klade důraz na bezpečnost a ochranu soukromí uživatelů. Všechny komunikace jsou zabezpečeny end-to-end šifrováním.

Multiplatformita: Uživatelé mohou využívat Jami na mobilních zařízeních s operačními systémy iOS a Android, stejně jako na počítačích s operačními systémy Windows, macOS a Linux.

Další funkce: Mezi další funkce patří možnost volání na pevné linky a mobilní čísla, což vyžaduje kredit a sdílení obrazovky během hovoru.

7 ŠIFROVÁNÍ ZPRÁV V KOMUNIKAČNÍCH PLATFORMÁCH

Šifrování komunikace v instant messaging aplikacích je významným aspektem zajišťujícím bezpečnost a soukromí uživatelů při výměně zpráv. Tato technologie umožňuje zašifrovat obsah zpráv tak, aby nebyl čitelný pro neoprávněné osoby, které by se pokoušely zprávy odposlouchávat nebo číst. Díky šifrování se uživatelé mohou cítit jistěji, že jejich soukromé konverzace zůstanou mezi nimi a jejich komunikačními partnery, aniž by byly ohroženy vnějšími zásahy nebo útoky.

Šifrování v platformách pro okamžité odesílání zpráv funguje obvykle na principu asymetrického šifrování, kde každý uživatel má svůj unikání klíč pro šifrování a dešifrování zpráv. To znamená, že zprávy jsou zašifrovány pomocí klíče adresáta a pouze on sám, jako držitel tohoto klíče, je schopen tuto zprávu dešifrovat. Tento mechanismus zajišťuje, že pouze zamýšlený příjemce může číst zprávy a nikdo jiný, včetně provozovatelů služby nebo potencionálních útočníků, nemá přístup k obsahu konverzací.

Tato analýza se zaměřuje na to, zda a jaké aplikace nabízejí end-to-end šifrování ve svých komunikačních platformách. Zároveň zkoumá, od kterého roku jej zavedli a jestli je toto šifrování automaticky aktivní pro všechny konverzace ve výchozím nastavení, nebo či je nutné ručně ho zapnout.

V tabulce číslo 1 jsou uvedeny informace o implementaci end-to-end šifrování v chatovacích aplikacích WhatsApp, WeChat, Facebook Messenger a Telegram. Je důležité zdůraznit, že některé aplikace již toto šifrování poskytovaly od samého počátku své existence, což může zvýšit důvěru uživatelů v jejich bezpečnostní opatření. Naopak u jiných aplikací bylo end-to-end šifrování zavedeno až po určité době od vzniku aplikace. Tím se odráží vývoj v oblasti zabezpečení a odpověď na rostoucí poptávku po ochraně soukromí.

Tabulka 1: End-to-end šifrování v aplikacích 1 (vlastní zpracování)

	WhatsApp	**WeChat**	**Facebook Messenger**	**Telegram**
Rok vzniku:	2009	2011	2011	2013
End-to-end šifrování:	ANO	NE	ANO	ANO
Implementováno od roku:	2016	-	2016	2013
Dostupné ve výchozím nastavení pro všechny konverzace:	ANO	-	ANO	NE
Implementováno od roku:	2016	-	2023	-

V kontextu této analýzy je důležité poznamenat, že aplikace **WeChat,** pocházející z Čínské lidové republiky, nenabízí end-to-end šifrování, které by ochraňovalo obsah komunikace před jakýmkoli nepovolaným přístupem, včetně samotné platformy WeChat. Tato skutečnost může být vnímána jako riziko z hlediska ochrany soukromí uživatelů, zejména vzhledem k povaze regulace a dohledu ze strany čínských úřadů. Absenci šifrování lze interpretovat jako zásah do soukromí uživatelů, protože veškerá komunikace prostřednictvím aplikace může být přístupná čínským autoritám.

Bez end-to-end šifrování je veškerá komunikace na WeChatu vystavena riziku odposlechu a sledování, což je značným zabezpečovacím problémem pro uživatele, kteří chtějí chránit svou soukromí a citlivé informace. Fakt, že WeChat podléhá čínským právním předpisům a regulacím, dále zvyšuje obavy ohledně bezpečnosti dat, která jsou prostřednictvím této aplikace sdílena. Pokud jde o citlivé komunikace a informace, uživatelé by měli zvážit použití alternativních platforem, které poskytují robustnější bezpečnostní opatření a ochranu soukromí.

Nejpoužívanější aplikace **WhatsApp** platí za z předního hráče v oblasti instantních zpráv, zejména díky své široké dostupnosti, jednoduchému použití a vysoké míře zabezpečení soukromí. Klíčovým prvkem, který přispívá k důvěryhodnosti WhatsAppu, je jeho implementace end-to-end šifrování, které proběhlo v roce 2016. To znamená, že ani

WhatsApp jako platforma, ani jiné třetí strany nejsou schopny přečíst nebo sledovat obsah zpráv.

WhatsApp rovněž zdůrazňuje svůj závazek k ochraně osobních údajů svých uživatelů. Ačkoli aplikace sbírá určité informace o uživatelích, jako jsou telefonní čísla a metadata spojená s komunikací, tvrdí, že tyto údaje jsou chráněny proti neoprávněnému přístupu a nejsou sdíleny s třetími stranami pro marketingové účely. Tím se snaží zajistit, že uživatelé mají kontrolu nad svými daty a mohou se cítit bezpečně při používání aplikace.

End-to-end šifrování v WhatsAppu není pouze volitelnou funkcí, ale je aktivní pro všechny konverzace ve výchozím nastavení, což znamená, že uživatelé nemusí nic speciálně nastavovat, aby si mohli užívat vyšší úrovně zabezpečení svých komunikací. Tato implicitní ochrana soukromí přispívá k široké adopci aplikace mezi uživateli, kteří hledají spolehlivý a zabezpečený nástroj pro komunikaci.

Nicméně není třeba opomíjet možné výzvy spojené s ochranou soukromí v WhatsAppu. Ačkoli samotná komunikace je šifrovaná, aplikace může stále shromažďovat metadata o uživatelském chování, která mohou být využita k analytickým účelům nebo pro cílený marketing. Tyto otázky by měly být brány v úvahu při posuzování celkové úrovně důvěryhodnosti a soukromí v aplikaci.

Třetí nejoblíbenější chatovací aplikace co do počtu uživatelů **Facebook Messenger** (označovaný zkráceně jako Messenger), kterou používá téměř 1 miliarda uživatelů, zavedl funkci end-to-end šifrování v roce 2016. Netýkalo se to však všech konverzací ve výchozím nastavení a tato funkce byla k dispozici pouze v tajných konverzacích, které uživatelé museli aktivně zapnout.

Od roku 2023 implementoval Facebok Messenger end-to-end šifrování do všech konverzací, což znamená, že tato úroveň zabezpečení je nyní poskytována implicitně pro všechny uživatele. Tímto krokem Facebook reagoval na zvyšující se důraz na ochranu soukromí a zvýšené očekávání uživatelů ohledně bezpečnosti jejich komunikace.

Také aplikace **Telegram** se stala využívanou platformou pro komunikaci díky svým rozmanitým funkcím a snaze o zachování soukromí uživatelů. End-to-end šifrování bylo implementováno do aplikace Telegram již v roce 2013 a to v podobě funkce s názvem tajný chat. Nicméně, je důležité poznamenat, že end-to-end šifrování není aktivní ve všech typech konverzací v Telegramu. Standardní konverzace mimo tajné chaty nejsou šifrovány end-to-end, což znamená, že obsah těchto konverzací může být přístupný Telegramu a jeho

serverům. Tato nešifrovaná komunikace může být považována za zranitelnou vůči kybernetickým útokům a sledování třetími stranami.

Důvodem, proč end-to-end šifrování není standardně aktivní pro všechny konverzace v Telegramu, může být snaha o zachování rychlosti a efektivity platformy. Šifrování všech konverzací by mohlo zpomalit komunikaci a zatížit serverové zdroje Telegramu. Tím, že umožňuje uživatelům aktivovat end-to-end šifrování pouze pro vybrané konverzace, Telegram nabízí vyvážený přístup mezi zabezpečeností a uživatelskou pohodlí.

V tabulce číslo 2 jsou uvedeny informace o implementaci end-to-end šifrování v chatovacích aplikacích Instagram, Skype, Signal a Jami.

Tabulka 2: End-to-end šifrování v aplikacích 2 (vlastní zpracování)

	Instagram	**Skype**	**Signal**	**Jami**
Rok vzniku:	2010	2003	2014	2016
End-to-end šifrování:	ANO	ANO	ANO	ANO
Implementováno od roku:	2016	2018	2014	2016
Dostupné ve výchozím nastavení pro všechny konverzace:	NE	NE	ANO	ANO
Implementováno od roku:	-	-	2014	2016

Instagram se zaměřuje na sdílení fotografií a videí mezi uživateli. Avšak pokud jde o zabezpečení a šifrování, Instagram se soustředí především na ochranu účtů a obsahu před neoprávněným přístupem, a nikoli na end-to-end šifrování pro veškerou komunikaci mezi uživateli. Přestože tato platforma podporuje end-to-end šifrování od roku 2016, uživatelé musí tuto funkci ručně aktivovat a spustit chat s koncovým šifrováním.

Zprávy v aplikaci tak mohou být přístupné Instagramu a jeho serverům. Toto rozhodnutí může být způsobeno snahou zachovat přístupnost a pohodlí platformy pro uživatele a zároveň umožnit Instagramu monitorovat obsah pro dodržení svých podmínek služeb a ochranu proti spamu a zneužití.

Instagram se patrně rozhodl neimplementovat end-to-end šifrování pro veškerou komunikaci kvůli zdůraznění veřejného charakteru své platformy. Instagram je primárně sociální síť určená k sdílení obsahu s ostatními uživateli a budování veřejného profilu. Proto může mít snaha o zachování otevřenosti a transparentnosti přednost před implementací end-to-end šifrování, které by mohlo omezit schopnost Instagramu monitorovat a moderovat obsah.

I přes absenci end-to-end šifrování pro veškerou komunikaci nabízí Instagram uživatelům některá bezpečnostní opatření, jako je možnost nastavení soukromí účtu, filtrování nežádoucích zpráv a blokování nebo hlášení uživatelů. Tyto funkce slouží k ochraně soukromí a bezpečnosti uživatelů, i když nedosahují úrovně zabezpečení poskytované end-to-end šifrováním.

Další platforma **Skype** je jednou z nejznámějších aplikací pro komunikaci a videokonference, která je široce používána pro osobní i firemní účely. Co se týče zabezpečení, Skype poskytuje určité bezpečnostní prvky, ale end-to-end šifrování, které je považováno za zlatý standard v zabezpečené komunikaci, není v této aplikaci standardní.

End-to-end šifrování je sice ve Skype implementováno od roku 2018 ale není ve výchozím nastavení a platí pouze pro určité typy komunikace. Zpravidla je šifrování aktivováno pouze pro hlasové a videohovory, zatímco textové zprávy nejsou šifrovány end-to-end. To znamená, že obsah textových zpráv může být přečten nebo zachycen třetími stranami, včetně provozovatele Skype, Microsoftu.

Důvod, proč Skype neimplementuje end-to-end šifrování pro všechny své chaty, může být spojen s jeho integrací do ekosystému Microsoftu a snahou o kompatibilitu a pohodlí uživatelů. Šifrování v reálném čase může představovat technické výzvy v oblasti synchronizace zpráv mezi různými zařízeními a platformami.

Absence end-to-end šifrování pro textové zprávy ve Skype může být pro některé uživatele důvodem k obavám ohledně ochrany soukromí a bezpečnosti jejich komunikace. Zejména pro uživatele, kteří požadují vyšší úroveň zabezpečení pro svou komunikaci, může tento nedostatek šifrování znamenat hledání alternativních platforem, které nabízejí end-to-end šifrování pro všechny typy komunikace.

Signal je naopak známý pro svou zabezpečenou a soukromou komunikaci, která se zaměřuje na ochranu uživatelského soukromí a bezpečnost. Implementace end-to-end šifrování v Signalu je zásadním prvkem jeho bezpečnostní architektury a je jeho součástí od roku 2014.

Signal používá end-to-end šifrování pro veškerou komunikaci mezi uživateli, ať už jde o textové zprávy, hlasové hovory, videokonference nebo sdílení souborů. Toto šifrování je standardně zapnuto pro všechny konverzace a není možné jej vypnout, což zajišťuje konzistentní úroveň bezpečnosti pro všechny uživatele.

Důvodem, proč Signal implementoval end-to-end šifrování pro všechny své chaty, je poskytnutí maximálního zabezpečení a soukromí pro uživatele. Tato volba reflektuje prioritní zaměření Signalu na ochranu uživatelských dat a soukromí, což je klíčovým faktorem pro mnoho uživatelů, kteří vyhledávají zabezpečenou komunikační platformu.

Poslední chatovací aplikací je **Jami**, což je open-source platforma pro komunikaci, která se zaměřuje na zabezpečení a soukromí uživatelů. Jami implementuje funkci end-to-end šifrování pro všechny své konverzace a to od roku 2016. Díky tomu mohou uživatelé Jami komunikovat bez obav o možné odposlouchávání či únik jejich soukromých informací. Tato funkce je klíčovým faktorem, který láká uživatele, kteří kladou důraz na ochranu svého soukromí a bezpečnost své komunikace.

Výhodou implementace end-to-end šifrování je také to, že uživatelé nemusejí řešit složitý proces nastavení šifrování nebo se starat o bezpečnost své komunikace. Šifrování je aktivní ve výchozím nastavení a funguje automaticky pro všechny konverzace. To zjednodušuje uživatelskou zkušenost a zajišťuje, že všechny komunikace jsou zabezpečeny bez nutnosti dalších kroků ze strany uživatele.

V analýze end-to-end šifrování ve vybraných komunikačních aplikací lze identifikovat různé přístupy k zabezpečení dat a koncového šifrování. WhatsApp, Facebook Messenger a Signal, Jami implementovali end-to-end šifrování ve výchozím nastavení pro všechny konverzace, což zajišťuje vysokou úroveň ochrany dat v průběhu jejich přenosu. Naopak u aplikací jako Telegram a Instagram musí uživatelé manuálně aktivovat koncové šifrování a to může vést k nedostatečné ochraně soukromí, zejména pokud tato možnost není využita. Skype poskytuje volitelné šifrování. Znamená to tedy, že uživatelé mají možnost aktivovat tuto funkci, ale není to standardní nastavení. WeChat naopak koncové šifrování neposkytuje, a tím se jeví jako nedůvěryhodná aplikace.

Celkově lze konstatovat, že aplikace jako WhatsApp Facebook Messenger, Signal, a Jami se jeví jako bezpečné volby pro uživatele, kteří kladou důraz na ochranu svých dat a soukromí. Avšak s WhatsAppem a Facebook Messengerem byly v minulosti spojovány bezpečnostní incidenty a úniky osobních dat uživatelů. Z tohoto důvodu se tedy mohou jevit

jaké méně důvěryhodné. Na druhou stranu, aplikace jako Telegram, Instagram, Skype vyžadují větší obezřetnost a možná i dodatečná opatření k zajištění úrovně bezpečnosti, která by odpovídala současným standardům ochrany dat.

Je také důležité se zamyslet nad tím, co přiměje běžné uživatele zajímat se o koncové či jiné šifrování v chatovacích aplikacích. Pokud se lidé chtějí podělit o velmi citlivé informace, měli by zvážit, zda je vhodné je vůbec sdílet prostřednictvím těchto aplikací, i když jsou zabezpečeny koncovým šifrováním. Je důležité si uvědomit, že bezpečnostní opatření nemohou zaručit, že citlivé informace zůstanou utajeny, pokud jsou sdíleny s nespolupracujícími nebo nedůvěryhodnými lidmi. Místo toho by měli lidé zvážit, za jsou tyto informace vhodné ke sdílení prostřednictvím takových kanálů a měli by hledat alternativní způsoby komunikace, které by jim poskytly vyšší míru bezpečnosti a ochrany soukromí.

8 ANALÝZA VLASTNOSTÍ CHATOVACÍCH APLIKACÍ

Následující kapitola je zaměřena na důležité faktory spojené s chatovacími aplikacemi, které mají zásadní vliv na uživatelskou zkušenost a bezpečnost. Zabývá se několika klíčovými aspekty, které zahrnují zemi původu aplikace, majitele, dostupnost zdrojového kódu, požadavky na osobní údaje, přítomnost reklam a finanční model aplikace. Tato analýza umožní lépe porozumět kontextu jednotlivých aplikací, osvětlit jejich funkce a politikách týkajících se soukromí a bezpečnosti a poskytne informace potřebné k rozhodování o vhodnosti používání daných aplikací.

V tabulce číslo 3 jsou uvedeny klíčové informace, týkající se aplikace WhatsApp. Zahrnují důležité údaje o vlastnostech a dalších charakteristikách této komunikační platformy.

Tabulka 3: WhatsApp (vlastní zpracování)

WhatsApp	
Země původu:	USA
Majitel:	Meta Platforms, Inc.
Osobní údaje, které vyžadují:	Telefonní číslo
Open-source:	NE
Reklamy:	ANO
Financování prostřednictvím:	Placená reklama

WhatsApp je aplikace, která je financována společností Facebook, která ji akvizovala v roce 2014. Tato akvizice přinesla změny v tom, jak se aplikace integruje s ekosystémem Facebooku a jeho reklamní platformou. WhatsApp není open-source aplikace, což znamená, že kód aplikace není veřejně dostupný a nemůže být volně auditován nezávislými vývojáři a bezpečnostními experti. Tato skutečnost vyvolává otázky ohledně transparentnosti a důvěryhodnosti aplikace, protože uživatelé nemají přístup k celému kódu a nemohou tak ověřit, jak jsou jejich údaje zpracovávány a chráněny.

Jedním z hlavních bezpečnostních rizik WhatsAppu je skutečnost, že aplikace sbírá a uchovává určité osobní údaje uživatelů, jako jsou telefonní čísla, kontakty, metadata o

komunikaci a další. Navíc, od akvizice Facebookem, WhatsApp začal sdílet určité údaje s mateřskou společností, což vyvolalo obavy o ochranu soukromí a bezpečnost uživatelů.

WhatsApp byl tradičně bez reklam, avšak od roku 2019 začal WhatsApp zkoušet různé modely monetizace, včetně zavedení placených funkcí pro podniky a reklamních zpráv v rámci aplikace WhatsApp Business. Tento krok vyvolal obavy ohledně ochrany soukromí uživatelů a jejich osobních dat. WhatsApp je nyní financován prostřednictvím různých modelů, včetně přímých investic od společnosti Facebook, placených funkcí pro podniky a potenciálně i reklamních příjmů. Tento finanční model umožňuje WhatsAppu poskytovat bezplatnou službu pro uživatele, zatímco současně generuje příjmy pro své vlastníky.

Nicméně, v roce 2021 získala nezisková organizace ProPublica, která je zaměřená na investigativní žurnalistiku, interní dokumenty WhatsAppu, podle kterých se Facebook rozhodl sdílet některé citlivé informace, jako jsou telefonní čísla uživatelů s reklamními partnery. Facebook tvrdil, že sdílení mezi ním a WhatsAppem je anonymní a je chráněno šifrováním, avšak existují obavy ohledně skutečného rozsahu sdílení dat a způsobu, jakým jsou tyto informace využívány k cílení reklam a sledování uživatelské aktivity. (Elkind, Gillum, Silverman, 2021)

Analyzujeme-li tyto informace, lze vidět, že WhatsApp se i přes svou popularitu a široké uživatelské základny potýká s různými otázkami týkajícími se transparentnosti ohledně zpracování dat, ochrany soukromí, financování a bezpečnostních rizik spojených s aplikací, což vyžaduje neustálé sledování a kritickou analýzu ze strany uživatelů a odborníků na bezpečnost a ochranu soukromí.

Tabulka číslo 4 poskytuje přehled důležitých údajů o aplikaci WeChat.

Tabulka 4: WeChat (vlastní zpracování)

WeChat	
Země původu:	Čína
Majitel:	Tencent
Osobní údaje, které vyžadují:	Telefonní číslo
Open-source:	NE
Reklamy:	ANO
Financování prostřednictvím:	Tencent / Placená reklama

WeChat je těsně propojen s čínským internetovým ekosystémem a funguje jako klíčový hráč v digitálním životě mnoha lidí v Číně a v asijském regionu obecně. Patří společnosti Tencent, která generuje příjmy z reklamy, placených služeb, mikrotransakcí a dalších zdrojů.

WeChat není open-source aplikace a bezpečnostní rizika s ním spojená jsou zvláště významná kvůli jeho původu z Číny a skutečnosti, že čínské zákony a regulace mohou vyžadovat, aby společnosti jako Tencent poskytovaly přístup k uživatelským datům čínským úřadům. To může vyvolat obavy o ochranu soukromí a bezpečnost uživatelů i mimo Čínu.

V roce 2023 Národní úřad pro kybernetickou bezpečnost varoval před používáním aplikace WeChat. Hlavními důvody byly obavy z rozsáhlého sběru uživatelských dat, nedostatečného zabezpečení a možného vlivu čínských bezpečnostních složek na společnost Tencent, se kterou je WeChat spojen. Ačkoliv počet aktivních uživatelů WeChatu v České republice v porovnání s jinými podobnými platformami je výrazně nižší, mohou mezi nimi být i exponované osoby, jako jsou diplomaté nebo obchodníci, což zvyšuje riziko zneužití dat. (NÚKIB upozorňuje na hrozbu spojenou s aplikací WeChat společnosti Tencent, 2023)

NÚKIB upozornil, že WeChat disponuje schopností stažení a instalace kódu bez vědomí uživatele, což lze zneužít k instalaci malware do zařízení. Dalším problémem je také absence funkce end-to-end šifrování, což může umožnit cenzuru a sledování soukromé komunikace. Doporučení od NÚKIB pro uživatele, kteří potřebují WeChat používat, tedy bylo mít aplikaci nainstalovanou na separátním zařízením a povolovat pouze nezbytně nutná

oprávnění. (NÚKIB upozorňuje na hrozbu spojenou s aplikací WeChat společnosti Tencent, 2023)

Z pohledu kybernetické bezpečnosti vydaná upozornění od NÚKIB reflektují rostoucí obavy ze zneužití osobních dat a možného vlivu státu na soukromé společnosti. Tyto obavy jsou podpořeny geopolitickými souvislostmi, které naznačují úzké propojení společnosti Tencent s čínským státem a jeho bezpečnostními složkami. Ve spojení s nedostatečným zabezpečením aplikace a její schopností shromažďovat velké množství uživatelských dat toto varování zdůrazňuje potřebu obezřetnosti při používání WeChatu.

S ohledem na zájmy soukromí a bezpečnosti by měli uživatelé hledat alternativy k WeChatu, které jsou provozovány mimo Čínu a které nabízejí vyšší úroveň soukromí a ochrany dat. Existuje mnoho dalších chatovacích aplikací, které prioritizují bezpečnost a soukromí uživatelů a které mohou být vhodnější pro ty, kteří mají obavy ohledně cenzury a monitorování jejich online aktivity.

V tabulce číslo 5 jsou uvedeny klíčové údaje, týkající se aplikace Facebook Messenger.

Tabulka 5: Facebook Messenger (vlastní zpracování)

Facebook Messenger	
Země původu:	USA
Majitel:	Meta Platforms, Inc.
Osobní údaje, které vyžadují:	Jméno, telefonní číslo / e-mail
Open-source:	NE
Reklamy:	ANO
Financování prostřednictvím:	Placená reklama

Aplikace Facebook Messenger je součástí širšího ekosystému služeb Meta Platforms a je pevně propojen s ostatními produkty a službami této společnosti, jako je sociální síť Facebook a Instagram. Uživatelé mohou používat stejný účet pro přihlášení do všech těchto platforem a mohou sdílet obsah a komunikovat přes různé aplikace v rámci ekosystému Meta.

Facebook Messenger vyžaduje různé osobní údaje od svých uživatelů. Mezi tyto údaje patří identifikační informace, jako je jméno, které uživatelé poskytují při vytváření účtu. Dále

aplikace žádá o kontaktní údaje, jako jsou telefonní číslo a e-mailová adresa. Komunikační data jsou také sbírána, což zahrnuje obsah zpráv, fotografie, videa a další multimediální obsah, který uživatelé sdílejí prostřednictvím aplikace. Kromě toho Messenger získává metadatové údaje, jako jsou časy odeslání zpráv, frekvence interakcí a další metadata, která umožňují analýzu uživatelského chování a personalizaci obsahu a reklam. Polohové údaje jsou také vyžadovány, pokud uživatel povolí polohové služby, což umožňuje aplikaci získávat informace o aktuální poloze uživatele pro účely zobrazení umístění, navigace a personalizovaných obsahů nebo reklam.

Facebook Messenger není open-source aplikace. Tato uzavřenost a nedostatek transparentnosti ohledně fungování aplikace může vyvolávat obavy u některých uživatelů ohledně ochrany soukromí a bezpečnosti jejich dat.

Financování Facebook Messengeru pochází z různých zdrojů, včetně reklamních příjmů, placených funkcí pro podniky a dalších komerčních iniciativ. Facebook Messenger je tedy financován převážně reklamními příjmy, které Meta Platforms generuje z celého svého ekosystému produktů a služeb. Navíc existuje obava ohledně ochrany soukromí uživatelů vzhledem k historii incidentů souvisejících s Facebookem, včetně skandálu s Cambridge Analytica.

Tabulka číslo 6 poskytuje klíčové informace, týkající se aplikace Telegram.

Tabulka 6: Telegram (vlastní zpracování)

Telegram	
Země původu:	Rusko
Majitel:	Telegram FZ-LLC
Osobní údaje, které vyžadují:	Telefonní číslo
Open-source:	ANO
Reklamy:	NE
Financování prostřednictvím:	Soukromé investice

Telegram byl vyvinut ruským občanem Pavlem Durovem, ale společnost nyní sídlí v Dubaji. Po svých uživatelích požaduje poskytnutí telefonního čísla, které slouží jako identifikátor

účtu v Telegramu. Telefonní číslo je klíčové pro propojení uživatele s jeho účtem a umožňuje mu přistupovat ke svým konverzacím a kontaktům.

Aplikace není open-source a financování Telegramu je částečně založeno na osobních prostředcích Pavla Durova a je známý svým soukromým a decentralizovaným financováním, což může být problematické z hlediska transparentnosti financí.

Bezpečnostní rizika spojená s Telegramem zahrnují obavy ohledně soukromí uživatelů a ochrany dat. Ačkoli Telegram nabízí end-to-end šifrování pro soukromé konverzace, je kritizován za nedostatečnou transparentnost vůči prováděným bezpečnostním auditům. Dříve byl Telegram kritizován za svůj přístup k ochraně soukromí, zejména kvůli způsobu, jakým uchovával metadata o uživatelích a otevřeným kanálům, které mohou být využity k monitorování komunikace. Navíc, kvůli svému soukromému financování může být Telegram vnímán jako potenciálně méně transparentní a méně zodpovědný v porovnání s jinými aplikacemi, které jsou financovány tradičnějšími způsoby. To může vyvolávat obavy ohledně možných rizik spojených s úmyslným nebo neúmyslným porušením soukromí uživatelů a ochrany jejich dat.

V tabulce číslo 7 jsou uvedeny klíčové údaje, týkající se aplikace Instagram.

Tabulka 7: Instagram (vlastní zpracování)

Instagram	
Země původu:	USA
Majitel:	Meta Platforms, Inc.
Osobní údaje, které vyžadují:	Telefonní číslo / e-mail, datum narození
Open-source:	NE
Reklamy:	ANO
Financování prostřednictvím:	Placená reklama

Další součástí ekosystému služeb Meta Platforms je Instagram. Co se týče osobních údajů, Instagram vyžaduje při registraci uživatelské jméno, e-mailovou adresu, telefonní číslo a datum narození. Kromě toho může aplikace získávat další osobní údaje, jako jsou informace o uživatelově aktivitě na platformě, sledované profily, interakce s příspěvky a další.

Instagram není open-source platforma a uživatelé tak nemají možnost zkontrolovat, jakým způsobem je aplikace navržena nebo jak jsou v ní implementována bezpečnostní opatření.

Financování Instagramu je spojeno s jeho mateřskou společností Facebook, který generuje většinu svých příjmů z reklamních kampaní na svých platformách. Instagram také nabízí placenou reklamu a některé funkce, jako je například Instagram Shopping, která umožňuje uživatelům nakupovat přímo z aplikace.

Pokud jde o bezpečnostní rizika a hrozby, Instagram čelí několika obavám uživatelů, jako je například nedostatečná ochrana osobních údajů, případy kyberšikany a manipulace s obsahem. Existuje také obava z toho, že Instagram může být zneužíván k šíření dezinformací a nevhodného obsahu.

Pro některé uživatele může být důvodem k obavám i skutečnost, že Instagram vlastní Facebook, což znamená, že údaje a informace sdílené na Instagramu mohou být použity pro cílení reklam a personalizovaný obsah na dalších platformách vlastněných Facebookem. Tato propojenost také způsobuje obavy ohledně soukromí a ochrany osobních údajů, zejména vzhledem k historii Facebooku v oblasti ochrany dat uživatelů.

V tabulce číslo 8 jsou uvedeny klíčové informace o aplikaci Skype.

Tabulka 8: Skype (vlastní zpracování)

Skype	
Země původu:	Estonsko
Majitel:	Microsoft Corporation
Osobní údaje, které vyžadují:	Telefonní číslo / e-mail
Open-source:	NE
Reklamy:	ANO
Financování prostřednictvím:	Placené služby

Aplikace Skype byl založena v Estonsku, ale po akvizici je součástí společnosti Microsoft Corporation. Skype vyžaduje při registraci uživatelské jméno, e-mailovou adresu a heslo. Kromě toho může aplikace získávat další informace o uživatelích, jako jsou kontaktní seznamy, historie hovorů a zpráv, IP adresy a další.

Skype není open-source aplikace. Reklamy nejsou běžně zobrazovány přímo v aplikaci Skype, ale některé placené verze mohou obsahovat reklamní prvky. Financování Skype je spojeno s jeho mateřskou společností Microsoft. Microsoft generuje příjmy z různých zdrojů, včetně prodeje softwaru a služeb, cloudového úložiště, placených verzí Skype a dalších produktů.

Skype čelí obavám týkajícím se ochrany soukromí a bezpečnosti dat. Existují případy, kdy došlo k únikům dat nebo zneužití služby k šíření malware. Někteří uživatelé se obávají i možného odposlouchávání jejich hovorů a nedostatečné ochrany proti kybernetickým útokům. Navíc propojení s ekosystémem Microsoftu může vyvolávat obavy z možného sledování uživatelských aktivit a sdílení dat mezi různými službami.

V tabulce číslo 9 jsou uvedeny klíčové údaje, týkající se aplikace Signal.

Tabulka 9: Signal (vlastní zpracování)

Signal	
Země původu:	USA
Majitel:	Signal Foundation
Osobní údaje, které vyžadují:	Telefonní číslo
Open-source:	ANO
Reklamy:	NE
Financování prostřednictvím:	Dary od nadací a soukromých osob

Signal byl založen v USA a je známý svým důrazem na bezpečnost a ochranu soukromí uživatelů. Jeho majitelem je nezisková organizace Signal Foundation, kterou založil Brian Acton, spoluzakladatel WhatsAppu. Signal sbírá a uchovává minimum uživatelských dat a aplikace vyžaduje pro registraci pouze telefonní číslo.

Aplikace je open-source, její zdrojový kód je veřejně dostupný a může být prozkoumán a ověřen komunitou vývojářů a bezpečnostními experty. Signal neobsahuje reklamy a je financován prostřednictvím darů a grantů od různých nadací, včetně Signal Foundation.

Signal je považován za jednu z nejbezpečnějších komunikačních platforem díky svému silnému šifrování a důrazu na soukromí. Nicméně, jako každá aplikace, i Signal může čelit

hrozbám, jako jsou kybernetické útoky, phishing nebo zneužití softwaru. Někteří uživatelé však mohou mít obavy z možného sledování jejich aktivit ze strany vládních organizací nebo třetích stran.

NÚKIB v roce 2022 vydal doporučení pro používání aplikace Signal, ze kterého vyplývá, že Signal je vyzdvihován pro svůj důraz na bezpečnost a end-to-end šifrování ve všech typech komunikace a to poskytuje uživatelům zabezpečené prostředí. Na druhou stranu také přiznává, že i když aplikace jako Signal nabízí vysokou úroveň bezpečnosti díky koncovému šifrování, stále existují výzvy spojené s ochranou osobních údajů a soukromí uživatelů. Nedostatky v šifrování a provázanost s problematickými společnostmi mohou ohrozit bezpečnost a soukromí uživatelů a také jejich důvěru ve zmíněné aplikace. Důležité je proto vybírat komunikační platformy s ohledem na jejich bezpečnostní funkce a prověřené postupy ochrany dat. (Doporučení pro používání aplikace Signal, 2022)

Toto doporučení poukazuje na to, že důrazná bezpečnostní opatření nejsou vždy dostatečná k zajištění úplné ochrany dat také, že by uživatelé měli být ostražití při volbě komunikačních platforem a pečlivě zvážit jejich bezpečnostní aspekty i přesto, že je Signal ceněn pro svou důraznou bezpečnostní politiku.

V tabulce číslo 10 jsou uvedeny klíčové informace o platformě Jami.

Tabulka 10: Jami (vlastní zpracování)

Jami	
Země původu:	Kanada
Majitel:	Savoir-faire Linux Inc.
Osobní údaje, které vyžadují:	Telefonní číslo
Open-source:	ANO
Reklamy:	NE
Financování prostřednictvím:	Placené služby

Jami je platforma pro peer-to-peer komunikaci vyvíjená a udržovaná projektem GNU. Je navržena tak, aby poskytovala bezpečné a decentralizované služby pro zasílání zpráv, hlasové a videohovory.

Jami je koncipován s důrazem na ochranu soukromí a bezpečnost. Pro vytvoření účtu a používání služeb je nutné zadat telefonní číslo. Uživatelé mohou komunikovat přímo mezi sebou bez spoléhání na centralizované servery, což minimalizuje sběr osobních dat. Jelikož Jami je open-source platforma, kód aplikace je veřejně dostupný a podléhá pravidelným auditům a kontrolám komunity. Tato transparentnost přispívá k důvěře uživatelů v bezpečnost a spolehlivost aplikace.

V aplikaci Jami nejsou zobrazovány reklamy. Její decentralizovaná povaha znamená, že neexistuje žádná centralizovaná entita, která by se snažila monetizovat uživatelská data nebo zobrazovat cílené reklamy. Jami je financován různými způsoby, včetně darů, grantů a příspěvků od projektu GNU a dalších podpůrných organizací. Jako projekt svobodného softwaru spoléhá na podporu komunity a dobrovolných příspěvků k jeho dalšímu vývoji a údržbě.

Přestože Jami zdůrazňuje bezpečnost a soukromí, jako každý software může být stále zranitelný vůči bezpečnostním rizikům. Mezi tyto rizika mohou patřit softwarové chyby, zranitelnosti nebo útoky cílené na infrastrukturu. Nicméně, díky tomu, že je open-source, mohou bezpečnostní experti identifikovat a adresovat jakékoli bezpečnostní problémy promptně. Někteří uživatelé se mohou obávat o použitelnost a přijetí Jami ve srovnání s populárnějšími komunikačními platformami. Navíc decentralizovaná povaha Jami znamená, že uživatelé jsou zodpovědní za správu svých komunikačních koncových bodů, což může vyžadovat vyšší úroveň technického povědomí ve srovnání s centralizovanými komunikačními službami.

Z celkového hlediska lze shledat, že aplikace, které generují svůj zisk z cílené reklamy, mohou být považovány za méně důvěryhodné s ohledem k ochraně soukromí uživatelů. To je způsobeno tím, že tyto aplikace často sbírají uživatelská data pro účely personalizované reklamy, což může vést k riziku zneužití osobních informací. Na druhé straně jsou aplikace s otevřeným zdrojovým kódem obecně považovány za důvěryhodnější, protože umožňují veřejnou kontrolu a audit kódu. Tento přístup zvyšuje transparentnost a důvěru v zabezpečení aplikace. Uživatelé mají tendenci preferovat aplikace s otevřeným zdrojovým kódem, protože mají větší jistotu ohledně ochrany svých dat a soukromí. Zároveň je důležité zdůraznit, že bezpečnostní opatření a důvěryhodnost aplikace nezávisí pouze na jejím obchodním modelu nebo zdrojovém kódu, ale také na implementaci šifrování, transparentnosti o sběru dat a dalších bezpečnostních funkcích. Aplikace, které se po zvážení těchto skutečností jeví jako důvěryhodné, jsou tedy Signal a Jami.

9 HISTORICKÉ BEZPEČNOSTNÍ INCIDENTY

Tato kapitola se zaměřuje na historické bezpečnostní incidenty související s chatovacími aplikacemi. Digitální komunikace se stala nedílnou součástí moderního života a s tím souvisí i zvýšené riziko bezpečnostních hrozeb. Bezpečnostní incidenty jako jsou úniky dat a zranitelnost softwaru představují významné hrozby, které mohou mít závažné důsledky pro uživatele. Únik citlivých informací může vést k vážným důsledkům, včetně ohrožení soukromí, úniku citlivých informací, finančních ztrát, narušení důvěry i poškození pověsti jednotlivců či organizací. Analyzování těchto incidentů pomáhá lépe porozumět povaze rizik spojených s používáním chatovacích aplikací a identifikovat opatření nezbytná k ochraně uživatelů.

9.1 Cambridge Analytica (2018)

V roce 2018 se odehrál skandál týkající se zneužití osobních dat, které rezonovalo kolem britské společnosti Cambridge Analytica, zabývající se poradenskou činností, a sociální sítě Facebook. Předmětem skandálu bylo neoprávněné shromažďování dat více než 50 milionů uživatelů Facebooku, které byly následně využity pro cílenou politickou reklamu během důležitých politických událostí, jako byly americké prezidentské volby a britské referendum o odchodu z Evropské unie Brexit. Základní mechanismus, jakým byla data získána, spočíval ve využití aplikace „*This Is Your Digital Life*“, kterou vytvořil akademik Aleksandr Kogan ve spolupráci s Cambridge Analytica. Tato aplikace vyžadovala od uživatelů přístup k jejich osobním údajům, ale zároveň neoprávněně shromažďovala informace i o jejich přátelích na Facebooku, což vedlo k masivnímu úniku dat. (Cadwalladr, Graham-Harrison, 2018)

Facebook, jako platforma, na které ke zneužití došlo, nesplnil své základní povinnosti v oblasti ochrany osobních údajů. Nepodnikl adekvátní kroky k zabezpečení dat svých uživatelů, neinformoval je o zneužití jejich údajů a nehlásil tento incident regulačním orgánům, což je v rozporu s pravidly pro ochranu dat. (Cadwalladr, Graham-Harison, 2018)

Výsledkem tohoto skandálu bylo zahájení vyšetřování ze strany několika institucí, včetně britského Úřadu informačního komisaře a Volební komise, které se zaměřily na možné zneužití dat pro manipulaci politického procesu. Reakce na odhalení byla rychlá a rozsáhlá, zahrnující veřejné odsouzení, právní kroky a také legislativní návrhy. (Cadwalladr, Graham-Harrison, 2018)

Případ Cambridge Analytica odhalil, jak může být soukromí uživatelů na internetu zneužito nejen k ekonomickému zisku ale i k politickému ovlivnění a otevřel veřejnou debatu o ochraně osobních údajů. Tato kauza odkryla hlubší problémy v digitálním věku, které se týkají etiky a práva a také poukázala na složitost a výzvy spojené s ochranou osobních údajů. Také zdůraznila naléhavou potřebu efektivnější regulace a větší transparentnosti ze strany technologických společností, aby byla zajištěna ochrana individuálních práv uživatelů.

Tento incident vyvolal požadavky na zpřísnění pravidel a zavedení nových opatření pro ochranu osobních údajů, což vyplynulo i v následném uvedení Obecného nařízení o ochraně osobních údajů (GDPR) v Evropské unii. GDPR klade důraz na získání explicitního souhlasu od uživatelů před shromažďováním a zpracováním jejich dat. Toto nařízení také určuje, jaké opatření musí firmy přijmout, aby zajistily ochranu osobních údajů, a stanoví sankce pro ty, kdo tato pravidla poruší. (Luponis, Besnard, 2018)

V reakci na skandál Facebook přistoupil k zásadním změnám v pravidlech pro vývojáře, zvláště pak zrušil možnost sběru kontaktních údajů z uživatelských účtů bez jejich výslovného souhlasu. Tyto kroky byly zaměřeny na obnovu důvěry uživatelů a zlepšení obrazu společnosti, který byl tímto skandálem výrazně poškozen. Facebook také čelil možnosti vysokých finančních sankcí, které mu mohly být uloženy, kdyby se podobný incident odehrál po zavedení GDPR, což v případě Facebooku mohlo znamenat pokutu až 1,6 miliardy eur. (Luponis, Besnard, 2018)

Společnost Cambridge Analytica se dostala pod veřejný a mediální tlak a vyšetřování, které následovalo, bylo tak nákladné a poškozující pro reputaci firmy, že v roce 2018 oznámila svůj konec. Společnost se sice snažila obnovit důvěru veřejnosti a svých klientů, ale právě ztráta klientů a nedostatek nových zakázek ji přivedly k rozhodnutí o ukončení činnosti. (Ballhaus, Gross, 2018)

Celkově případ Cambridge Analytica poukázal na přístup k osobním údajům prostřednictvím nelegitimních metod skrze aplikaci, která byla původně vytvořena pro akademický výzkum, ale následně byla zneužita ke shromažďování dat uživatelů. Dále také odhalila nedostatečné zabezpečení dat na platformě Facebook, který umožnil, aby tato data byla použita pro politické a komerční účely bez jejich vědomí a souhlasu. Cambridge Analytica využila získaná data k vytvoření profilů uživatelů a jejich cílení s politickými reklamami a propagandou. Tímto způsobem mohla manipulovat politickými preferencemi a chováním uživatelů, což vyvolalo obavy ohledně integrity demokratických procesů a svobodného rozhodování. V neposlední řadě tato kauza zdůraznila nedostatečnou regulaci a

dohled nad sběrem a zpracováním osobních dat na internetu. To vyvolalo diskuzi o nutnosti posílení ochrany soukromí a zavádění přísnějších pravidel pro společnosti zabývající se zpracováním osobních údajů. Tento případ také posloužil jako varování pro ostatní firmy v oblasti digitálního marketingu a datové analytiky.

9.2 WhatsApp Pegasus Spyware (2019)

V roce 2019 byla odhalena zásadní bezpečnostní slabina v populární komunikační aplikaci WhatsApp. Tato zranitelnost umožňovala útočníkům zavést špionážní software do mobilních zařízení uživatelů bez jejich vědomí, pouze prostřednictvím příchozího hovoru. Přitom k instalaci nebylo zapotřebí, aby uživatel hovor aktivně přijal. Tento špionážní software, známý pod názvem Pegasus, byl vyvinut izraelskou společností NSO Group, která prohlašovala, že její produkt je určen primárně pro boj proti terorismu a kriminalitě a je přísně regulován izraelským Ministerstvem obrany. (Gilbert, 2019)

Pegasus je sofistikovaný nástroj schopný nejen sledovat hovory, zprávy, e-maily a kontakty, ale také aktivovat mikrofony a kamery na infikovaných zařízeních, což umožňuje dálkový dohled nad uživatelem bez jeho vědomí. Tato schopnost zásadně zasahuje do soukromí uživatelů a vyvolává vážné obavy o ochranu dat a osobního života. (Gilbert, 2019)

V reakci na tuto bezpečnostní hrozbu WhatsApp vydal aktualizaci, která měla zranitelnost opravit. Společnost také apelovala na své uživatele, aby software neustále aktualizovali a zachovali důvěru v šifrované komunikační platformy. Argumentovali, že i přes existující bezpečnostní rizika zůstává šifrování klíčovým nástrojem pro ochranu soukromí uživatelů v digitálním světě. (Gilbert, 2019)

Událost měla také soudní dohru. V roce 2019 bylo zahájeno soudní řízení společností WhatsApp proti firmě NSO Group, která byla obviněna z nelegálního špehování 1400 mobilních telefonů a jejich uživatelů. Podle tvrzení WhatsApp byl software Pegasus využíván k získávání neoprávněného přístupu k šifrovaným zprávám nejen mezi uživateli WhatsAppu ale i Skypu, Telegramu, WeChatu, Facebook Messengeru a dalších. V březnu 2024 americký federální soudce nařídil firmě NSO Group, aby poskytla společnosti WhatsApp zdrojový kód tohoto softwaru. (Hale, 2024)

Tento cílený útok na uživatele WhatsAppu ukázal, že ani komunikační aplikace s velkou uživatelskou základnou nejsou imunní vůči sofistikovaným útokům. Další následek bylo závažné porušení soukromí a důvěrnosti komunikace uživatelů. WhatsApp však na tuto

skutečnost zareagoval okamžitým vydáním aktualizace k opravě této zranitelnosti a také podnikl další opatření ke zlepšení bezpečnosti aplikace a prevenci podobných útoků v budoucnosti.

Tato událost však vyvolala širší otázky ohledně rovnováhy mezi bezpečností a soukromím a roli států a soukromých společností v digitálním dohledu. Existence a prodej špionážního softwaru jako je Pegasus ukazuje, že státy a korporace mají nástroje, které mohou zneužívat pro sledování občanů bez jejich vědomí nebo souhlasu. To staví uživatele smartphonů do zranitelné pozice, kdy jejich osobní informace mohou být snadno a tajně přístupné. Případ WhatsApp Pegasus odhalil jak složitá je dnes otázka digitální bezpečnosti a jak naléhavě je potřeba komplexního přístupu k regulaci a kontrole špionážního softwaru. Uživatelé a vlády by měly být ostražité a vyžadovat transparentnost a etické jednání od technologických společností, zatímco ty by měly být povinny zodpovídat za bezpečnostní hyby a zranitelnosti ve svých produktech.

9.3 Únik dat uživatelů Facebooku (2021)

V roce 2021 se svět dozvěděl o masivním úniku dat, který postihl více než 533 milionů uživatelů Facebooku z celkem 106 zemí. Tento únik vyvolal vážné obavy o bezpečnost a soukromí dat na internetu. Data, která byla zveřejněna na hackerském fóru, zahrnovala širokou škálu osobních informací - od telefonních čísel, přes Facebook ID, plná jména, lokality, data narození a v některých případech i emailové adresy uživatelů. (Holmes, 2023)

Společnost Facebook reagovala prohlášením, ve kterém uvedla, že se jedná o data, která byla získána již v roce 2019 a že v témže roce bylo také odstraněno zranitelné místo, které umožnilo tento únik. Přestože byla tato zranitelnost opravena, informace ukradené před tímto datem zůstali relevantní pro možné zneužití. (Holmes, 2023)

Důsledky tohoto úniku byly značné. Uživatelé, jejichž data unikla, čelili zvýšenému riziku sociálního inženýrství, podvodů a dalších hackerských útoků. Tyto incidenty poté mohou vést k dalším vážným následkům, od krádeže identity po finanční ztráty. Únik dat byl prezentován jako výrazné porušení důvěry uživatelů, což kladlo na společnost Facebook zvýšenou odpovědnost za ochranu osobních údajů svých uživatelů. Společnost čelila tlaku na zlepšení svých bezpečnostních protokolů a zajistila tak lepší ochranu dat uživatelů. (Holmes, 2023)

Případ navíc připomínal dřívější incidenty, jako byl skandál Cambridge Analytica, který také ukázal slabiny v ochraně dat uživatelů Facebooku. Tyto opakované problémy poukázaly na stálé výzvy, kterým čelí digitální soukromí a bezpečnost v současné době. Je jasné, že ochrana dat a soukromí na internetu zůstává komplexním a neustále se vyvíjejícím problémem, který vyžaduje neustálou pozornost a inovace.

9.4 Příčiny, následky a nápravná opatření

V rámci uvedených bezpečnostních incidentů bylo identifikováno několik **příčin**, které k těmto událostem vedly. K nim patří:

1. **Nedostatečná ochrana dat –** Všechny tyto případy ukázaly na nedostatečná bezpečnostní opatření, která byla implementována uvnitř těchto společností. Facebook, WhatsApp a Cambridge Analytica nesprávně spravovaly a chránily osobní údaje uživatelů.
2. **Technické chyby –** Některé úniky dat byly způsobeny technickými chybami a zranitelnostmi v systémech těchto společností, což umožnilo neoprávněným jedincům získat přístup k citlivým informacím.

Dále byly identifikovány **následky** úniků dat:

1. **Ztráta důvěry –** Tyto bezpečnostní incidenty způsobily ztrátu důvěry uživatelů v ochranu jejich osobních údajů. Uživatelé se stali obezřetnějšími při sdílení svých dat na těchto platformách a mohou se obrátit k alternativním službám, které nabízejí lepší zabezpečení.
2. **Právní důsledky –** Společnosti, které byly zapojeny do úniků dat, musely čelit právním důsledkům a regulačním sankcím.
3. **Dopady na pověst –** Tyto společnosti musely čelit ostré kritice a snaze obnovit svou pověst veřejnosti.

Byla implementována **nápravná opatření** s cílem eliminovat opakování těchto incidentů:

1. **Posílení ochrany dat –** Jako reakci na tyto incidenty provedly Facebook a WhatsApp změny ve svých bezpečnostních politikách a zavedly nová opatření pro ochranu osobních údajů uživatelů.

2. **Regulační intervence –** Úřady pro ochranu osobních údajů v mnoha zemích zahájily vyšetřování a uvalily pokuty na společnosti zapojené do úniků dat. Regulace ochrany osobních údajů byla posílena, aby se zabránilo podobným incidentům v budoucnosti.

Závěrem lze konstatovat, že analýza bezpečnostních incidentů spojených s aplikacemi Facebook, WhatsApp a Cambridge Analytica poukazuje na vážné nedostatky v ochraně osobních údajů uživatelů a technické chyby v bezpečnostních opatřeních těchto společností. Tyto incidenty měly široké důsledky, včetně ztráty důvěry uživatelů, právních následků a negativních dopadů na pověst dotčených firem. Pro eliminaci opakování podobných událostí byla provedena opatření zaměřená na posílení ochrany dat, regulační intervence a zlepšení bezpečnostních politik. Nicméně aby byla zajištěna trvalá ochrana osobních údajů uživatelů a předešlo se budoucím bezpečnostním incidentům, je nezbytné, aby společnosti i regulační orgány pokračovaly v úsilí o vylepšení bezpečnostních standardů a dodržování příslušných zákonů a předpisů.

10 HROZBY SPOJENÉ S CHATOVACÍMI APLIKACEMI

V komunikačních aplikacích existují různé hrozby spojené s bezpečností a soukromím uživatelů. Chatovací aplikace často vyžadují přístup k široké škále osobních informací, jako jsou kontakty, fotky nebo lokace. Tyto údaje mohou být vystaveny riziku zneužití, pokud nejsou adekvátně chráněny. Pokud má aplikace bezpečnostní slabiny, je pravděpodobné, že dojde k úniku citlivých informací, což může vést ke krádeži identity nebo finanční ztrátě.

10.1 Sociální inženýrství

Sociální inženýrství se v posledních letech stalo jednou z nejrozšířenějších a zároveň nejnebezpečnějších manipulačních technik, které útočníci využívají k dosažení svých cílů. Tato metoda spočívá v manipulaci s lidmi za účelem získání důvěryhodných informací, které by pro ně jinak byly nedostupné. Útočníci, využívající sociální inženýrství, se zaměřují na psychologické aspekty lidského chování, aby dokázali ovlivnit své oběti a přimět je k nežádoucím akcím, jako je sdílení hesel, osobních údajů nebo přístup k chráněným systémům. Pachatelé, kteří tuto praktiku využívají, jsou často vysoce kvalifikovaní v oblastech psychologie a komunikace. Jsou schopni rychle rozpoznat slabiny své oběti a využít je ve svůj prospěch.

Jednou z nejzáludnějších metod, jakými mohou útočníci zneužívat chatovací aplikace je, že se mohou vydávat za osoby, které jejich oběti znají a důvěřují jim. Dále se také může jednat o falešné profily, které jsou na první pohled k nerozeznání od skutečných. Jakmile si tedy útočník získá důvěru nic netušícího uživatele, otevírá se mu cesta k dalším manipulacím. Mohou začínat nevinně, například prosbou o pomoc nebo zdánlivě neškodným dotazem. Postupně však mohou eskalovat do žádostí, které již mají za cíl získat citlivé informace, jako jsou hesla, čísla kreditních karet nebo dokonce přístupy k bankovním účtům. To v nejhorším případě může vést k finančním ztrátám nebo ke krádeži identity.

Pro oběti je často obtížné pochopit, že byly napadeny, dokud není příliš pozdě. Útočníci se totiž mohou velmi dobře maskovat a využívat sofistikované techniky, aby se vyhnuli odhalení. V důsledku toho mohou jejich manipulace pokračovat dlouhodobě, aniž by se oběti dozvěděly o pravé identitě útočníka. Je tedy zřejmé, že využívání sociálního inženýrství v chatovacích aplikacích představuje vážný bezpečnostní problém, který vyžaduje neustálou pozornost jak od samotných uživatelů, tak od vývojářů aplikací. Každý uživatel by tak měl být ostražitý a skeptický vůči jakýmkoliv neobvyklým nebo nečekaným požadavkům zaslaným prostřednictvím online komunikace.

10.2 Phishing

Útočníci pro své činnosti používají různé techniky sociálního inženýrství. Jednou z nich je takzvaný phishing. Jedná se o typ bezpečnostního rizika a internetového podvodu, který je maskován tak, aby působil důvěryhodně a nalákal nic netušící uživatele do pasti. Útočníci, kteří stojí za těmito podvody, se specializují na vytváření falešných zpráv nebo webových stránek, které na první pohled vypadají jako opravdové. Tyto stránky jsou vytvářeny tak, aby dokonale napodobily vzhled a styl originálních služeb, což uživatelům ztěžuje rozpoznání podvodu.

Phishingové útoky se neustále vyvíjejí a adaptují, což ztěžuje jejich rozpoznání. Útočníci neustále hledají nové metody, jak obejít bezpečnostní opatření a lépe zacílit na své oběti. S rostoucí popularitou sociálních sítí se začali objevovat phishingové útoky i na těchto platformách, kde útočníci využívají falešné profily pro získání důvěry a následné zmanipulování uživatelů k poskytnutí jejich osobních údajů.

Co se týče chatovacích aplikací, stávají se ideálním prostředím pro tyto druhy útoků z několika důvodů. Prvním z nich je vysoký stupeň důvěry, kterou uživatelé těmto platformám obvykle věnují. Lidé často předpokládají, že zprávy přicházející od přátel nebo známých jsou bezpečné, a právě tento předpoklad zneužívají útočníci.

Phishingový útok v chatovacích aplikacích obvykle začíná získáním kontroly nad účtem skutečné osoby, kterou útočník napodobuje. To může být dosaženo různými metodami, jako je krádež hesel skrze jiné kompromitované weby, využití malware nebo technikou sociálního inženýrství, kde útočník přesvědčí oběť, aby mu poskytla své přihlašovací údaje.

Jakmile má útočník přístup k účtu, může začít rozšiřovat škodlivé zprávy mezi kontakty oběti. Tyto zprávy mohou obsahovat přesvědčivé výzvy k akci, jako je například kliknutí na odkaz, který vede na falešnou přihlašovací stránku, nebo přílohy obsahující malware. Útočník může dokonce přetvářet, že potřebuje finanční pomoc, což vede k žádosti o převod peněz.

Dalším faktorem, který činí chatovací aplikace atraktivním cílem pro phishing, je jejich rozšířené užívání a integrace do každodenního života. Uživatelé často reagují na zprávy rychle a bez hlubšího promýšlení, což zvyšuje pravděpodobnost, že na phishingový pokus naletí. Navíc, sofistikovanější útočníci mohou využít funkcí, jako jsou skupinové chaty, k šíření škodlivého obsahu mezi velkým počtem uživatelů najednou.

Pro ochranu proti phishingovým útokům je důležité vědět, jak rozpoznat podezřelé zprávy. Často obsahují gramatické chyby, nabízejí neobvykle výhodné nabídky, nebo pocházejí od osoby, která se chová netypicky. Je také klíčové vždy ověřovat identitu osoby, která požaduje citlivé informace nebo peněžní transakce, a to i v případě, že se zdá být důvěryhodná.

Je také důležité, aby uživatelé byli vždy na pozoru a kontrolovali pravost odkazů a zpráv, které obdrží a to i když pocházejí od známých osob. Používání dvoufaktorové autentizace a pravidelná změna hesel je také efektivní strategií pro zvýšení online bezpečnosti. Vždy je lepší přistupovat k neznámým zprávám s opatrností a skeptickým pohledem, aby se předešlo možným phishingovým útokům.

10.3 Malware

Další hrozbou je možnost šíření malwaru a virů prostřednictvím chatovacích aplikací. Útočníci využívají různé taktiky jako je odesílání škodlivých odkazů nebo souborů infikovaných těmito viry, které vypadají jako neškodné zprávy od známých osob. Uživatelé mohou být lákáni k jejich otevření pomocí sofistikovaných triků. Kliknutím na takový odkaz nebo stažením souboru, uživatel nevědomky nainstaluje škodlivý software, který může napáchat vážné škody na zařízení. Takto aktivovaný malware může napadnout zařízení a tajně krást citlivé informace, monitorovat online aktivitu uživatele nebo dokonce plně ovládat infikované zařízení.

Prostřednictvím takovýchto útoků kybernetičtí zločinci požadují výkupné od obětí, prodávají ukradené informace na černém trhu nebo manipulují se zařízeními pro další distribuci malware. Je tedy nezbytné, aby sami uživatelé přijali aktivní ochranu ve své kybernetické obraně a pravidelně aktualizovali své aplikace, věnovali pozornost povolením při instalaci nových aplikací a byli ostražití vůči jakýmkoliv neobvyklým zprávám a požadavkům.

10.4 Kyberšikana

Kromě technických hrozeb existují i sociální a psychologické aspekty spojené s používáním chatovacích aplikací. Kyberšikana je alarmujícím fenoménem, který v posledních letech získává na síle a stále více ovlivňuje online prostředí. A chatovací aplikace představují platformy, na kterých se tato negativní interakce často odehrává.

Uživatelé, a to zejména mladiství, mohou být vystaveni zastrašování, urážkám nebo dokonce vydírání, což může mít vážné následky na jejich psychické zdraví a pohodu. Pachatelé prostřednictvím těchto aplikací využívají anonymitu, kterou internet poskytuje. Uživatelé se za svými obrazovkami cítí v bezpečí, což může vést k odvážnějšímu a agresivnějšímu chování, než by bylo pravděpodobné v osobním setkání. To může vyústit v situace, kdy jednotlivec používá aplikaci k šíření lží, pomluv, k vyhrožování či zveřejňování kompromitujících materiálů a vyvíjení psychického tlaku na své oběti.

Navíc dostupnost těchto aplikací znamená, že šikana může pokračovat nepřetržitě 24 hodin denně a to i mimo školní prostředí nebo pracoviště, a tím je tento druh šikany zvláště zákeřný. Oběti kyberšikany často pociťují depresi a mohou se cítit osamocené. Stigma spojené s tímto zážitkem způsobuje, že se oběti bojí hledat pomoc nebo promluvit o svých zkušenostech. Dlouhodobé následky kyberšikany mohou zahrnovat sebevražedné myšlenky a v krajních případech dokonce sebevraždy.

Je nezbytné, aby společnost i jednotlivci rozpoznali závažnost a potenciální dopady kyberšikany. Klíčovou roli v prevenci a řešení tohoto problému mají školy a rodiče a vzdělání o digitálním prostředí a bezpečnosti na internetu by mělo být součástí školních programů.

10.5 Nadměrné používání a závislost

Nadměrné používání chatovacích aplikací představuje problém, který se v současné době dotýká mnoha aspektů našeho každodenního života, a to jak v osobní, tak profesní sféře. Jedním z hlavních problémů je nadužívání těchto aplikací během pracovní doby, což vede k výraznému poklesu produktivity. Zaměstnanci často podléhají pokušení zkontrolovat nové zprávy nebo se zapojit do dlouhých neformálních konverzací, což odvádí jejich pozornost od pracovních úkolů.

Kromě toho, nevhodné užití chatovacích aplikací mívá negativní dopad i na mezilidské vztahy. Například šíření neověřených informací a dezinformací mezi uživateli může vést k nedorozuměním a konfliktům. Toto šíření falešných informací je obzvláště nebezpečné v době, kdy společnost čelí krizovým situacím, jako jsou pandemie nebo politické volby.

Nadměrné používání často vede k postupnému rozvoji závislosti, kdy uživatelé cítí nutkání neustále kontrolovat své telefony, aby zjistili, zda nedostali novou zprávu nebo upozornění.

Tato potřeba být neustále online vede k zanedbávání osobních vztahů v reálním životě, protože virtuální interakce nahrazuje skutečné lidské kontakty.

Na druhou stranu, závislost na chatovacích aplikacích může mít i fyzické důsledky. Dlouhé hodiny strávené zíráním do obrazovek mohou způsobit problémy s viděním, chronickou únavu očí, bolesti hlavy či nespavost. Bolesti krku a zad, jsou také časté u lidí, kteří tráví příliš mnoho času používáním svých mobilních zařízení.

Je důležité najít rovnováhu mezi využíváním technologických vymožeností a udržením zdravého životního stylu. Omezování času stráveného na chatovacích aplikacích, stanovení konkrétních časů pro kontrolu zpráv a vědomé vypínání notifikací mohou pomoci redukovat závislost a zlepšit kvalitu života.

10.6 Nevhodné užití

Riziko může představovat i využití chatovacích aplikací k posílání nevhodných zpráv druhé osobě. Tyto zprávy mají různé formy, ať už se jedná o slovní urážky, nevyžádané sexuální obsahy nebo manipulativní a agresivní výhružky. Takové chování nejenže narušuje důvěru v bezpečné využívání chatovacích aplikací, ale také může mít dopad na psychickou pohodu příjemce těchto zpráv. Osoby, které jsou cílem nevhodných zpráv, se často cítí ohroženy, osaměle a zranitelně, což může vést k úzkosti nebo depresi.

Toto chování bývá motivováno různými faktory. Někteří uživatelé mohou využívat anonymitu, kterou internet poskytuje, k vyjádření negativních emocí nebo frustrace, které by si v běžném životě neodpustili. V jiných případech může jít o nedorozumění sociálních norem a hranic, což vede k tomu, že jednotlivci nejsou schopni rozpoznat, kdy jejich chování překračuje meze přijatelnosti. Vytváření jasných pravidel co je a co není přijatelné v digitální komunikaci, a poskytování nástrojů pro nahlášení nevhodného chování, jsou základní kroky k zajištění, že chatovací aplikace zůstanou prostředkem pro pozitivní a produktivní výměnu mezi lidmi.

V konečném důsledku je důležité si uvědomit, že za každou obrazovkou je skutečný člověk s reálnými emocemi a že slova mají váhu a ovlivňují životy druhých. Pochopení tohoto může vést k zodpovědnějšímu využívání digitálních nástrojů a kultivaci prostředí, kde je bezpečnost a vzájemný respekt na prvním místě.

11 HODNOCENÍ KOMUNIKAČNÍCH APLIKACÍ

Z hlediska bezpečnosti a ochrany soukromí uživatelů lze tedy říci, že aplikace Messenger není vhodný hned z několika důvodů. Za prvé Messenger je provozován společností Meta, která má problematickou minulost v oblasti ochrany dat a bezpečnosti uživatelů a je spojována s několika bezpečnostními incidenty. Financování aplikace probíhá prostřednictvím cílené reklamy a prodeje osobních dat a to vyvolává obavy ohledně soukromí uživatelů. Navíc aplikace shromažďuje rozsáhlé množství dat včetně polohy, kontaktních informací a historie prohlížení, která jsou posílána mateřské společnosti.

Další aplikace, která není doporučována, je Skype. Šifrování není ve výchozím nastavení a aplikace vydělává na osobních datech uživatelů. Společnost Microsoft shromažďuje data, jako jsou kontaktní informace a uživatelský obsah a není transparentní ohledně zpracování těchto dat. To stejné platí i pro aplikaci Instagram, která sice koncové šifrování implementováno má, avšak nemá ho zavedeno pro chaty automaticky a uživatel na něj musí v nastavení přepnout. Telegram, podobně jako Skype, má problémy s nedostatečným šifrováním a špatným obecným postojem k soukromí uživatelů. Navíc aplikace shromažďuje uživatelská data a metadata a není open-source.

WhatsApp, který vlastní společnost Meta, je také kritizován kvůli nedostatečné ochraně soukromí uživatelů a nedostatečnému šifrování. Společnost shromažďuje široké spektrum uživatelských dat a metadata a má problematickou minulost v oblasti ochrany dat a je také spojen s několika bezpečnostními incidenty. Naopak aplikace Jami je chválena pro svou bezpečnost a ochranu soukromí. Komunikace probíhá mezi uživateli bez serverů a aplikace používá koncové šifrování. Jami je multiplatformní, anonymní a open-source, což přispívá k jeho vysoké úrovni bezpečnosti a důvěryhodnosti. Co se týče aplikace Jami, problémem je spíše to, že se jedná o platformu, která zatím není mezi uživateli příliš známá.

Aplikace Signal je doporučována pro svůj důraz na bezpečnost a ochranu soukromí. Poskytuje koncové šifrování ve všech typech komunikace a má dobrý obecný postoj k soukromí uživatelů. Signal není financován prostřednictvím cílené reklamy ale prostřednictvím nadace Freedom of the Press, což zvyšuje jeho důvěryhodnost. Aplikace také shromažďuje pouze minimální množství uživatelských dat. Výhodou Signalu oproti dalším chatovacím aplikacím je, že má open-source protokol vytvořený samotným Signalem a tudíž jeho zdrojový kód může být kontrolován a upravován kýmkoli.

WeChat, ačkoliv není spojován s bezpečnostními incidenty, vyvolává oprávněné obavy kvůli svému kontroverznímu původu. Dalším důvodem k obezřetnosti je vydání varování ze strany NÚKIB ohledně možných hrozeb spojených s touto aplikací. Uživatelé by se tak této aplikaci měli v nejlepším případě zcela vyhnout.

Z analýzy bezpečnostních aspektů uvedených komunikačních aplikací vyplývá, že Signal a Jami mají výrazné výhody oproti ostatním platformám. Signal se vyznačuje vysokou úrovni bezpečnosti díky koncovému šifrování ve všech typech komunikace, což je důležitý faktor pro ochranu soukromí uživatelů. Důraz na nezávislé ověření a open-source přístup posiluje důvěryhodnost a transparentnost této aplikace. Navíc Signal nabízí uživatelsky přívětivé funkce a je provozován neziskovou nadací.

Podobně Jami nabízí koncové šifrování a další bezpečnostní prvky, které přispívají k ochraně soukromí uživatelů. Multiplatformnost, anonymita při registraci a možnost komunikace bez centrálního serveru jsou další výhody této aplikace. Nicméně, jedním z jejích omezení je relativní neznámost ve srovnání s jinými populárními aplikacemi, což může způsobit nedostatek důvěry některých uživatelů. A také z toho může plynout neochota uživatelů přestoupit na toto pro mnohé neznámé komunikační médium. Mnoho uživatelů má tendenci zůstat raději u známých komunikačních platforem, jako je WhatsApp nebo Messenger. Toto chování může být důsledkem preferencí spojených s existujícími skupinami přátel či obav z toho, že přestup na novou platformu omezí jejich možnosti komunikace. Uživatelé často preferují jednoduchost a pohodlí jediné aplikace, která jim umožňuje spojit se s většinou svých známých, před používáním více aplikací pro různé skupiny kontaktů.

Celkově lze říci, že Signal a Jami se jeví jako nejlepší volby pro uživatele, kteří kladou důraz na bezpečnost a ochranu soukromí. Signal se vyznačuje vysokou bezpečností a širokou uznávaností, zatímco Jami nabízí podobné bezpečnostní funkce a je zároveň multiplatformní a anonymní. Avšak pro Jami je důležité zdůraznit, že je potřeba zvýšit povědomí o této aplikaci, aby si uživatelé uvědomili její potenciál a využili ji jako bezpečnou alternativu k běžnějším komunikačním platformám.

12 NAVRHOVANÁ DOPORUČENÍ

Při výběru vhodné chatovací platformy je nezbytné, aby uživatelé vzali v úvahu několik klíčových faktorů, které ovlivňují bezpečnost a ochranu soukromí uživatelů. Následující doporučení mohou uživatelům pomoci k zajištění bezpečnějšího a soukromějšího prostředí pro jejich komunikaci.

12.1 Šifrování

Šifrování zpráv v chatovacích aplikacích představuje důležitý prvek moderní komunikační bezpečnosti. Jeho důležitost spočívá v ochraně soukromí jednotlivců i firem před neoprávněným přístupem třetích stran. V současné době, kdy jsme stále více propojeni prostřednictvím digitálních technologií, je tato ochrana nezbytná.

Takové šifrování zpráv chrání osobní informace, které jsou vyměňovány během každodenních konverzací. Tyto informace mohou zahrnovat citlivé údaje, jako jsou finanční informace, osobní identifikační čísla, nebo i intimní detaily osobního života. Pokud by tyto informace byly přístupné neoprávněným osobám, mohlo by to vést k řadě negativních důsledků, včetně finančních ztrát nebo osobního zneužití.

Chatovací aplikace, které si zakládají na přítomnosti koncového šifrování, které zajišťuje, že veškerá komunikace mezi uživateli je zabezpečena a nepřístupná pro neoprávněné osoby, se jeví jako důvěryhodnější. Aplikace, které používají koncové šifrování ve výchozím nastavení pro všechny chaty, poskytují vyšší úroveň bezpečnosti a ochrany dat, což je důležité zvláště při sdílení citlivých informací. Jedná se o aplikace WhatsApp, Facebook Messenger, Signal a Jami.

V neposlední řadě, šifrování přispívá k udržení důvěry mezi uživateli chatovacích aplikací. Když lidé vědí, že jejich konverzace jsou bezpečné a soukromé, jsou ochotnější využívat tyto služby pro osobní i profesionální komunikaci. Tato důvěra je zásadní pro udržení uživatelské základny a pro růst aplikací ve velmi konkurenčním prostředí digitálních technologií.

12.2 Ochrana soukromí

S rostoucím počtem aplikací, které uživatelé využívají pro každodenní aktivity, je nezbytné, aby také zaměřili na politiky ochrany soukromí těchto nástrojů. Většina uživatelů si ovšem

často není vědoma, jaké údaje jsou sbírány, jak jsou tyto informace využívány a zda jsou data sdílena s třetími stranami.

Jedním z prvních kroků, který by měl uživatel učinit před stažením nebo používáním jakékoli aplikace, je důkladné pročtení politiky ochrany soukromí. Tato politika by měla jasně specifikovat, které osobní údaje aplikace sbírá. Mohou to být údaje, jako je geolokace, informace o zařízení, kontakty, osobní identifikátory, ale i citlivější data jako zdravotní informace nebo finanční záznamy.

Dalším důležitým aspektem je způsob, jakým aplikace s těmito údaji nakládá. Uživatelé by měli hledat informace o tom, zda jsou data používána výhradně pro účely, pro které byla shromážděna, nebo zda jsou využívána i pro další činnosti, jako je cílení reklam. V neposlední řadě je klíčové zjistit, zda jsou data sdílena s třetími stranami a za jakým účelem. Tato třetí strana může být například reklamní agentura, analytická firma nebo dokonce vládní instituce.

Transparentnost provozovatele aplikace je rovněž klíčová. Uživatelé by měli vyhledávat aplikace, které byly vytvořeny společnostmi s dobrým jménem v oblasti kybernetické bezpečnosti. Společnosti, které jsou transparentní ve svých postupech, poskytují jasné informace o tom, jak jsou data chráněna, jaké bezpečnostní protokoly jsou implementovány a jak rychle reagují na bezpečnostní incidenty. Firmy, které investují do zabezpečení a mají prokazatelné zkušenosti s ochranou uživatelských dat, obvykle poskytují vyšší úroveň důvěry a spolehlivosti.

Ve světle skandálů spojených s úniky dat je více než zřejmé, že uživatelé musí být proaktivní. Využití aplikací, které neposkytují dostatečné záruky ochrany osobních údajů, může vést k vážným rizikům, včetně zneužití identity a finančních ztrát. Proto je nutné, aby uživatelé nejenže přečetli a pochopili politiku ochrany soukromí, ale také sledovali jakékoli změny v pravidlech a pravidelně kontrolovali, jaké aplikace mají přístup k jejich datům.

Uživatelé by se také měli zaměřit na aplikace, které respektují soukromí a nevyžadují přístup k nadbytečnému množství osobních údajů, jako jsou kontaktní seznamy či fotografie, pokud to není absolutně nezbytné pro správné fungování dané aplikace. Tímto se minimalizuje riziko neoprávněného sběru a zneužití citlivých informací uživatelem. Je důležité se zajímat o to, jaké konkrétní údaje aplikace vyžaduje a zda jsou tyto informace skutečně nezbytné pro poskytování služeb, které aplikace nabízí. Uživatelé by měli dbát na to, aby jejich osobní

údaje zůstaly chráněny a byly sdíleny pouze tehdy, když je to nezbytně nutné a důvěryhodně zabezpečeno.

12.3 Způsoby financování

Dalším hledisko, které by mělo být pro uživatele předmětem zvýšené pozornosti, je způsob financování aplikace. Aplikace na trhu mohou být financovány různými způsoby, které mají přímý dopad na to, jak je zacházeno s daty uživatelů.

Jedním z běžných modelů je financování prostřednictvím cílené reklamy. V tomto modelu aplikace shromažďují data o chování a preferencích uživatelů, aby mohly nabízet reklamy, které jsou přizpůsobeny jejich zájmům. Tento přístup může vést k tomu, že ochrana soukromí uživatelů je obětována ve prospěch zisku. Reklamní společnosti a vývojáři aplikací mohou být motivováni k co nejpodrobnějšímu profilování uživatelů, což zvyšuje riziko úniků osobních dat nebo jejich zneužití.

Dalším způsobem financování, který vyvolává obavy, je prodej osobních dat třetím stranám. Některé aplikace mohou uživatelům nabízet bezplatné služby, ale poté prodávají shromážděná data různým společnostem, které pak mohou tato data využít pro své komerční účely. Tento model často není zcela transparentní, a uživatelé tak nemusí mít plnou kontrolu nad tím, kdo a jak může jejich informace využívat.

Vzhledem k těmto rizikům je zásadní, aby si uživatelé při výběru aplikací pečlivě pročítali podmínky užívání a zásady ochrany osobních údajů. Důležité je hledat aplikace, které jsou financovány modely, jež neohrožují soukromí uživatelů. Příkladem mohou být aplikace, které se financují předplatným nebo jednorázovým nákupem, kde není potřeba další monetizace prostřednictvím dat.

Pro zajištění maximální ochrany soukromí je také doporučeno využívat aplikace od renomovaných vývojářů, kteří mají prokazatelnou historii dodržování etických standardů v ochraně dat a soukromí. K tomu může přispět i aktivní komunita uživatelů, kteří aplikace hodnotí a diskutují o nich, což může pomoci identifikovat potenciální rizika a nežádoucí praktiky.

12.4 Aktualizace

Zásadní je také sledovat pravidelné aktualizace a zabezpečení aplikace. Tento proces není pouze rutinní údržbou, ale je základním kamenem pro zajištění ochrany dat a soukromí

uživatelů. Aktualizace a zabezpečení aplikací jsou komplexní procesy, které vyžadují neustálou pozornost a adaptaci na nově vznikající hrozby a bezpečnostní slabiny.

Na první pohled se může zdát, že pravidelné aktualizace softwaru jsou primárně určeny k rozšíření funkcionalit nebo vylepšení uživatelského prostředí. Avšak hlubší pohled odhalí, že mnoho z těchto aktualizací zahrnuje klíčové bezpečnostní opravy. Vývojáři neustále monitorují své aplikace za účelem identifikace a opravy bezpečnostních zranitelností, které by mohly být zneužity škodlivými útočníky. Tyto bezpečnostní díry mohou existovat v různých formách, od jednoduchých chyb v kódu po složité systémové nedostatky.

Aktivní a pravidelné aktualizace zabezpečení, prováděné vývojářskými týmy, jsou nezbytné pro ochranu aplikací před nejnovějšími typy útoků, které se neustále vyvíjejí. Například, jakmile je objeven nový typ malwaru, vývojáři musí rychle reagovat a implementovat opatření pro blokování těchto hrozeb před tím, než mohou způsobit škody.

Kromě samotných aktualizací je důležité, aby aplikace obsahovala robustní vnitřní zabezpečení. To zahrnuje šifrování dat, bezpečnou autentizaci uživatelů, a implementaci různých obranných mechanismů, jako je detekce a prevence průniku. Tyto prvky zabezpečení hrají klíčovou roli v ochraně osobních a citlivých informací uživatelů a zajišťují, že aplikace zůstává důvěryhodná a bezpečná.

Pokud aplikace pravidelně aktualizuje své bezpečnostní protokoly a rychle reaguje na nové hrozby, poskytuje svým uživatelům výrazně vyšší úroveň ochrany. To nejenže zvyšuje důvěru uživatelů v produkt, ale také posiluje celkovou reputaci firmy na trhu. U uživatelů, kteří se cítí bezpečně při používání aplikace, je pravděpodobnější, že zůstanou věrni dané platformě a doporučí ji i dalším.

Ve světě, kde se bezpečnostní hrozby objevují a vyvíjejí se značnou rychlostí, nemůžeme podceňovat význam pravidelných aktualizací a pečlivě navrženého zabezpečení aplikací. Tyto kroky nejenže chrání uživatele, ale celou infrastrukturu a integritu digitálních služeb. Je to neustálý boj s časem a škodlivými aktéry, ve kterém musí být vývojáři a bezpečnostní týmy vždy o krok napřed.

12.5 Ochrana před phishingem

Z pohledu obrany je důležité implementovat několik základních kroků, aby bylo možné chránit se před phishingovými útoky. Jedním z nejefektivnějších způsobů je vzdělávání uživatelů o tom, jak tyto útoky vypadají a jaké jsou nejnovější metody, které útočníci

používají. Dále je důležité používat pokročilá bezpečnostní řešení, která zahrnují antivirové programy a firewally. Tyto nástroje mohou pomoci identifikovat a blokovat škodlivé e-maily a webové stránky, dříve než mohou způsobit škodu. Navíc je zásadní pravidelně aktualizovat všechny systémy a aplikace, aby byly chráněny proti známým hrozbám a zranitelnostem, které by mohli útočníci využít.

ZÁVĚR

Cílem této diplomové práce bylo zhodnotit stav komunikačních služeb, analyzovat rizika a hrozby spojená s datovou bezpečností a navrhnout doporučení ke zlepšení stávajícího stavu.

Je patrné, že služby pro okamžité odesílání zpráv, jako jsou WhatsApp, Messenger, Signal, či Instagram, jsou neodmyslitelnou součástí moderní digitální komunikace. Tyto aplikace přinášejí rychlost a efektivitu při komunikaci, ale zároveň s sebou nesou i různá rizika spojená s datovou bezpečností.

Analýza a srovnání těchto aplikací a s nimi spojených bezpečnostních incidentů odhalila, že některé z nich poskytují vysokou úroveň zabezpečení, jako je například Signal, který nabízí end-to-end šifrování ve všech typech komunikace a klade důraz na ochranu soukromí uživatelů. Na druhou stranu jsou zde aplikace, které nedosahují stejné úrovně bezpečnosti, jako například Instagram, jehož šifrování není ve výchozím nastavení a také shromažďuje data uživatelů pro účely reklamy a prodeje. Důležité je mít na paměti i nebezpečí související s nadměrným používáním a závislostí na těchto službách, které může negativně ovlivnit soukromí a produktivitu uživatelů.

Vzhledem k neustálému vývoji technologií a kybernetických hrozeb je nezbytné, aby poskytovatelé služeb pro okamžité odesílání zpráv soustavně aktualizovali své systémy a zlepšovali zabezpečení aplikací. Stejně tak je důležité, aby se uživatelé informovali o aplikacích, které využívají, o způsobu jejich financování, o nebezpečích online prostředí a naučili se rozpoznávat podezřelé aktivity a zprávy.

Celkově lze konstatovat, že datová bezpečnost v kontextu služeb pro okamžité odesílání zpráv je nezbytným aspektem moderní digitální komunikace. Používání těchto aplikací přináší mnoho výhod, ale zároveň s sebou nesou i určitá rizika a výzvy. Je zásadní, aby uživatelé byli obezřetní a chránili své osobní údaje před potenciálními kybernetickými hrozbami.

.

SEZNAM POUŽITÉ LITERATURY

ALI, Al-Rahim a ALSAAD, Saad Najim, 2020. Instant Messaging Security and Privacy Secure Instant Messenger Design. Online. *Materials Science and Engineering.* Č. 881, s. 1-10. Dostupné z: https://doi.org/doi: 10.1088/1757-899X/881/1/012117. [cit. 2024-03-30].

BALLHAUS, Rebecca a GROSS, Jenny, 2018. *Cambridge Analytica Closing Pperations Following Facebook Data Controversy.* Online. WSJ pro Cybersecurity. Dostupné z: https://www.wsj.com/articles/cambridge-analytica-closing-operations-following-facebook-data-controversy-1525284140. [cit. 2024-04-16].

BANOTH, Rajkumar a REGAR, Rekha, 2023. *Classical and Modern Cryptography for Begginers.* Springer Nature Switzerland. ISBN 978-3-031-32958-6.

BERLOVE, Orlee. 2024. *End-to-End Encryption: The Ultimate Guide to How it Works.* Online. Preveil. Dostupné z: https://www.preveil.com/blog/end-to-end-encryption/. [cit. 2024-04-12].

BHATTACHARYYA, Dhruba Kumar a KALITA, Jugal Kumar, 2016. *DDoS Attacks: Evolution, Detection, Prevention, Reaction and Tolerance.* 1. Boca Raton: CRC Press. ISBN 978-1-4987-2965-9.

BINNS, Rob. 2023. *Websites Banned in China: Acces, Alternatives and Unblocked Sites.* Online. Independent Advisor. Dostupné z: https://www.independent.co.uk/advisor/vpn/websites-banned-in-china. [cit. 2024-04-12].

CADWALLADR, Carole a GRAHAM-HARRISON, Emma, 2018. *Revealed: 50 Million Faebook Profiles Harvested for Cambridge Analytica in Major Data Breach.* Online. The Guardian. Dostupné z: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. [cit. 2024-04-16].

Co je kyberkriminalita. 2022. Online. Správa sítě. Dostupné z: https://www.sprava-site.eu/kyberkriminalita/. [cit. 2024-02-29].

Co jsou kybernetické hrozby, 2023. Online. Aptien. Dostupné z: https://aptien.com/cs/kb/articles/what-are-cybersecurity-threats. [cit. 2024-02-24].

ČESKO. *Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.* Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN. [cit. 2024-04-12].

ČESKO. *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).* Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32022L2555. [cit. 2024-04-12].

ČESKO. *Vyhláška 317/2014 Sb., ze dne 15. prosince 2014 o významných informačních systémech a jejich určujících kritériích.* Online. Dostupné z: https://nukib.gov.cz/download/publikace/legislativa/2021-06-14_vyhlaska-o-VIS.pdf. [cit. 2024-04-12].

ČESKO. *Vyhláška ze dne 24. srpna 2021 o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.* Online. Dostupné z: https://nukib.gov.cz/images/2021-08-31_vyhlaska-bezpecnostni-urovne.pdf. [cit. 2024-04-12].

ČESKO. *Vyhláška ze dne 24. srpna 2021 o některých požadavcích pro zápis do katalogu cloud computingu.* Online. Dostupné z: https://nukib.gov.cz/images/2021-08-31_vyhlaska-vstupni-kriteria.pdf. [cit. 2024-04-12].

ČESKO. *Vyhláška ze dne 7. června 2023 o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.* Online. Dostupné z: https://nukib.gov.cz/download/publikace/legislativa/vyhlaska-bezpecnostni-pravidla.pdf. [cit. 2024-04-12].

ČESKO. *Zákon 181/2014 Sb. ze dne 23. července 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* Online. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181. [cit. 2024-04-12].

DAIMI, Kevin (ed.), 2018. *Computer and Network Security Essentials*. 1. Springer International Publishing. ISBN 978-3-319-58423-2.

DOFFMAN, Zak, 2021. *Proč byste měli soukromé zprávy přestat posílat přes Messenger?* Online. Forbes. Dostupné z: https://forbes.cz/proc-byste-meli-sve-soukrome-zpravy-prestat-posilat-pres-messenger/. [cit. 2024-03-28].

Doporučení pro používání aplikace Signal, 2022. Online. NÚKIB. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1816-doporuceni-pro-pouzivani-aplikace-signal/. [cit. 2024-03-20].

ELDRIDGE, Alison. 2024. *Instagram – Social Networking Service.* Online. Brittanica. Dostupné z: https://www.britannica.com/topic/Instagram. [cit. 2024-02-21].

ELKIND, Peter; GILLUM, Jack a SILVERMAN, Craig, 2021. *How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users.* Online. ProPublica. Dostupné z: https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users. [cit. 2024-04-22].

Firewall, 2024. Online. Eset. Dostupné z: https://www.eset.com/cz/firewall/. [cit. 2024-02-21].

GILBERT, Ben, 2019. *An Insider Reveals How the Nasty Spyware Used in the WhatsApp Breach Lets Governments Secretly Access Everything in Your Smartphone, from Text Messages to the Microphone and Cameras.* Online. Business Insider. Dostupné z: https://www.businessinsider.com/whatsapp-hack-what-is-pegasus-2019-5. [cit. 2024-04-18].

HALE, Craig, 2024. *WhatsApp Wins Access to NSO Group´s Pegasus Spyware Code in New Court Hearing.* Online. Techradar. Dostupné z: https://www.techradar.com/pro/security/whatsapp-wins-access-to-nso-groups-pegasus-spyware-code-in-new-court-hearing. [cit. 2024-04-18].

HANSON, Ralph E., 2020. *Mass Comunication: Living in a Media World.* 1. SAGE Publications. ISBN 978-1-5443-8302-6.

HOLMES, Aaron, 2021. *533 Milion Facebook Users‘ Phone Numbers and Personal Data Have Been Leaked Online.* Online. Business insider. Dostupné z: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?amp&. [cit. 2024-04-18].

HRUBÝ, Jan, 2023. *Nová funkce ve WhatsApp zajistí maximální bezpečnost. Jak ji zapnout?* Online. Fonetech. Dostupné z: https://www.fonetech.cz/nova-funkce-ve-whatsapp-zajisti-maximalni-bezpecnost-jak-ji-zapnout/. [cit. 2024-03-28].

CHÁBERA, Jiří; DANHOFEROVÁ, Jana; LAPÁČEK, Jiří; SIMR, Pavel a SÝKOROVÁ, Květuše, 2016. *ECDL Průvodce přípravou na testy.* 1. Brno: Computer Press. ISBN 978-80-251-4761-0.

JAMES, Gilad, 2023. *Introduction to Internet.* 1. Gilad James Mystery School. ISBN 978-4-2104-3125-0.

KILIÁN, Karel, 2023. *Čím nahradit WhatsApp: Vyberte si z 10 alternativních komunikátorů*. Online. Živě. Dostupné z: https://www.zive.cz/clanky/cim-nahradit-whatsapp-vyberte-si-z-10-alternativnich-komunikatoru/sc-3-a-207956/default.aspx#part=6. [cit. 2024-03-28].

KOLOUCH, Jan, 2016. *Cybercrime.* 1. Praha: CZ.NIC. ISBN 978-80-88168-16-4.

KOLOUCH, Jan; BAŠTA, Pavel; KROPÁČOVÁ, Andrea a KUNC, Martin, 2019. *CyberSecurity.* 1. Praha: CZ.NIC. ISBN 978-80-88168-32-4.

Komunikační aplikace s end-to-end šifrováním: současný trh nabízí širokou škálu možností, liší se komfortem, bezpečností a důvěryhodností provozovatele, 2022. PDF. 1.

Koncové šifrování – co to je a proč jej používat?, 2023. Online. Kvalitní internet. Dostupné z: https://www.kvalitni-internet.cz/koncove-sifrovani-co-je-proc-jej-pouzivat. [cit. 2024-02-29].

KUNCOVÁ, Izabela, 2022. *Signal vs. Telegram: Kterou aplikaci zvolit pro šifrované zprávy*. Online. Life24. Dostupné z: https://www.life24.cz/technologie/signal-vs-telegram-kterou-aplikaci-zvolit-pro-sifrovane-zpravy. [cit. 2024-03-28].

Legislativa KB, 2024. Online. Národní úřad pro kybernetickou bezpečnost. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2024-04-12].

LUPONIS, David a BESNARD, Jean-Michel, 2018. *Cambridge Analytica Case: Last Wakeup Call Before GDPR.* Online. Mazars. Dostupné z: https://www.mazars.com/services/consulting/insights/cambridge-analytica-case. [cit. 2024-04-16].

MENEZES, Alfred J.; OORSCHOT, Paul C. a VANSTONE, Scott, 2018. *Handbook of Applied Cryptography.* Boca Raton: CRC Press. ISBN 978-04-29881-32-9.

Messenger As of: 11.03.2024, 2024. Online. Messenger-Matrix. Dostupné z: https://www.messenger-matrix.de/messenger-matrix-en.html. [cit. 2024-01-28].

Meta zavádí end-to-end šifrování pro osobní zprávy a hovory na Messengeru a Facebooku, 2023. Online. Applenovinky. Dostupné z: https://applenovinky.cz/2023/12/meta-zavadi-end-to-end-sifrovani-pro-osobni-zpravy-a-hovory-na-messengeru-a-facebooku/. [cit. 2024-02-29].

MOREAU, Elise, 2021. *Facebook Messenger: Everything You Need to Know*. Online. Lifewire. Dostupné z: https://www.lifewire.com/facebook-messenger-4103719. [cit. 2024-02-21].

Most Popular Global Mobile Messenger Apps as of January 2024, Based on Number of Monthly Active Users, 2024. Online. Statista. Dostupné z: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/. [cit. 2024-03-20].

Národní bezpečnostní úřad, 2024. Online. NBÚ. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/. [cit. 2024-04-12].

Nebuďte naivní. Proč nesmíte v žádném případě používat Messenger?, 2023. Online. Mobilizujeme. Dostupné z: https://mobilizujeme.cz/clanky/nebudte-naivni-proc-nesmite-v-zadnem-pripade-pouzivat-messenger. [cit. 2024-03-28].

Nejzávažnější kybernetické hrozby v EU, 2024. Online. Evropská rada. Dostupné z: https://www.consilium.europa.eu/cs/infographics/cyber-threats-eu/. [cit. 2024-02-24].

Nevěříte Telegramu ani Signalu? Tady jsou komunikační aplikace pro opravdové „privacy freaky", 2021. Online. Lupa.cz. Dostupné z: https://www.lupa.cz/clanky/neverite-telegramu-ani-signalu-tady-jsou-komunikacni-aplikace-pro-opravdove-privacy-freaky/. [cit. 2024-03-24].

NING, Huansheng, 2022. *A Brief History of Cyberspace.* Boca Raton: CRC Press. ISBN 978-1-032-07832-8.

NÚKIB a legislativa, 2021. Online. KYBEZ. Dostupné z: https://kybez.cz/nukib-a-legislativa/. [cit. 2024-02-29].

Ochrana před útoky phishing, 2024. Online. Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44. [cit. 2024-02-29].

OPPLIGER, Rolf, 2014. *Secure Messaging on the Internet.* 1. Boston: Artech House. ISBN 978-1-60807-717-5.

OPPLIGER, Rolf, 2020. *End-to-End Encrypted Messaging.* 1. Boston: Artech House. ISBN 978-1-63081-733-6.

Pět důvodů, proč aktualizovat software, 2019. Online. Portál Digi. Dostupné z: https://portaldigi.cz/5-duvodu-proc-aktualizovat-software/. [cit. 2024-02-29].

Phishing - stále aktuální hrozba, 2015. Online. NÚKIB. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/. [cit. 2024-03-04].

Phishing Activity Trends Reports, 2023. Online. AWPG. Dostupné z: https://apwg.org/trendsreports/. [cit. 2024-02-29].

Phishing, 2024. Online. Eset. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2024-02-29].

Posílejte soukromé zprávy, 2024. Online. WhatsApp. Dostupné z: https://www.whatsapp.com/privacy. [cit. 2024-02-24].

Proč používat službu Signal?, 2024. Online. Signal. Dostupné z: https://signal.org/cs/. [cit. 2024-03-04].

ROCCIA, Thomas, 2023. *Visual Threat Intelligence: An Illustrated Guide For Threat Researchers.* 1. SecurityBreak. ISBN 979-83-73228-37-4.

ROUSE, Margaret, 2023. *What Does Cyberspace Mean?* Online. Techopedia. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace. [cit. 2024-02-24].

Řešení bezpečnostních událostí a incidentů s využitím SOC a IRT, 2022. Online. NGSS. Dostupné z: https://www.ngss.cz/clanek/reseni-bezpecnostnich-udalosti-a-incidentu-s-vyuzitim-soc-a-irt-2022-01-21. [cit. 2024-03-02].

SAYER, Faye. 2015. *Public History.* 1. Londýn: Bloomsbury Publishing. ISBN 978-1-4725-0837-9.

Sdílejte svobodně a soukromě, 2024. Online. Jami. Dostupné z: https://jami.net/#. [cit. 2024-03-19].

Secure Messaging Apps Comparison, 2024. Online. Secure Messaging Apps. Dostupné z: https://www.securemessagingapps.com/. [cit. 2024-03-28].

SHAW, Julia, 2020. Evil: *The Science Behind Humanity´s Dark Side.* Abrams Press. ISBN 978-14-1973-519-6.

Sociální inženýrství, 2016. Online. NÚKIB. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1497-socialni-inzenyrstvi/. [cit. 2024-03-04].

Statista, 2024. Online. Edesiderata. Dostupné z: https://edesiderata.crl.edu/resources/statista#crl-review. [cit. 2024-04-12].

Telegram FAQ, 2024. Online. Telegram. Dostupné z: https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here. [cit. 2024-03-20].

The First E-mail Message of Ray Tomlinson, 2023. Online. History-Computer. Dostupné z: https://history-computer.com/the-first-e-mail-message-of-ray-tomlinson/. [cit. 2024-02-21].

What is malware?, 2024. Online. Malwarebytes. Dostupné z: https://www.malwarebytes.com/malware. [cit. 2024-03-04].

What is Skype?, 2024. Online. Microsoft. Dostupné z: https://www.skype.com/en/about/. [cit. 2024-02-29].

WHITMAN, Michael E. a MATTORD, Herbert J., 2014. *Principles of Information Security.* 1. Boston: Cengage Learning. ISBN 978-1-28544-836-7.

Zákon č. 181/2014 Sb. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* Online. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181. [cit. 2024-03-02].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CIA	Confidentiality, Integrity, Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
GIF	Graphics Interchange Format
IM	Instant Messaging
IT	Informační technologie
NÚKIB	Národní úřad pro kybernetickou bezpečnost
SMS	Short Message Service
TLP	Traffic Light Protocol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK