Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra jazyků

Bakalářská práce

Kybernetické útoky na banky jako hrozba pro hospodářský rozvoj

Otto KLIKAR

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Otto Klikar

Informatika

Název práce

Kybernetické útoky na banky jako hrozba pro hospodářský rozvoj

Název anglicky

Cybercrime in the Banking sector as a Threat to Economic Development

---

Cíle práce

Cílem práce je identifikovat způsoby kybernetických útoků na bankovní instituce a následně jejich dopad na hospodářský rozvoj v České republice. Práce zároveň hodnotí, na základě způsobu a typu útoku, různé způsoby prevence pro zachování bezpečnosti klienta i banky, včetně jejich efektivity.

Metodika

Bakalářská práce bude rozdělena na teoretickou a praktickou část.

V teoretické části budou definovány způsoby, jakými mohou útočníci prostřednictvím počítačů napadat banky a jejich systémy, jakou hrozbu takové útoky představují nejen pro banky, ale i pro jejich klienty, jak se lze proti těmto útokům bránit a jak tato oblast počítačové kriminality ovlivňuje hospodářský rozvoj.

Jako hlavní zdroj informací budou použity odborné publikace zaměřené na kybernetické útoky se zvláštním důrazem na útoky v bankovním sektoru. Kromě literatury a spolehlivých zdrojů na internetu budou použity informace přímo z prostředí bank.

V praktické části práce budou využity rozhovory se zaměstnanci v bankách a dotazníkový průzkum mezi klienty bank ohledně jejich zkušeností s počítačovou kriminalitou v bankách. Součástí šetření bude také vyhodnocení preventivních prostředků využívaných proti kyberútokům.

Doporučený rozsah práce

30 – 40

Klíčová slova

Kyberútoky, banky, bankovnictví, phishing, prevence, krádež, obrana

---

Doporučené zdroje informací

KOLOUCH, J., BAŠTA, p., 2019. P. Cybersecurity. 1. vyd. Praha: CZ.NIC,z.s.p.o., 560s. ISBN 978-80-88168-34-8; 978-80-88168-33-1; 978-80-88168-32-4

KOLOUCH, J., 2016. Cybercrime. 1. vyd. Praha: CZ.NIC,z.s.p.o., 522s. ISBN: 978-80-88168-15-7

Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech. 1. vyd. Praha: Policejní akademie České republiky v Praze. 2020. 328s. ISBN 978-80-7251-505-9

Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka. Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka [online]. Dostupné z: https://www.nukib.cz/cs/

SEDLÁK, P., KONEČNÝ, M., a kol. 2021. Kybernetická (ne)bezpečnost. 1. vyd. Brno: CERM, akademické nakladatelství. 429s. ISBN 978-80-7623-068-2

Úvod | Česká bankovní asociace. Úvod | Česká bankovní asociace [online]. Copyright © [cit. 09.05.2023]. Dostupné z: https://cbaonline.cz/

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Ivan Hrbek

Garantující pracoviště

Katedra jazyků

Elektronicky schváleno dne 12. 6. 2023

PhDr. Mgr. Lenka Kučírková, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 28. 02. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Kybernetické útoky na banky jako hrozba pro hospodářský rozvoj" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 13.03.2024

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu práce panu Ing. Ivanu Hrbkovi, za vstřícný a profesionální přístup, za jeho ochotu pomáhat a poskytovat své zkušenosti dalším a za vřelou atmosféru, kterou se mu během jeho vedení bakalářské práce podařilo vytvořit.

Kybernetické útoky na banky jako hrozba pro hospodářský rozvoj

Abstrakt

Tato bakalářská práce je zaměřena na počítačovou kriminalitu v oblasti bankovnictví. Analyzuje a hodnotí dopady útoků na klienty a jejich vztah k bance, zároveň zkoumá znalosti klientů o nejznámějších typech kyberútoků, jejich reakce na ně a integritu důvěry k jejich bankám. V teoretické části jsou detailně představeny principy fungování útoku typu DDoS a sociálního inženýrství včetně strategií zmírnění obou typů. V praktické části je vyhodnocováno dotazníkové šetření, které se uskutečnilo mezi klienty bank a bylo zaměřeno na zjištění současných vztahů a důvěry klientů k jejich bankám v oblasti kyberbezpečnosti. Kromě zkoumání jejich vztahů a vzájemné interakce byl zjišťován také současný stav znalostí klientů. Důležitým aspektem celé práce je upozornit na zlepšení komunikace mezi klienty a bankami a na budování pevnějších vztahů, které sebou nesou i solidnější a efektivnější vzájemnou informovanost.

Klíčová slova: phishing, DDoS, kyberútoky, prevence, banky, klienti, interakce, bankovnictví, obrana

Cybercrime in the Banking sector as a Threat to Economic Development

Abstract

This bachelor thesis focuses on cybercrime in the banking industry. It analyses and evaluates the impact of attacks on customers and their relationship with their banks, while also examining customers' knowledge of the most well-known types of cyber-attacks, their reactions to them and the integrity of their trust in their banks. The theoretical section details the principles of DDoS attacks and those of social engineering, including mitigation strategies for both types. In the practical part, a questionnaire survey conducted among bank customers is evaluated to determine the current relationship and trust of customers towards their banks in the area of cyber security. In addition to examining their relationships and interactions, the current state of clients' knowledge was also investigated. An important aspect of the whole work is to highlight the improvement of communication between the client and the bank and the building of stronger relationships, which entails more solid and effective mutual information.

Keywords: phishing, DDoS, cyberattacks, prevention, banks, clients, interaction, banking, defense

Obsah

1. Úvod

Kriminalita a zločiny provázejí lidstvo již od nepaměti, možná od dob, kdy si člověk uvědomil, že lze nějaký zločin spáchat. Po uplynutí několika tisíciletí se kriminalita a zločiny přesouvají i mimo fyzický svět, do světa obvodů, polovodičů, optických vláken, čipů, sítí, tedy do světa počítačů.

V počítačovém světě se téměř 100 lidí za jedinou hodinu stane obětí kybernetického útoku, což znamená, že oběť takového útoku se vyskytne přibližně každých 37 sekund.[1]

Takové údaje jsou znepokojivé. Typů útoků je velké množství a s každým rokem způsobů přibývá, stejně tak i četnost útoků, které jsou provedeny. S tímto růstem se každý den úměrně zvyšuje potřeba připravenosti bank i jejích klientů takovým útokům čelit. Cílem se může stát banka i klient. Spolupráce mezi nimi je klíčová pro utlumení útoků a jejich dopadů. Komunikují-li spolu a vzájemně se upozorňují na útoky, ať už se jedná o nové, probíhající či jiné, mohou se varovat a pomáhat tak útoky včas zneškodnit, nebo alespoň omezit škody. V této práci je zjišťováno, jestli klienti nahlašují pokusy o útoky své bance, jestli je sama banka varuje ohledně nebezpečí a je prověřována také důvěra mezi klientem a bankou. Kromě toho je zjišťován stav aktuálních znalostí klientů o způsobech útoků a jejich reakce na případná nebezpečí. Na důvěře klienta a banky stojí celé bankovnictví, které je jedním z hlavních pilířů státní ekonomiky. Pokud je tento vztah narušen, či jinak poškozen, pak taková skutečnost ohrožuje hospodářství, včetně jeho rozvoje.

V této bakalářské práci jsou nejčastější dva typy útoků v oblasti bankovnictví uvedeny v teoretické části a v praktické části je proveden výzkum mezi klienty bank se zaměřením na jejich znalosti a zkušenosti s kybernetickými útoky, dále na analýzu vztahů respondentů a bank a také na jejich současné zkušenosti s prevencí ze strany bank.

2. Cíl práce a metodika

2.1. Cíl

Cílem práce je identifikovat způsoby kybernetických útoků na bankovní instituce a jejich klienty a následně jejich možný dopad na vztah klienta a banky, resp. jeden z nejdůležitějších pilířů ekonomiky, celé bankovnictví. Práce zároveň charakterizuje, na základě typu útoku, různé způsoby prevence, resp. zmírnění útoků. pro zachování bezpečnosti klienta i banky.

2.2. Metodika

Bakalářská práce je rozdělena na teoretickou a praktickou část.

V teoretické části jsou definovány způsoby, jakými mohou útočníci prostřednictvím počítačů napadat banky a jejich klienty, jakou hrozbu takové útoky představují a jak se lze proti těmto útokům bránit. Jsou zde představeny detailněji principy fungování sociálního inženýrství a DDoS útoku. V konečném zhodnocení výsledků a závěru je hodnoceno, jak tato oblast počítačové kriminality ovlivňuje ekonomiku, resp. bankovnictví a jak je důležité budovat vztah mezi bankou a klientem.

V praktické části práce je využit dotazníkový průzkum mezi klienty bank ohledně jejich zkušeností s počítačovou kriminalitou a jejich znalostmi obecně. Součástí šetření je také vyhodnocení preventivních prostředků využívaných proti kyberútokům bankami a komunikace mezi klientem a bankou.

3. Teoretická východiska

3.1. Sociální inženýrství

Množství kybernetických útoků nabývá znepokojujících hodnot. Než aby se útočníci snažili složitě prolomit zabezpečení počítače, je pro ně jednodušší zaútočit na nejslabší článek každé bezpečnostní oblasti – na člověka. Proto je velká část práce věnována právě sociálnímu inženýrství.

Cílem sociálního inženýrství je podvodem vylákat citlivé informace, hesla či přístupy, nebo nechat oběť, aby si sama stáhla škodlivý software na svůj počítač. Sociální inženýrství používá řadu útoků; existuje například phishing (resp. smishing, vishing) nebo scareware. Každá z těchto technik svým určitým způsobem chce dosáhnout poškození oběti, nejčastěji s úmyslem odcizit peníze.

3.2. Phishing

V okamžiku, kdy je snaha nalézt nejrozšířenější způsob kybernetického útoku v oblasti bankovního sektoru, a nejen v tomto sektoru, tak se ve většině případů objeví pojem *phishing*. Tento pojem je spojen s rodinou podobných technik, technik *sociálního inženýrství*, které mají společný cíl: s využitím lidského strachu, chamtivosti, zvědavosti nebo závisti vylákat od důvěřivých uživatelů osobní citlivé informace.[2]

Postup takového útoku bývá většinou běžně známý, ale je tak rafinovaný, že i nadále počty obětí tohoto útoku neklesají – naopak. Útočníci využívají lidské důvěřivosti, mnohdy i neznalosti či nepoučenosti, a vydávají se za důvěryhodné zdroje. Mohou se vydávat za banku a tvrdit, že účet oběti je v ohrožení a naléhat na ni, aby klikla na odkaz, kde zadá své údaje a oni už se o všechno postarají. Mohou se vydávat i za nejlepšího kamaráda, který nutně potřebuje pomoci kliknutím na následující odkaz, nebo za mobilního operátora, který nutně vyžaduje přihlášení na stránkách a další a další lži. Všechny tyto podvodné návnady mají tři společné prvky, totiž naléhavost, podezřelý odkaz a vymáhání citlivých údajů. Kdo si nedá dostatečný pozor, podlehne tlaku a klikne na zaslaný odkaz nebo zadá údaje, dává útočníkovi plnou moc nad svými údaji a útočník s jejich pomocí může vykrást celý bankovní účet, nebo si může na ukradené údaje vzít úvěr.[3]

Mnohdy stačí pouze kliknutí na odkaz, a to zapříčiní stažení škodlivého programu, kterému se říká *malware.* Tomu je věnována kapitola 3.3. Existuje několik druhů phishingu, které jsou v rámci pochopení tohoto širokého pojmu popsány níže.

3.2.1. Spear phishing

Toto je druh phishing útoku, který cílí, jako při vrhání kopím (spear) během bitvy, na určitého konkrétního člověka, na určitý cíl. Tento konkrétní člověk je pro útočníka určitým způsobem zajímavý a výhodný. Útočníkova vybraná oběť má často přístup k velmi citlivým datům. Může se jednat o významně postavenou osobu ve firmě, v bance či jiné organizaci, tedy někoho, kdo zkrátka má přístup tam, kam se nelze normálně dostat.

Útočník sleduje a studuje svou oběť, aby získal potřebné informace k získání maximální důvěryhodnosti v očích oběti. Chce se stát osobou nebo subjektem, kterému oběť důvěřuje. To může být přítel, nadřízený, spolupracovník, nebo finanční instituce, kterou oběť dobře zná.

Po získání dostatečných údajů o oběti může útočník na jejich základě poslat podvrženou zprávu, ve které se vydává za vybranou oběť a s pomocí její odcizené identity se snaží vylákat peníze od jiných zaměstnanců, či dalších spřízněných stran společnosti. Může se jednat například o proplacení falešné faktury.[4]

Jedná o mimořádně nebezpečnou formu útoku, protože útočník si dává opravdu záležet na věrohodnosti a je schopen zjistit informace, které dokáží přesvědčit oběť o útočníkově nepopíratelné důvěryhodné identitě.

3.2.2. Smishing

Jinak také SMS phishing. Největší rozdíl oproti jiným způsobům phishingu je z názvu patrný. Je zde rozdíl v prostředku, v médiu použitém k vylákání citlivých informací z oběti. Lidé dnes s větší pravděpodobností kliknou na odkaz v textové zprávě (SMS, WhatsApp a další) než v e-mailu. Útočníci se mohou vydávat za organizace, ale také mohou ukrást profil na Facebooku a s ukradenou identitou někoho jiného napsat kontaktům oběti či jejím přátelům o pomoc, či jiné informace, opět často i s podezřelým odkazem. Číslo mohou útočníci snadno schovat a lidé jsou od svých bank a jiných firem zvyklí na zkrácené odkazy a k takovému typu komunikace jsou důvěřivější.

Zarážejícím faktem je, že je opět takové množství identit, za které se může podvodník vydávat. Příkladem takové velice podlé identity je identita *přepravce, kurýra*. V praxi takový

podvodník napíše, že došlo k problému s doručovanou zásilkou a je potřeba doplatit jistý poplatek za doručení, kde je uvedeno číslo účtu, či jiný odkaz, který samozřejmě žádnou zásilku neurychlí a oběť pouze přijde o své peníze a čas. Dalším typem falešné identity může být *špatné číslo (wrong number).* V takovém případě dojde oběti SMS zpráva od útočníka. Pokud oběť útočníka upozorní, že se jedná o mýlku a začne komunikaci, útočník se toho chytí a snaží se vytrvale budovat dlouhodobější komunikaci, ve které se chce oběti přiblížit a získat důvěru a přátelství, nebo to dojde tak daleko, že se útočník bude snažit vyvolat romantické pocity a následně žádat finanční výpomoc, nebo něco podobného. Známým případem je americký voják, který po ukončení služby nemá dostatek peněz na živobytí. Může si s obětí domlouvat i schůzky, ale na poslední chvíli záhadným způsobem vždy dojde k převelení.[5]

3.2.3. Vishing

Dalším druhem je voice phishing, zkráceně vishing. V tomto typu útoku už oběť ani nemá čas na promyšlení situace, ověření, zda se jedná o podvod či nikoli, útočník kontaktuje oběť přímo telefonním hovorem. Nemusí se jednat o jediný hovor. Je znepokojující, že nejprve může volat jeden podvodník, vydávat se za banku a z „bezpečnostních“ důvodů naléhavě požadovat převod peněz na účet, který sám označí za bezpečný a toto celé řešení pouze za dočasné. Následně se ozve falešný policista, druhý podvodník, který dosvědčí oběti tuto situaci i z pohledu policie a snaží se tak celé akci dodat více věrohodnosti. Existuje způsob, jak lze napodobit jakékoliv telefonní číslo tak, že oběť skutečně uvěří, že se jedná o jeho banku, firmu či jinou instituci. Takové technice se říká *spoofing*[6].

3.3. Malware

Zkratka pro malicious software, tedy škodlivý software, který má za cíl infikovat zařízení (PC, mobil, notebook) a poškodit nejen infikované zařízení, ale předně jeho uživatele. Cíle malware mohou být různé, ale všechny chtějí uškodit. Cílem může být získání dat, neoprávněného přístupu k citlivým datům, napadnutí nejdůležitějších systémů v organizacích.[9]

Způsob, jakým je tento škodlivý software rozšířen do cílových zařízení, využívá základní principy sociálního inženýrství. Opět se jedná o naléhání a odkaz. Právě kliknutí na nebezpečné odkazy, stahování příloh, zkrátka neopatrné jednání v kyberprostoru je nejčastější příčinou infekce malware. Existuje poměrně velké množství typů malware, a proto je vhodné popsat některé známější druhy.

3.3.1. Ransomware

Cílem ransomware je získání výkupného. Podle výkupného (angl. ransom) je i tento malware pojmenován. Jakmile se tento druh software dostane v počítači ke slovu, začne docházet k samotnému útoku. Ransomware je schopen zašifrovat uživatelská data nebo dokonce znemožnit kompletní přístup k systému. Data jsou zašifrovaná a nelze je tedy správně číst ani do nich jinak zasahovat. V praxi to vypadá tak, že se objeví zpráva s informací o tom, že dešifrování dat proběhne po zaplacení určité částky výkupného na útočníkův účet. Často chtějí útočníci zaplatit v nějaké kryptoměně kvůli zachování anonymity a sledovatelnosti transakce. Zaplacením výkupného nicméně nemá oběť žádnou garanci dešifrování souborů.

Nejvhodnějším prostředkem proti takovým útokům je častá záloha dat a aktualizace záloh tak, aby bylo možné data zrekonstruovat bez nutnosti platit výkupné.

Pro lepší pochopení je k dispozici příklad z reálné organizace, ve které k takovému útoku došlo. Útočník se zřejmě naboural do databáze skrze počítač, který slouží jako vzdálená plocha pro používání určitých druhů nezbytných software, které se v organizaci sdílí. Soubory byly zašifrovány a nebylo možné je otevřít. Jediné, co bylo vidět, byla již zmíněná zpráva o možnosti zaplatit výkupné. Naštěstí se však v takových situacích vedou, nebo by rozhodně měly vést, zálohy dat a je možné celou situaci vyřešit bez placení.[10]

3.3.2. Scareware

Jistě už nespočet uživatelů vidělo podobně naléhavou, červeně blikající zprávu, která vybízí, aby si uživatelé okamžitě stáhli antivirový program, neboť ona nesmyslná zpráva říká, že: „!!!Na vašem zařízení bylo nalezeno 23 virů, kliknutím sem je okamžitě odstraňte!!!“. Vyvinutí tlaku a bezodkladného řešení je zde zcela záměrným a prvořadým cílem, protože útočník nechce, aby uživatel přehodnocoval situaci, zjistil si informace, ale aby rychle jednal a sáhl po zcela jednoduchém řešení na jediné kliknutí. Toto kliknutí povede ke stažení software, který v momentě začne shromažďovat data o oběti. Nepoučeného uživatele může sdělení, citované výše, skutečně vyděsit natolik, že podvodníkům uvěří a nebezpečný program stáhne.[11]

3.3.3. Spyware

Špionážní malware, jak by se to dalo doslovně přeložit do českého jazyka, operuje v infikovaném počítači skrytě, snaží se být nepozorován. Stále je to typ malware, tedy i zde je

hlavní cíl získávat informace a posílat je zpět útočníkovi. Známým typem spyware je tzv. keylogger, který zaznamenává všechny uživatelovy úhozy do klávesnice a umožňuje útočníkovi zjistit hesla a přístupové údaje oběti, která nemá tušení, že něco takového operuje v jejím zařízení.[9] A navíc dokáže sbírat i historii prohlížení stránek, čísla kreditních karet a další zneužitelné údaje. Často bývá ukryt jako součást zdarma stažitelných programů.

3.3.4. Trojský kůň

Podobně jako v Troji, i zde se za zdánlivě neškodným darem, často v podobě freeware, ukrývá bezpečnostní hrozba a nebezpečí, které dokáže způsobit nevýslovné škody. V dnešní době je útočníci ukrývají pod různé programy, hry nebo antivirové programy, které jsou zdarma. Uživatel si stáhne instalační program a ten kromě něj nainstaluje společně s ním malware – Trojského koně. Nicméně pojmem Trojský kůň nemusí být míněn pouze malware, ale obecně každý program, který bez dotázání uživateli nainstaluje na zařízení další, nežádoucí programy. I takové programy lze rozpoznat s trochou pozornosti, zadívá-li se uživatel na příponu souboru. Pokud si někdo stahuje zvukový soubor (např. písničku) a jeho soubor vypadá takto „tvojePisnicka.mp4.exe“, měl by okamžitě zpozornět a nejlépe daný soubor vymazat z paměti počítače.[13] Cílem je opět poškodit zařízení a krádež dat.

3.4. Obrana proti phishingu

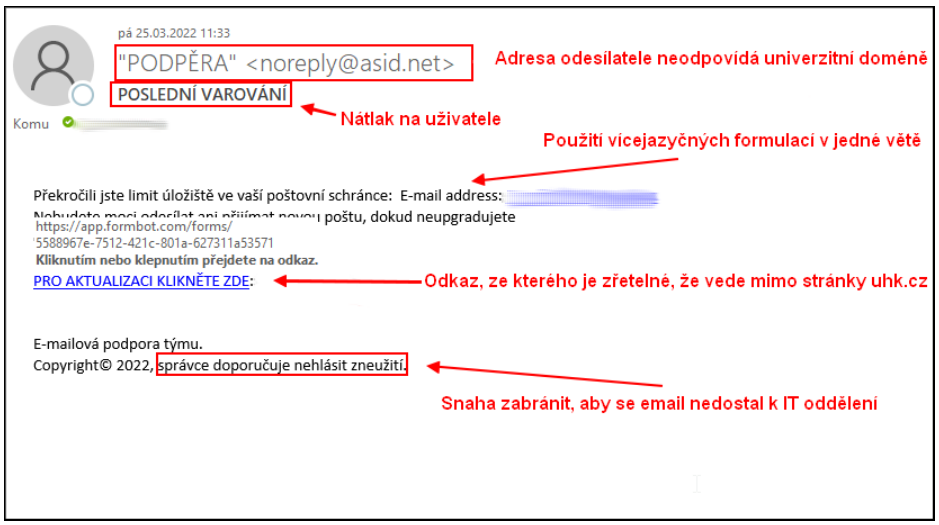
3.4.1. Pečlivé čtení

Již prvním vykřičníkem v takovém podezřelém mailu je jeho předmět a potažmo i adresa odesílatele. Uživatel by neměl email ani otevírat, pokud uvidí velkými písmeny napsáno příkladně následující: „VÁŠ BANKOVNÍ ÚČET BYL NAPADEN!“, „VELKÉ BEZPEČNOSTNÍ RIZIKO“ a jiné. Pokud uživatel e-mail rozklikne, měl by se pořádně věnovat textu podvodníkovy zprávy. Narazí-li na neobvyklá slovní spojení nebo výrazné gramatické chyby, pravděpodobně se jedná o podvod a neměl by s e-mailem dále pracovat. Lidé by si měli povšimnout oslovení a zakončení zprávy. Není obvyklé, aby se někdo podepisoval „webový tým bezpečnosti“, „oddělení univerzity“. Správně by mělo být uvedeno jméno, pozice, nejlépe i nějaký kontakt. Samozřejmě i podpis se dá kvalitně zfalšovat, avšak zbytek obsahu zprávy, případně přílohy, podvodníka prozradí.[14] Kromě gramatických chyb a dalších nesrovnalostí má e-mail často i velice naléhavou povahu.

3.4.2. Odkazy

Mnohokrát bývá součástí podvodných zpráv určitý odkaz. Takové odkazy mohou být podezřelé již na první pohled. Škodlivé odkazy ale nemusí být pouze součástí emailů. Existovala stránka, kde se daly generovat citace online zdrojů, avšak pravděpodobně byla stránka napadena a nyní slouží jako inkubátor k infikování zařízení po kliknutí na odkaz. Podezřelý odkaz je uveden jako příloha 1. Ať už je odkaz nebezpečný nebo ne, v té chvíli je třeba zpozornět a dále raději nepokračovat, neboť odkaz obsahuje velice podezřelou dotazovací část za otazníkem v jeho URL adrese. Avšak jiné odkazy mohou být rafinovanější a rozdíly oproti originálním odkazům mohou být velice nepatrné. Například: „http://www.csob.com/portal/“. Změny zde jsou v protokolu a v doméně. Správný odkaz je „https://www.csob.cz/portal/“.[14] Je potřeba si všímat detailů, protože kliknutí na falešný odkaz může mít katastrofální důsledky. Pokud i přes to uživatel klikne na upravený odkaz, stránka může vypadat zcela jako kopie oficiálních stránek ČSOB, nicméně mohou zde být políčka navíc či jiné nesrovnalosti. Podvodná stránka ale požaduje totéž jako oficiální stránka, totiž přihlášení a zadání údajů. I zde se mohou stránky lišit v maličkostech a je třeba dbát na detaily. Někdy však ani nejvyšší pozornost nemůže pomoci, jako v případě BGP hijackingu, což je typ útoku, kdy je internetový provoz přesměrován k útočníkovi a tváří se jako zcela legitimní oficiální stránka. Ať se uživatel rozhodne jakkoliv, první krok by měl být vyhledání oficiálních stránek jeho banky a nalezení oficiálního telefonního čísla, na kterém si uživatel potvrdí informace sdělené v obdrženém e-mailu. Příklad takového podvodného e-mailu (ad absurdum) s pochybným odkazem je uveden jako obrázek č.1.

Obrázek č.1 – Prvky phishingového e-mailu



Zdroj: UHK (2022)

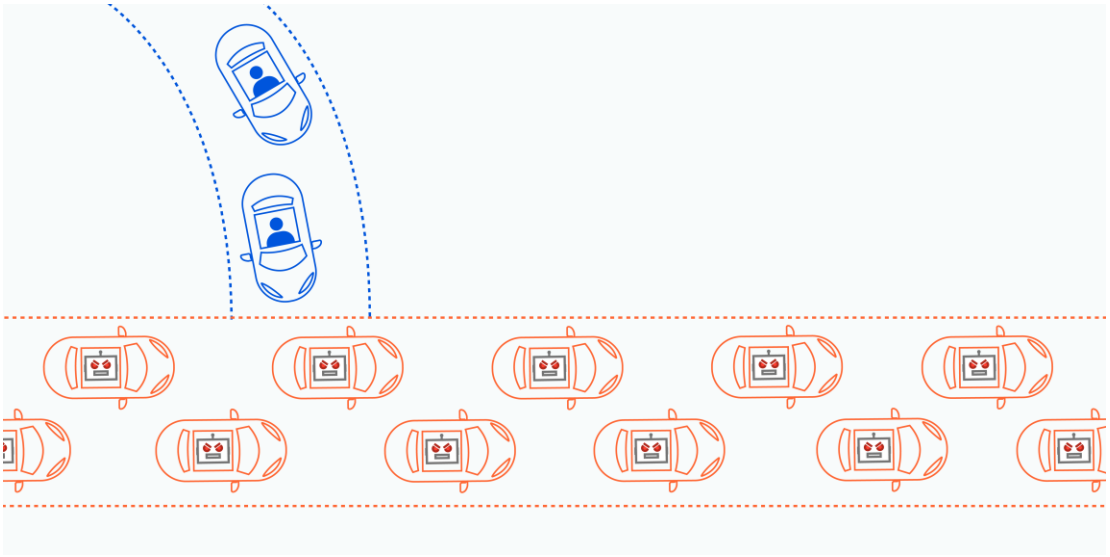
3.4.3. Neklikat

Ať už se e-mail jeví jako důvěryhodný či útočník vyhrožuje čímkoliv, nemůže dosáhnout ničeho, pokud uživatel nebude ochoten kliknout na žádný odkaz ani stáhnout jakoukoliv přílohu. Snahou útočníka je přinutit svou přesvědčivou falešnou rolí a svým naléháním oběť, aby mu na jeho odkazech poskytla své údaje. Pokud si uživatel není jistý, neměl by klikat na nic a ani neodpovídat na žádný pokus o komunikaci. Žádná organizace bezdůvodně nevyvíjí takový nátlak na kliknutí na odkaz, stažení přílohy či zadání svých údajů.

3.5. Distributed denial-of-service-DDoS

Do českého jazyka se DDoS útok dá přeložit jako „distribuované odmítnutí služby“. Klíčovým slovem v této zkratce je slovo „distributed“, které říká, že útok je prováděn přes celou síť infikovaných zařízení a takové síti se říká botnet. Pokud je útok prováděn pouze jedním zařízením, pak se používá zkratka DoS (Denial-of-Service). tedy odepření, nebo odmítnutí služby. Tato práce se věnuje distribuovanému útoku, tedy je dále používán pouze název DDoS Cílem takového útoku je odepřít požadovanou službu běžným legitimním uživatelům. Záměry útočníků provádějících tento útok mohou být rozličné. Může se jednat o vydírání za účelem zisku, politické motivy, odlákání od jiného útoku, kdy DDoS útok je jen prostředek k upoutání pozornosti od jiného hlavního útoku, aktivismus a spoustu dalších. Útočník chce narušit běžný provoz cílového serveru nebo cílové služby.[15] Takový útok by se dal přirovnat k dopravní zácpě na hlavní silnici, kdy auta stojící v koloně (spousta nežádoucích požadavků na serveru) blokují silnici a běžné požadavky z vedlejší silnice jsou zpomaleny, nebo úplně zastaveny a nemohou se dostat do cíle.[16] Ilustrační foto takové situace je označeno jako obrázek č. 2.

Obrázek č.2 - DDoS útok jako automobilová doprava



Zdroj: Cloudflare (2023)

V bankovním sektoru je tento typ útoku dobře znám. Během rozsáhlých útoků v září 2023 nešlo o poškození klientů, ukradení dat či peněz, ale o znepřístupnění webových stránek a internetového bankovnictví, kdy právě legitimní uživatelé v návaznosti na tento útok neměli možnost tyto bankovní služby používat. Podle Lukáše Kintra, ředitele Národního úřadu pro kybernetickou a informační bezpečnost, je jediný zásadní dopad DDoS útoku znemožnění běžného používání služeb poskytovaných bankou. Bezpečnost uložených prostředků nebo osobních údajů nemá útočník šanci tímto útokem jakkoliv narušit.[18]

3.5.1. Botnet

Východiskem pro pochopení distribuovaného DoS útoku je správné pochopení termínu Botnet. Jak bylo již zmíněno, tak tento útok používá síť infikovaných zařízení k zahlcení cíle (cílový server) velkým množstvím požadavků, které vychází ze stovek, tisíců, někdy i milionů infikovaných zařízení, a právě takovou síť označuje termín botnet. Záměrně je použit výraz zařízení, protože se nemusí jednat jen o běžné počítače, ale jakákoliv SMART zařízení, například televize nebo router, nebo také IoT zařízení. [17]

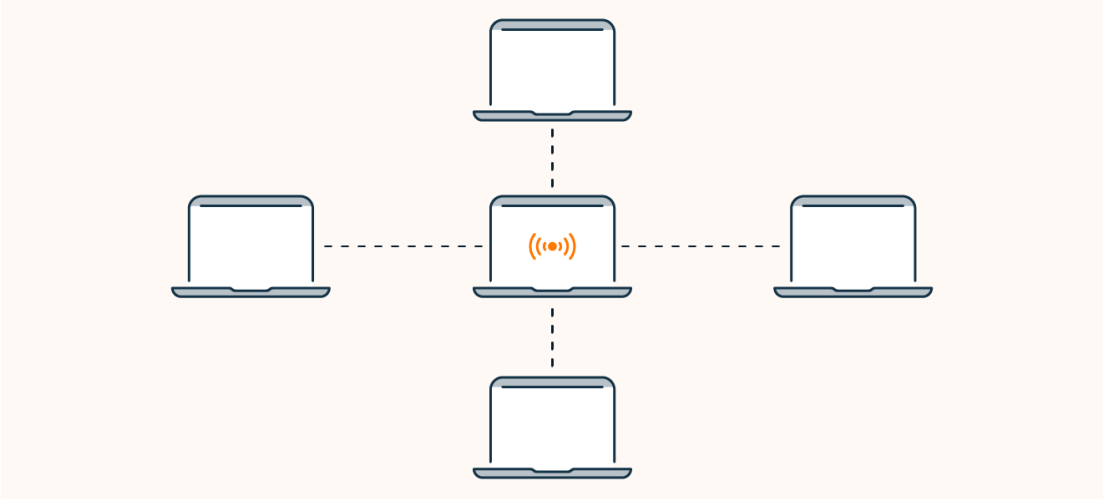
Zařízení, která mají být pro útok použita, musí být infikována a aby mohla být infikována, tak útočník provádí samotnou infikaci v zásadě ve třech krocích. Prvním je infikovat zařízení oběti, druhým pak rozšíření sítě a posledním krokem aktivace sítě a zahájení útoku. Síť infikovaných zařízení, jinak také „the zombie computer“, musí být nejprve rozhozena, vytvořena. Při prvním kroku je nutné přenést malware na zařízení oběti

(možnosti přenesení malware analyzuje následující podkapitola). Často se používají metody sociálního inženýrství, kdy je za použití phishingu cílem dovést uživatele k tomu, aby si stáhl a nainstaloval škodlivý software. Dalším způsobem může být forma Trojského koně, kdy se v nějakém freeware skrývá malware. Druhým krokem je rozšiřování sítě, kdy malware může být nastaven tak, aby byl schopen se sám šířit po síti a infikovat další zařízení. V momentě, kdy botnet dosáhne požadované velikosti, může být infikovaná síť aktivována a použita pro útok, nejen pro útoky typu DDoS, ale příkladně také pro těžbu kryptoměn.[19]

Když se řekne, že botnet je síť infikovaných zařízení, téměř to nevypovídá o možnostech, které útočník úspěšnou infikací zařízení získává. Takových možností je více. Infikovaný zombie computer, který by nebyl schopen určitých rozšířených akcí, by byl pro útočníka příliš nevýhodným nástrojem, aby ho stál za riziko odnětí svobody. Nakažené zařízení má možnost číst a upravovat systémová data. Může data přepsat a vložit nová data, ale i pouhé čtení by stačilo na způsobení škody, jelikož i minimální funkce čtení by mohla být příčinou úniku citlivých osobních dat. Pokud by to bylo pro útočníka výhodné, může také sledovat uživatelské akce a zjišťovat, co uživatel dělá. Další funkce zombie počítače souvisí s druhým krokem šíření botnetu, kdy jeden zombie počítač dokáže skrze síť, ve které se nachází, vyhledávat další potenciálně infikovatelná zařízení.[19]

Většina infikovaných sítí se z pohledu možnosti kontroly takové sítě dají rozdělit na dvě kategorie, kdy síť zařízení je řízena buď centralizovaně či decentralizovaně. Centralizovaná kontrola probíhá na základě modelu klient-server, kdy klientem je infikované zařízení a serverem je centrální bod, který se nazývá C&C (někdy nazývaný C2) server neboli Command-and-Control server, přeloženo jako řídící a kontrolní server. Takový server slouží jako centrální bod komunikace mezi útočníkem a botnetem, kdy tento server může přijímat příkazy od útočníka a odesílat je na infikovaná zařízení. Mimo přijímání a vydávání rozkazů umožňuje server také přenos dat, kdy taková data mohou obsahovat informace o stavu botnetu nebo výsledky útoků. C&C server má nevýhodu v tom, že může být snadno nalezen a deaktivován a vzhledem ke své centralizované povaze má zneškodnění C&C serveru za následek přerušení komunikace útočníka s botnetem. I v případě použití více C2 serverů není útočník zcela chráněn proti odhalení, protože kyberbezpečnostní týmy dokáží vysledovat při analýze sítě i více serverů najednou a tuto snahu útočníka o zvýšení ochrany sítě utnout.

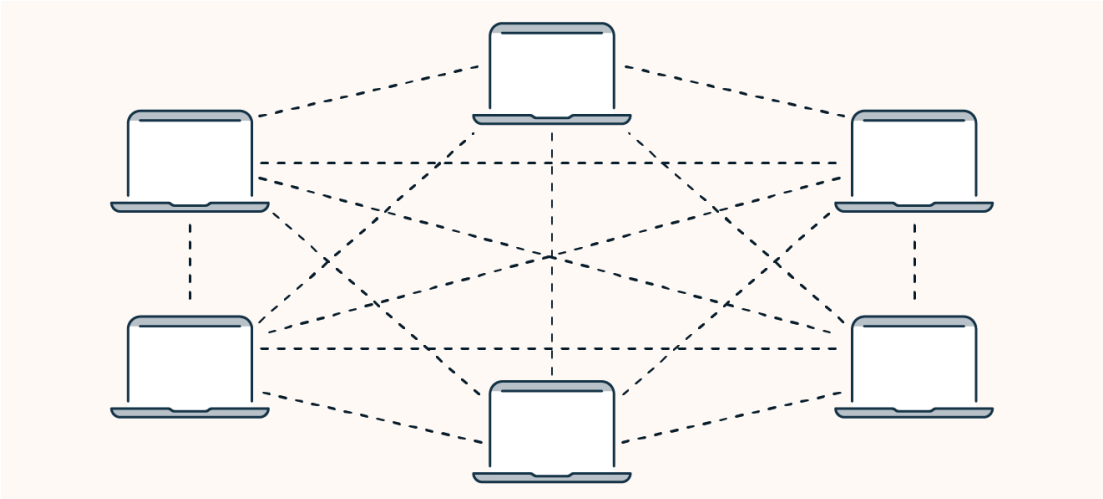
Obrázek č.3 - Centralizovaná kontrola botnetu



Zdroj:Avast (2021)

Další možností kontroly sítě je decentralizovaný způsob, který odhalení oproti centralizovanému způsobu značně stěžuje. Tento způsob funguje na principu P2P neboli peer-to-peer modelu, který využívá toho, že každé infikované zařízení může komunikovat s jiným a žádné zařízení není tím centrálním, které by bylo možné zneškodnit. Komunikace probíhá napříč celou sítí. V porovnání s klient-server botnety jsou P2P botnety nepoměrně nebezpečnějším soupeřem pro kyberbezpečnostní týmy. Vizuálně zobrazenou centralizovanou kontrolu zobrazuje obrázek č. 3 a decentralizovanou obrázek č.4.

Obrázek č.4 – Decentralizovaná kontrola botnetu

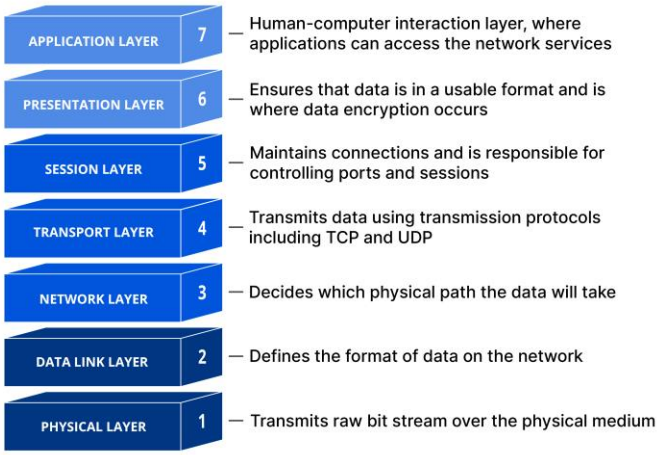


Zdroj: Avast (2021)

3.5.2. Typy útoků DDoS

Útoky typu DDoS mohou mít různé podoby v závislosti na výběru cílové vrstvy v síťovém ISO modelu. Porozumění stavbě síťového připojení se podobá (konkrétně u vrstvového modelu ISO/OSI) stavění budovy odspoda vzhůru, kdy každé patro, každá vrstva, zajišťuje svou úlohu, aby mohla proběhnout kvalitní a úspěšná komunikace. Grafická podoba s vysvětlením ISO modelu je uvedena na obrázku č. 5. Útoky mohou být rozděleny do 3 kategorií, kterými jsou útoky na aplikační vrstvě, protokolové útoky a volumetrické útoky.[16]

Obrázek č.5 – ISO/OSI vrstový model



Zdroj: Cloudflare (2023)

3.5.3. Útoky na aplikační vrstvě

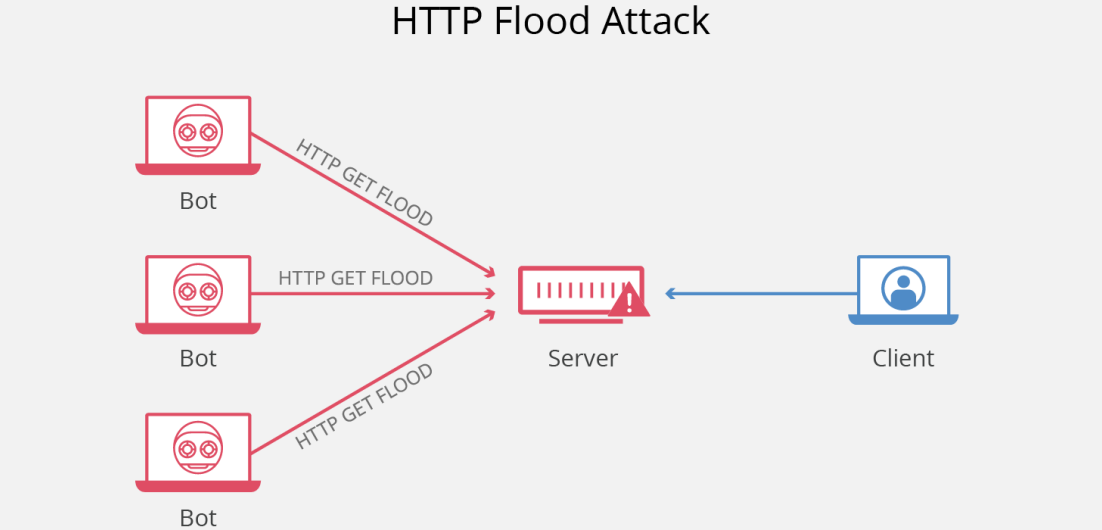
Někdy jsou nazývány také layer 7 DDoS útoky, protože tento útok cílí na nejvyšší vrstvu v ISO modelu, která už je viditelná uživateli a zajišťuje konečnou interakci mezi člověkem a zařízením. Cílem takového útoku je vyčerpat zdroje napadeného zařízení a znemožnit tak běžné fungování služby. Útoky jsou zaměřeny na vrstvu, ve které na serverech dochází ke zpracování a generování webových stránek a tyto webové stránky jsou zobrazeny u klienta jako odpověď na požadavky HTTP protokolu, který v aplikační vrstvě odpovídá za načítání obsahu webových stránek (běžné požadavky jako jsou GET a POST)[20]. Provedení požadavku ze strany klienta na načtení stránky není nijak výpočetně náročné, avšak poskytnutí odpovědi ze strany serveru už může být daleko náročnější. Zvláště když se vezme v úvahu, že takový server musí často načítat několik souborů a databáze, provést databázové

dotazy a načíst API, aby se webová stránka mohla správně zobrazit a být bez problémů používána. Obrana proti takovému typu útoku je obtížná, jelikož je nesnadné odlišit od sebe běžný provoz a útočnou snahu, jako je tomu například u útoku na aplikační vrstvu, kterému se říká HTTP Flood neboli HTTP záplava.[16] [20]

3.5.4. HTTP Flood

Účelem HTTP Flood, jak již bylo řečeno, je zahlcení cílového serveru velkým množstvím požadavků, aby tak došlo ke znemožnění běžného provozu a tím odepření možnosti používat služby serveru běžným uživatelům. Aby útočník mohl zvýšit své šance na úspěšné vyřazení serveru, je téměř jisté, že nebude používat jediné zařízení, ale použije síť infikovaných zařízení (princip je vysvětlen v kapitole 3.5.1). Použitím botnetu může útočník zmnohonásobit počet požadavků zahlcující server. Útoky HTTP Flood lze rozdělit na dvě možné varianty; jednou z nich je HTTP GET útok a druhou HTTP POST útok. Již z názvu těchto variant útoků je patrné, jakým způsobem se útočník snaží přehltit server. V případě HTTP GET útoku je botnet koordinován tak, aby posílal velké množství požadavků na obrázky, videa nebo jiné soubory a prostředky cílového serveru. Při útoku typu HTTP POST je možné uvést jako příklad odesílání formuláře, kdy server musí zpracovat příchozí požadavek a uložit příchozí data do databáze. Ve srovnání s odesláním požadavku POST je zpracování dat z formuláře a volání příslušných databázových dotazů ve srovnání s množstvím výpočetního výkonu a šířkou pásma nepoměrně náročnější. Právě takový nepoměr ve výpočetní a energetické spotřebě je využíván jako hlavní opěrný bod tohoto útoku, protože je možné bez větší zátěže na straně útočníka posílat tak velké množství požadavků, že se cílový server se s každým dalším požadavkem začíná přehlcovat, až nakonec zcela vypoví službu všem legitimním uživatelům. Rozdělení útoku na tyto dvě varianty neznamená neprostupnou zeď. Útočník může použít i metodu hybridního útoku, kdy kombinuje oba útoky zároveň a využívá slabin v serverové infrastruktuře.[20] [21] Vizualizace útoku typu GET je znázorněna na obrázku č.6.

Obrázek č.6 - HTTP Flood (typ GET) útok



Zdroj: Cloudflare (2023)

Jednou z možných metod, jak zmírnit útoky na aplikační vrstvu, či jim zabránit, je otestovat zařízení, ze kterého přichází požadavek, jestli se jedná o bota, či nikoliv. Takový test by se dal přirovnat k testu CAPTCHA, který se snaží prověřit, zda se nejedná o bota. Pokud se takové testování implementuje, lze dopad útoku značně zmírnit. Dalšími možnostmi zmírnění útoku jsou použití brány firewall pro webové aplikace, správa a filtrování provozu prostřednictvím databáze reputací IP adres a další podobně zaměřené metody. Cílem je odlišit zmiňované boty od legitimních požadavků a klíčovým prvkem pro zmírnění útoků je právě umění odlišit je od sebe. [20]

3.5.5. Protokolové útoky

Na rozdíl od útoků na aplikační vrstvy a volumetrických útoků se protokolové útoky snaží najít slabá místa v internetových komunikačních protokolech. Tyto jsou dnes používány celosvětově a jejich změna, snaha o úpravu a následné zavádění je komplikované a pomalé, právě vzhledem k mohutnosti jejich používání. U mnoha protokolů jejich přirozená komplexnost znamená, že i když jsou nakonfigurovány tak, aby byly odstraněny stávající nedostatky, mohou se často objevit nové slabiny, které umožňují útočníkům využít nové slabiny a použít tak nové typy útoků.[22] Příkladem protokolového útoku je například SYN Flood.

3.5.6. SYN Flood

Typ protokolového útoku SYN Flood (Synchronize Sequence Number) využívá tzv. handshake procesu TCP připojení a může se vyskytovat ve 3 podobách.[27] Jak tomu je ale u všech útoků, je nejprve nutné pochopit určité procesy, kterých takové útoky využívají a pak je teprve možné popsat samotnou proceduru útoku.

TCP je zkratka pro Transmission Control Protocol (protokol řízení přenosu), z čehož vyplývá, že tento protokol zajišťuje spolehlivou kontrolu nad přenosem dat. V současné době probíhá komunikace mezi zařízeními na internetu prostřednictvím modelu TCP/IP (model TCP/IP je "ořezaná" verze modelu OSI), kde i zde máme aplikační vrstvu, odkud aplikace, jako jsou webové prohlížeče, navazují spojení se serverem. Informace z aplikační vrstvy pak dále postupují do transportní vrstvy, na jejíž úrovni se aplikují útoky SYN flood.

V transportní vrstvě se nachází právě protokol TCP a také protokol UDP (User Datagram Protocol). TCP zajišťuje spolehlivost přenosu a UDP se uplatní při dotazování serveru DNS na doménové jméno. TCP handshake probíhá ve třech krocích.[28] Prvním krokem je snaha o navázání spojení klienta se serverem. Klient odesílá paket SYN, který informuje server o tom, že si klient přeje zahájit komunikaci se serverem a jaké pořadové číslo pakety mají.[28] Při druhém kroku server odpoví na požadavek klienta tím, že nastaví signální bity u paketu SYN-ACK. ACK, acknowledgement, potvrzení, je odpověď na přijatý paket od klienta a část SYN dává klientovi informaci, s jakými pořadovými čísly bude komunikace zahájena.[28]

V posledním kroku klient potvrdí serveru vysláním ACK paketu, že je připraven a že může být navázáno spojení a následný přenos dat mezi klientem a serverem. Po dokončení této sekvence je TCP spojení otevřené a komunikace může začít.[27] [28]

Jádro a princip celého útoku spočívá v druhém kroku během TCP handshake procesu, kdy útočník využije toho, že server pošle zpět SYN/ACK paket, nechá otevřený port a čeká, až mu přijde ACK potvrzovací paket od klienta, kterého se však ze strany útočníka nikdy nedočká. Útočník záměrně posílá na cílový server velké množství SYN paketů, často pod falešnými IP adresami, a zahajuje tak mnohonásobný počet TCP handshake procesů. Server odpovídá na každý tento paket, nechá otevřený port a očekává odpověď od klienta, která mu nikdy nedorazí. Útočník mezitím posílá další a další požadavky na server s cílem dosáhnout takového stavu, kdy jsou všechny dostupné porty využity a dojde k úplnému přehlcení cílového serveru. Podoby tohoto útoku lze přibližně rozdělit do tří kategorií. Jejich rozdělení

spočívá v tom, je-li IP adresa falšovaná, či nikoliv a provádí-li útok jedno, či více zařízení. První kategorií je přímý útok, kdy útočník nemaskuje svou IP adresu, a je velice snadné odhalit škodlivé zařízení a útok poměrně snadno zneškodnit. Při dnešních možnostech obrany je tento typ útoku už nepoužitelný. Spoofed IP útok představuje druhou kategorii, kdy IP adresa útočícího zařízení je falšována při každém odeslaném SYN paketu. Vystopovat zdroj útoků není nemožné ani u tohoto způsobu, zejména pokud jsou ochotni pomoci poskytovatelé internetových služeb. Poslední kategorií je distribuovaný útok, kdy posílání SYN paketů provádí botnet.[27]

Existuje více způsobů obrany proti SYN Flood, avšak uvedeny jsou jen tři nejznámější. První možný způsob obrany je zvyšování backlog zásobníku, kam se serveru ukládají ony nedokončené požadavky od útočníka. Cílem útočníka je serveru vyčerpat jeho zdroje. Dalo by se soudit, že navýšení zásobníku pro zpracování většího počtu požadavků je neefektivní, avšak i tento způsob se dá použít, protože pro vlastníka napadeného serveru je stále lepší, aby byl server pouze zpomalen a tlak nakonec ustál než aby se služba zhroutila úplně.[27] Další možností je recyklace nedokončených požadavků, kdy server přepisuje nejstarší nedokončené spojení. Tato strategie však vyžaduje, aby legitimní spojení byla navázána dříve, než se server zahltí SYN pakety a taková situace může, ale nemusí nastat.[27] Třetí možností jsou soubory SYN cookies. Server si vytvoří soubory cookies. Aby se předešlo selhání spojení při zaplnění zásobníku serveru požadavky, tak server na počáteční SYN paket od klienta odpoví ACK-SYN paketem, avšak požadavek SYN si uloží do vytvořených cookies souborů a nechá daný port otevřený a připravený pro další komunikaci. Jedná-li se o legitimní požadavek na spojení a přijde-li serveru odpověď ACK, pak z cookies souborů je server schopen původní SYN paket zrekonstruovat a legitimní spojení navázat.[27]

3.5.7. Volumetrické útoky

Zatímco předchozí dva typy útoků se zaměřují na konkrétní slabiny v protokolech a vrstvách internetových sítí, tento typ útoku se snaží využít všechny zdroje, co útočník má, aby vysláním masivního množství škodlivých požadavků zahltil kapacity sítě u oběti. Útok takového rozsahu může přetížit i zařízení speciálně určená na odchycení provozu DDoS útoku. Cíl útočníka je jasný: využít a maximálně spotřebovat šířku pásma (bandwidth, což jest rozsah v bitech/kilobitech/megabitech za sekundu, který odkazuje na množství dat, které může být za určitý časový úsek přeneseno přes určitý komunikační kanál).[29] Jako příklad

volumetrického útoku poslouží DNS Amplification, který využívá otevřených DNS resolverů, aby zahltil server a jeho okolní infrastrukturu.

3.5.8. DNS Amplification

Tento útok je kategorizován jako amplifikační volumetrický útok, využívající rozdílné spotřeby šířky pásma útočníka a cíle, na které se má útočit.[30] Při útoku tohoto typu se využívá veřejně přístupných DNS serverů k zahlcení systému oběti přenosem odpovědí DNS. Princip útoku je takový, že útočník odešle UDP požadavek DNS serveru na překlad doménového jména na odpovídající IP adresu (tzv. DNS name lookup request) s tím, že uvedená zdrojová adresa pro překlad není útočníka, ale cíle útoku. Když DNS odpoví, tak svou odpověď pošle na server oběti, a ne útočníkovi. Útočníci pošlou co nejvíce možných požadavků, aby maximalizovali amplifikující, zesilující efekt tohoto útoku. Při většině útoků tohoto typu, které zaznamenal US-CERT (Jednotka pro nouzovou počítačovou pohotovost Spojených států), jsou dotazy nejčastěji typu ANY, který vrací všechny známé informace o DNS zóně (soubor všech DNS záznamů pro danou doménu). Jelikož velikost odpovědi je podstatně větší (to je cíl dotazu ANY, tedy dostat co největší možnou odpověď) než velikost požadavku, útočník může touto nerovnováhou výrazně zvýšit provoz těchto velikých odpovědí na server oběti. Útočník s velkou pravděpodobností využije botnet, aby byla velikost útoku co největší a mohl posílat co nejvíce podvržených DNS požadavků. I přes to, že se jedná o požadavky z legitimních serverů a tyto útoky je obtížné odfiltrovat, existuje několik strategií zmírnění útoků.[31]

Vzhledem k širokému rozsahu a síle takových útoků může oběť jen málokdy zabránit odepření služby. Existují však způsoby, které mohou i takový útok výrazně zmírnit. Prvním z nich je ověřování zdroje IP adresy. Při těchto útocích je IP adresa, ze které odchází DNS dotazy, podvržená tak, aby se tvářila jako adresa oběti. První krok k zmírnění by měl přijít od poskytovatelů internetových služeb. Pracovní skupina Network Working Group of the Internet Engineering Task Force v březnu roku 2004 (aktualizováno v roce 2020 [32]) vydala dokument Best Current Practice 84, ve kterém jsou popsány metody pro internetové poskytovatele, jak efektivně filtrovat síťový provoz tak, aby odmítal pakety se zdrojovými adresami, které nejsou zpětně dosažitelné přes skutečnou cestu paketu. Konfigurace doporučená v tomto dokumentu způsobí, že směrovací zařízení vyhodnotí u každého DNS requestu, zda je možné dosáhnout zdrojové adresy paketu skrze rozhraní, přes které se paket přenesl. Pokud by nebylo možné dosáhnout zdrojové adresy, pak by to znamenalo, že se

pravděpodobně jedná o podvrženou IP adresu. Proto se všem poskytovatelům sítě doporučuje, aby prováděli filtrování vstupu do sítě.[30] [31] Dalším možným způsobem je snížení počtu otevřených DNS serverů. Otevřený DNS server, respektive jeho nalezení, je základní součást DNS amplifikace. Odpovídají-li DNS servery komukoliv z internetu, pak jsou snadno zneužitelné. Pokud útočník špatně nakonfigurovaný otevřený DNS server nalezne, nic mu nebrání v jeho využití. Tomu lze předejít tak, že jsou DNS servery přístupné pouze v rámci důvěryhodné domény. S takovým omezením se pak stává DNS server špatným prostředkem pro útok.[31]

3.5.9. Obecné strategie zmírnění DDoS útoků

Když se hovoří o obranné strategii proti jakémukoliv typu DDoS útoku, všechny obranné strategie se téměř vždy potýkají se stejným problémem, kterým je rozlišení mezi běžným a útočným provozem. Když se například na webových stránkách objeví dlouho očekávaný produkt a stránku zaplaví dychtiví zákazníci, byla by chyba určitým automatismem odříznout takové množství požadavků ze spousty důvodů, ať marketingových či finančních, nicméně i takové situace mohou útočníci využít, a proto je obtížné určit, o jaký druh provozu se jedná. V dnešní době se často používá i více-vektorový DDoS útok, který využívá více cest a více způsobů, aby zahltil cíl, a tak se opět více komplikuje možnost zmírnění útoku. Cílem útočníka je splynout s běžným provozem a neupozorňovat na sebe; strategie utínat bez rozmyslu nevybíravě přicházející požadavky zase může omezovat prospěšný provoz a útokům to zabránit nemusí. Avšak není žádoucí nechat útočníkům žádnou výhodu, a proto existují kromě již zmíněných strategií zmírnění na jednotlivé typy útoků také obecně možné postupy a strategie prevence proti DDoS útokům.[16]

3.5.10. Blackhole routing

Lze volně přeložit jako směrování do černých děr. Tato strategie představuje protiopatření používané proti DDoS útokům. Při použití této strategie je internetový provoz směřován do jakési černé díry, kterou představuje imaginární místo v síti, kam jsou nežádoucí pakety směřovány. Je nezbytné, aby tato strategie byla provedena s určitou filtrací, jinak by mohlo docházet k zahazování i legitimního provozu. Proto je potřeba na klíčových routerech nastavit příslušné filtrování a doufat, že útočník nebude využívat proměnlivé IP adresy a měnit strategii útoku. Tento způsob obrany se hodí v případě, že na jiné možnosti nejsou prostředky a je správně nakonfigurován router, protože jinak mohou být důsledky vážné.[33]

3.5.11. Rate limiting

Rate limiting je technika, která omezuje síťový provoz, aby uživatelé nebyli schopni vyčerpávat systémové prostředky. Použitím rate limiting je možné omezit nebo dočasně zablokovat příliš mnoho požadavků, které přicházejí z celého internetového prostoru. Pokud se podaří zpomalit či zcela odmítnout požadavky omezovaného uživatele, pak je možné dát průchod legitimním požadavkům a neohrozit chod aplikace. Podstatné je, že rate limiting funguje uvnitř aplikací, nikoliv na webovém serveru, a zahrnuje sledování IP adres, ze kterých přichází požadavky a také dobu, která mezi jednotlivými požadavky uplynula. Sledování IP adres je hlavní způsob, jak je aplikace schopna identifikovat, kdo jednotlivé požadavky poslal. Tato identifikace je velmi užitečná v následném procesu omezování příchozích požadavků. Rate limiting neustále měří dobu mezi příchozími požadavky z dané IP adresy. Pokud tedy daná IP adresa za určitý časový úsek provede příliš mnoho požadavků, pak rate limiting tuto adresu zablokuje a další požadavky z této adresy nebudou dále vyřizovány. Aby se zabránilo nedopatřením, aplikace používající rate limiting uživatele nejprve upozorní na to, že zadávají příliš mnoho požadavků a nedojde-li ke změně, dochází k zablokování. [35]

3.5.12. Anycast síť

Anycast je metoda síťového adresování a směrování, při níž mohou být příchozí požadavky směrovány do různých uzlů a do různých lokací. Příchozí provoz je obvykle směrován do nejbližšího datového centra s takovou kapacitou, která zajistí efektivní zpracovaní příchozích požadavků. Selektivní směrování sítě Anycast, nutně v kombinaci s dalšími filtry a prostředky, dokáže odolat vůči velkému objemu internetového provozu a snaze o přetížení sítě DoS útoky. Pokud by se někdo snažil přetížit původní server velkým množstvím požadavků, v síti Anycast je možné takovou zátěž rozdělit mezi další dostupná datová centra, kde každé z nich bude mít servery schopné zpracovat příchozí požadavky a odpovědět na ně. Poté, co ostatní nástroje pro zmírnění útoku odfiltrují část útočného provozu, síť Anycast dokáže zbývající útočný provoz rozdělit do více míst, do více datových center, čímž zabrání přehlcení jednoho místa. Pokud je kapacita Anycast sítě dostatečná, mohou být útoky účinně zmírněny. [36]

4. Praktická část práce

4.1. Metoda sběru dat

Za účelem získání dat od klientů bank bylo zvolena metoda ve formě dotazníkového šetření v nástroji Google Forms. Vzhledem k tématu bakalářské práce byl dotazník zaměřen na klienty bank a jejich zkušenosti s kybernetickými útoky, jejich znalosti v oblasti kyberbezpečnosti, prevence a osobní zkušenosti. Otázky jsou rozděleny do pěti sekcí. V první sekci jsou zjišťovány základní informace o respondentech, jako je věk, pohlaví a jiné. V druhé sekci jsou respondenti dotazováni na základní znalosti v kyberbezpečnosti. V třetí a čtvrté sekci jsou otázky konkretizovány na sociální inženýrství, konkrétně phishingový útok a DDoS útoky a poslední sekce se týká prevence, kterou banky aplikují, aby minimalizovaly počet obětí kybernetických útoků.

Sběr dat se uskutečnil od 26.2.2024 do 02.03.2024, kdy během této doby bylo obdrženo 93 odpovědí. Respondenti byli seznámeni s účelem dotazníku, jakož i se zachováním anonymity a zároveň byli požádáni o pravdivé a čestné vyplnění, nicméně nepravdivé odpovědi nelze vyloučit.

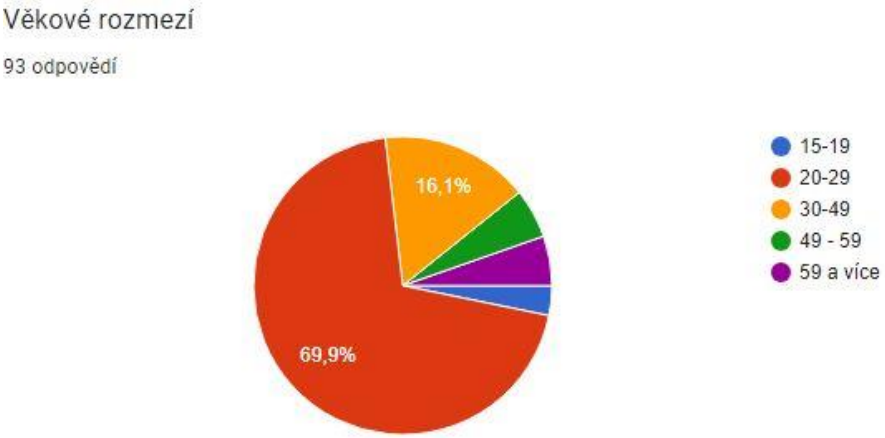
4.2. Cíl výzkumu

Smyslem celého dotazníku bylo zjistit, jakými znalostmi klienti bank disponují, jak se chovají v situacích spojených s kyberútoky, jak je jim sdělována prevence, jak moc jsou obeznámeni s pojmy Phishing a DDoS a konečně dopad kybernetických útoků na vztah klienta a banky. Vztah klienta a banky je pro hospodářský rozvoj velice důležitý. Více než sedm bank v současné době eviduje více než milion klientů.[36] To je jen spodní hranice a jen ta v součtu dává sedm milionů. Důvěra v banky tak masivního počtu lidí a jejich vztah k nim jsou důležitými prvky v ekonomice, které musí setrvat stabilní. Pokud by byla důvěra skrze kybernetické útoky narušena, důsledky by mohly být nepředstavitelné. Banky poskytují finanční služby a dávají možnosti investic do podnikání a infrastruktury a jsou důležitým ekonomickým pilířem. Kdyby klienti kvůli trvalejšímu pocitu ohrožení v kyberprostoru začali ztrácet ve větší míře v banky důvěru, mohl by hrozit ekonomický kolaps a selhání jednoho z nejdůležitějších pilířů ekonomiky.

4.3. Výsledky sběru dat v dotazníkovém šetření

4.3.1. Obecné otázky

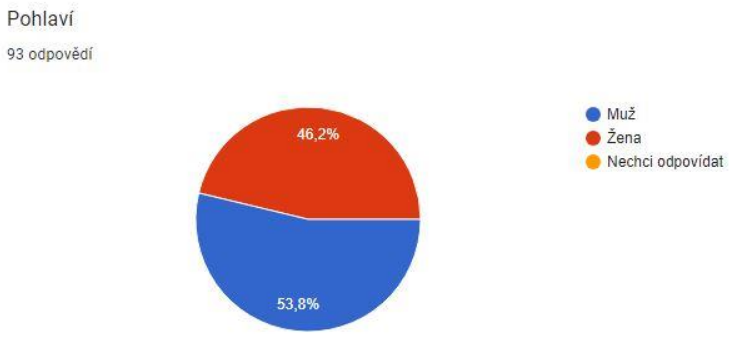
Graf č.1 – graf věkového rozmezí



Zdroj: dotazníkové šetření

Věkové rozmezí respondentů bylo zastoupeno všemi nabízenými kategoriemi. Největší část respondentů tvořili klienti v rozmezí 20-29 let, tedy celkem 65 osob. Druhou největší skupinu tvořili lidé mezi 30-49 lety v počtu 15, věk 49-59 byl zastoupen 5 respondenty. Se stejnými hodnotami byl zastoupen věk 59 a více, tedy 5 respondentů. Nejméně respondentů bylo v rozmezí 15-19, celkem 3.

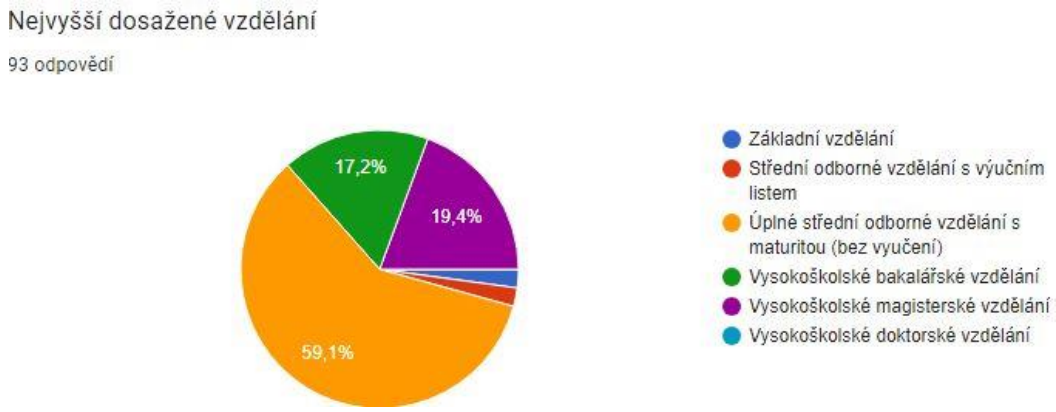
Graf č.2 - pohlaví



Zdroj: dotazníkové šetření

Dotazník vyplnilo z celkových 93 respondentů 50 mužů (53,8 %) a 43 žen (46,2 %). Možnosti neodpovědět na tuto otázku nevyužil žádný z respondentů.

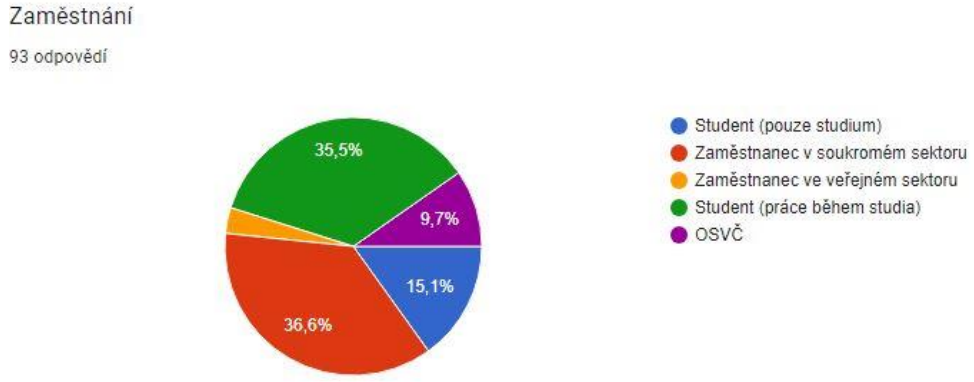
Graf č.3 – nejvyšší dosažené vzdělání



Zdroj: dotazníkové šetření

Nejvíce respondentů vyplňujících tento dotazník má ukončené úplné střední vzdělání s maturitou bez vyučení, celkem 55 osob, další největší skupinou jsou lidé s ukončeným magisterským studiem, 18 osob. S vysokoškolským bakalářským studiem je 16 osob a střední vzdělání s výučním listem mají 2 a základní vzdělání také 2 osoby.

Graf č.4 - zaměstnání



Zdroj: dotazníkové šetření

V tomto dotazníku odpovídalo nejvíce zaměstnanců v soukromém sektoru, kteří tvořili 36,6 % v počtu 34 odpovídajících. Druhou největší skupinou byli studenti, kteří během školy již pracují, celkem 33 respondentů s podílem 35,5 %. Dále následovalo 14 studentů, kteří pouze studují a nepracují s 15,1 %. Za nimi 9 OSVČ s 9,7 % a nakonec nejmenší skupinou byli zaměstnanci ve veřejném sektoru, kde odpověděli celkem 3 lidé s 3,1 %.

4.3.2. Obecné otázky ke kyberbezpečnosti

Graf č. 5 – důležitost základních znalostí z oblasti kyberbezpečnosti v dnešní době

Zdroj: dotazníkové šetření

Na stupnici od 1 (Naprosto nesouhlasím) do 5 (Naprosto souhlasím) v otázce důležitosti znalostí ohledně kyberbezpečnosti hlasovalo nejvíce respondentů stupněm 5, tedy 76 osob naprosto souhlasí, že takové znalosti jsou důležité. 14 respondentů spíše souhlasí, 2 respondenti považují znalosti za důležité, ale nijak významně a 1 respondent spíše nesouhlasí s tvrzením.

Graf č.6 – považují respondenti své znalosti za dostatečné?

Zdroj: dotazníkové šetření

V této otázce nejvíce respondentů považuje své znalosti za dostatečné, avšak více znalostí by se jim rozhodně hodilo, takovou možnost zvolilo 58 respondentů s 62,4 %. Další dvě velké části jsou takové, že jedna část své znalosti za dostatečné nepovažuje a takových

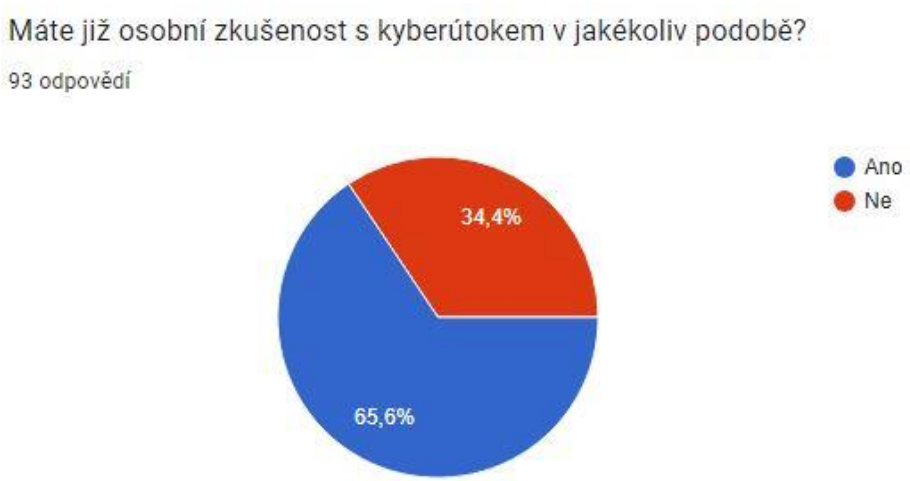
odpovídajících je 21 s 22,6 % a druhá část naopak považuje své znalosti za zcela dostačující, tak odpovědělo 13 lidí se 14 %. A jen jediného respondenta otázka kyberbezpečnosti vůbec nezajímá (1 %).

Graf č. 7 – zdroje k prohloubení znalostí o kyberbezpečnosti

Zdroj: dotazníkové šetření

Tato otázka měla povolených více možností. Nejvíce respondentů označilo jako svůj nejpravděpodobnější potencionální zdroj znalostí internet, a to 81 respondentů. 27 respondentů by se zúčastnilo vzdělávacího kurzu, 14 osob by vyhledalo vhodnou literaturu a 2 respondenti by nevěděli, kam by se měli v případě zájmu podívat.

Graf č.8 – osobní zkušenost s kybernetickým útokem

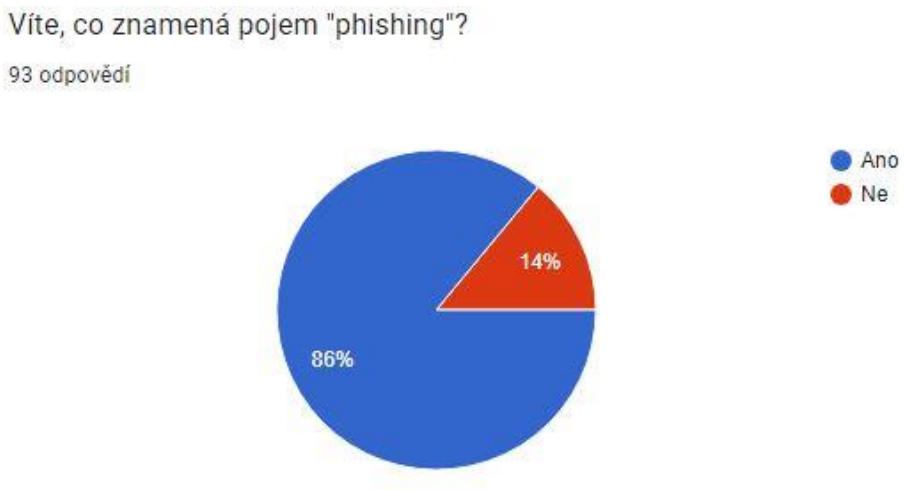


Zdroj: dotazníkové šetření

V této otázce 65,6 % respondentů, celkem 61 osob, odpovědělo, že mělo osobní zkušenost s kybernetickým útokem a 32 respondentů, 34,4 %, žádnou takovou zkušenost nemělo.

4.3.3. Sociální inženýrství (phishing)

Graf č.9 – pojem phishing



Zdroj: dotazníkové šetření

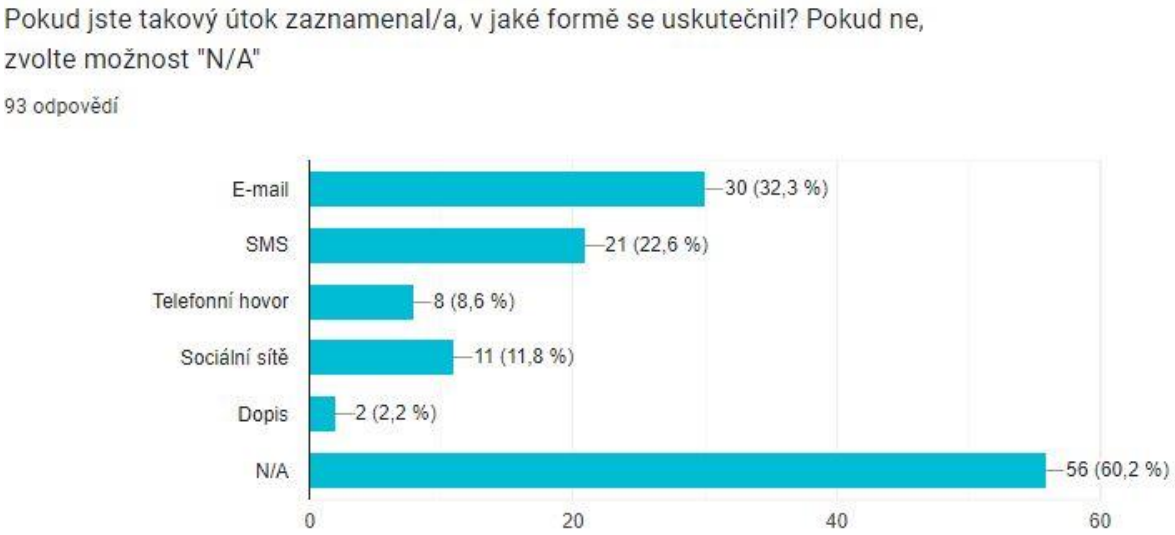
Ohledně znalosti pojmu phishing odpovědělo 86 %, tedy 80 respondentů, kladně, tedy že pojem phishing znají. Jen 14 % respondentů pojem phishing nezná, to činí 13 lidí.

Graf č. 10 – osobní zkušenost s podvodem, kdy se útočník vydával za banku

Zdroj: dotazníkové šetření

Celkem 61 osob, tedy 65,6% respondentů, osobní zkušenost s útokem podobného typu, že se někdo vydával za jejich banku, nemají. 32 osob, tedy 34,4 %, už ano.

Graf č.11 – způsob uskutečnění útoku vydáváním se za banku



Zdroj: dotazníkové šetření

Nejudávanější odpověď v této otázce souvisí s odpovědí na otázku předchozí. Nejvíce respondentů, 56 osob odpovědělo N/A, tedy, že nemohou určit, v jaké formě se útok uskutečnil, neboť takový útok nezaznamenali. Ti, kdo takovou zkušenost učinili, odpovídali, že nejvíce podvodníků se je snažilo kontaktovat e-mailem, tak odpovědělo 30 osob, přes SMS 21 osob či přes sociální sítě 11 osob. Méně časté jsou telefonní hovory, pouze 8 osob a nejméně útoků respondenti zaznamenali pomocí dopisů, a to pouze u dvou respondentů.

Graf č.12 – otevřeli by respondenti podežřelý email?

Zdroj: dotazníkové šetření

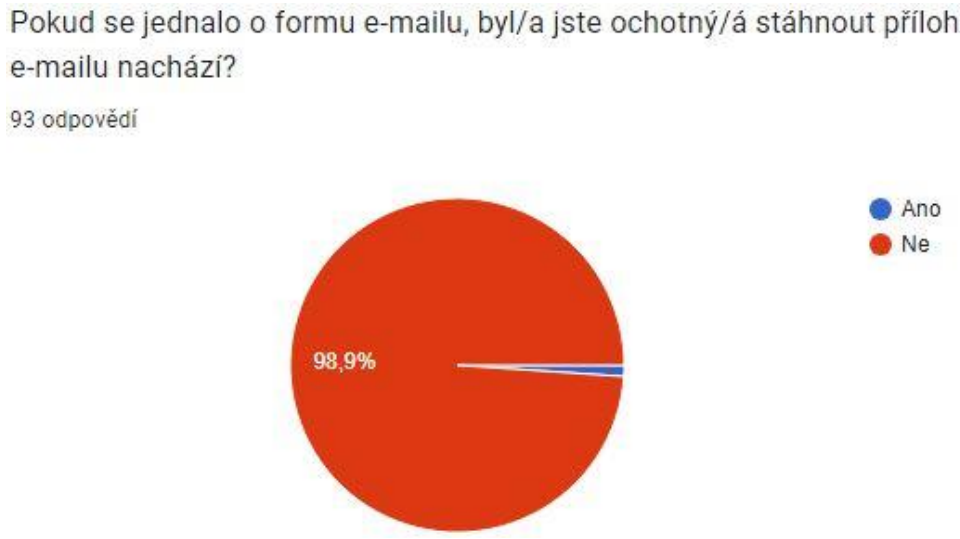
Většina respondentů, 65,6 %, tedy 61, by podezřelý email neotevřela, 34,4 %, tedy 32 respondentů, by podezřelý e-mail otevřelo.

Graf č. 13 – otevření odkazu

Zdroj: dotazníkové šetření

Poměrně jednotně odpovědělo 97,8 % respondentů (91 osob), že by odkaz v podezřelém e-mailu nikdy nerozklikli a pouze dvě osoby (2,2 %) by podezřelý odkaz rozklikli.

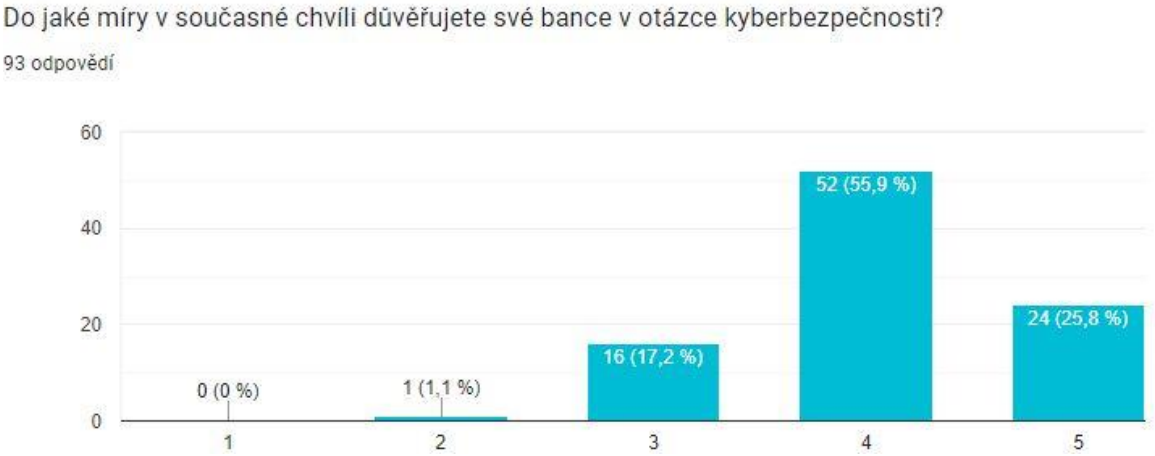
Graf č. 14 – stáhnutí přílohy



Zdroj: dotazníkové šetření

Až na jednoho respondenta, tedy 92 odpovídajících, 98,9 %, by přílohu v podezřelém e-mailu nikdy nestáhlo, avšak jediný respondent, 1,1 %, by přílohu stáhnul.

Graf č. 15 – důvěra respondentů jejich bankám v otázce kyberbezpečnosti



Zdroj: dotazníkové šetření

Na stupnici od jedné (nejméně) do pěti (nejvíce) nejvíce respondentů, 52 osob, odpovídalo stupněm 4, tedy že spíše důvěřují. 24 osob odpovědělo stupněm 5. 16 osob označilo stupeň 3 a stupeň 2 pouze jedna osoba.

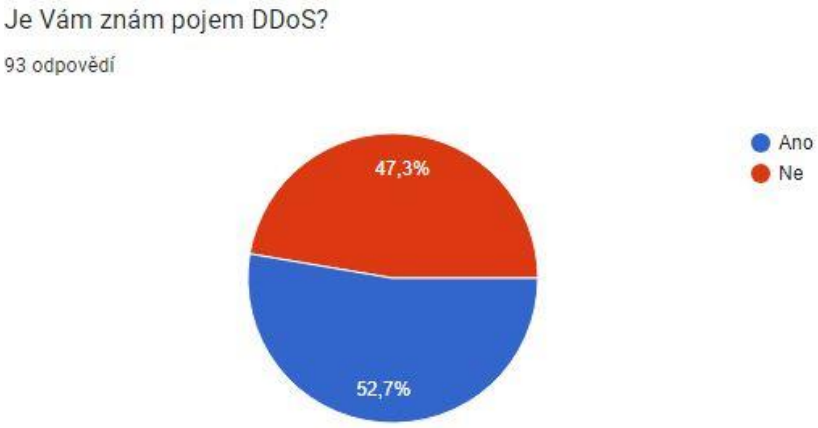
Graf č. 16 – přechod k jiné bance v případě útoku

Zdroj: dotazníkové šetření

Na stupnici od jedné (rozhodně ne) do pěti (určitě ano) nejvíce respondentů odpovědělo stupněm 3, tedy nerozhodný postoj, celkem 34 osob. 28 osob by banku spíše neměnilo, 8 lidí určitě ne. 16 osob by banku spíše měnilo a pouze 7 osob by banku změnilo určitě.

4.3.4. DDoS – Distributed Denial of Service

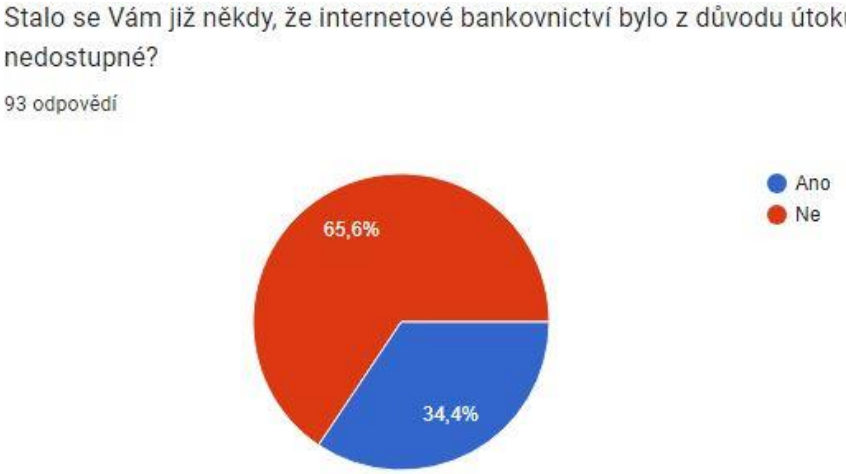
Graf č. 17 – pojem DDoS



Zdroj: dotazníkové šetření

U znalosti pojmu DDoS to nebylo tak jednoznačné a respondenti se rozdělili téměř na poloviny. Pojem zná 52,7 % respondentů (49 osob) a 47,3 % (44 osob) respondentů odpovědělo, že pojem nezná.

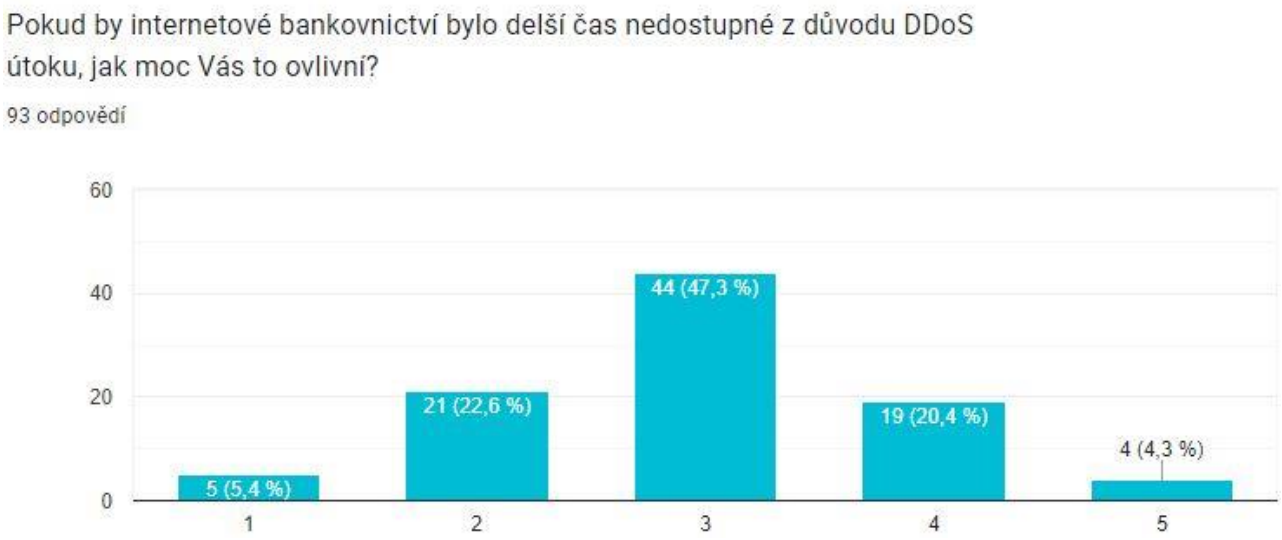
Graf č. 18 – nedostupné internetové bankovnictví z důvodu útoku



Zdroj: dotazníkové šetření

V případě nedostupného internetového bankovnictví z důvodu útoku odpovědělo 61 osob, že takový výpadek nezažili a 32 osob, že již zaznamenali takový výpadek.

Graf. č 19 – vliv na klienty z důvodu nedostupného el. bankovnictví



Zdroj: dotazníkové šetření

Na stupnici od jedné (rozhodně ne) do pěti (určitě ano) nejvíce respondentů, 44 osob, odpovědělo stupněm 3, kdy vliv výpadku by na ně měl jen nepatrný dopad a žádné zvláštní následky by neměl. Pro 5 respondentů by výpadek nebyl komplikací vůbec, pro 21 osob by spíše nebyl komplikací a naopak pro 4 osoby by byl velikou komplikací a pro 19 odpovídajících by spíše byl komplikací.

Graf č. 20 – délka výpadku bankovnictví z důvodu útoku

Zdroj: dotazníkové šetření

66 osob takový výpadek nikdy nezažilo. Žádný z respondentů také nezažil výpadek delší než jeden den. Od 3 do 24 hodin zaznamenalo výpadek 6 osob, mezi 1 a 3 hodinami pak 17 respondentů a do jedné hodiny pouze 4 lidé.

Graf č. 21 – ztráta důvěry v banku

Zdroj: dotazníkové šetření

Kdyby se banka stala obětí útoku, tak pro 79,6 % respondentů (74 osob) by se nedůvěryhodnou nestala a pro 20,4 % odpovídajících (19 osob) by se banka stala nedůvěryhodnou.

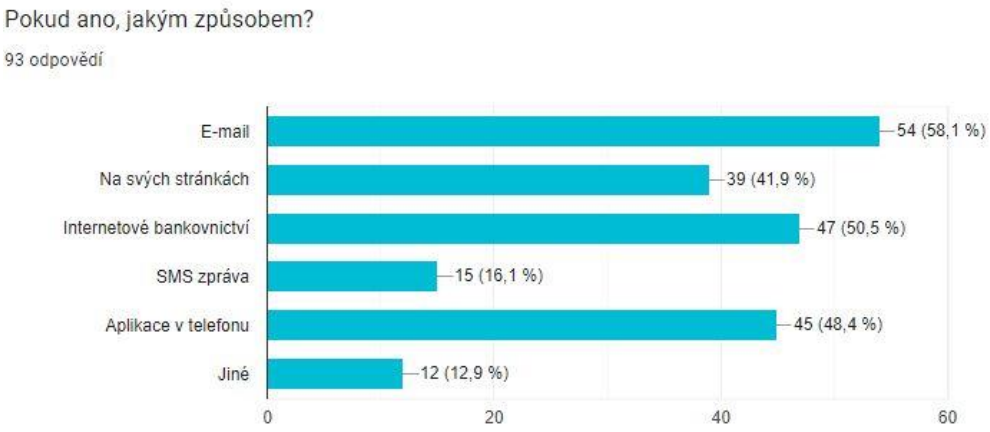
4.3.5. Prevence proti kybernetickým útokům

Graf č. 22 – varování ohledně kyberútoků

Zdroj: dotazníkové šetření

84,9 %, tedy 79 osob, bylo svou bankou už alespoň jednou varováno před kybernetickými útoky a pouze 15,1 % odpovídajících, tedy 14 osob, varováno nikdy nebylo.

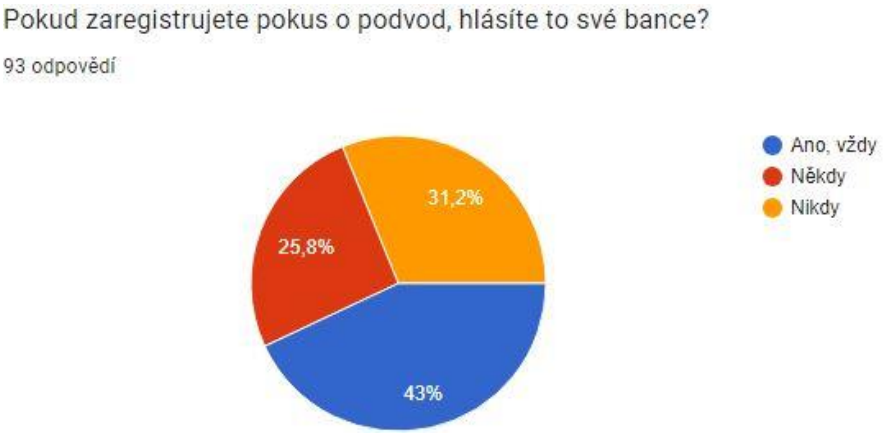
Graf č. 23 – forma varování bank ohledně kyberútoků



Zdroj: dotazníkové šetření

Nejvíce respondentů, celkem 54 osob, dostalo varování e-mailem, 47 osob skrze internetové bankovnictví, 45 klientů aplikací v telefonu. Dále prostřednictvím svých stránek bylo upozorněno 39 osob a jen 15 osob SMS zprávou a jiným způsobem 12 osob.

Graf č. 24 – oznámení pokusu o útok bance



Zdroj: dotazníkové šetření

Pokus o podvod by své bance nahlásilo v každém případě 43 % respondentů, celkem 40 osob, v určitých situacích pak 24 osob, 25,8 %. A takové pokus by nikdy nenahlásilo celkem 29 osob, tedy 31,2 %.

5. Zhodnocení výsledků

Tato kapitola se věnuje konkrétnímu zpracování a vyhodnocení výsledků z dotazníkového šetření, uvedení odpovědí do souvislostí a zhodnocení výsledků z celkového pohledu tématu této bakalářské práce.

5.1. Základní informace – otázky 1-4

Pro zjištění základních informací o respondentech byly vyhrazeny otázky č.1–4. Z věkového hlediska nejvíce respondentů odpovídalo z kategorie 20-29 let a mezi 30-49 lety. Tyto dvě se dají považovat za nejaktivnější v kyberprostoru, tedy věkové rozmezí zcela vyhovuje cílům zkoumání. Odpovídal víceméně vyrovnaný počet mužů a žen, avšak o něco více bylo mužů. Z hlediska vzdělání odpovídalo nejvíce respondentů s ukončeným středním vzděláním s maturitou a druhou největší skupinou byli vysokoškolští studenti s ukončeným magisterským studiem. Kromě studia bylo zjišťováno, zda respondenti pracují, či studují, resp. pracují i studují. Největší dvě skupiny se rozdělily téměř rovným dílem, a to zaměstnanci v soukromém sektoru a studenti pracující během studia. Složení respondentů je zcela odpovídající a vyhovující pro záměry zkoumání.

5.2. Obecné dotazy ke kyberbezpečnosti

5.2.1. Otázka č. 5 – Důležitost základních znalostí v kyberbezpečnosti

Většina respondentů považuje základní znalosti v kyberbezpečnosti za důležité. V online prostoru, kde dnes hrozí nespočet nebezpečí se bez nich lze jen těžko, bez určité újmy, obejít. Takový výsledek je příznivý, neboť 90 odpovídajících z 93 tuto důležitost vidí a jsou si vědomi, že takové znalosti jsou cenné.

5.2.2. Otázka č.6 – Dostatečnost vlastních znalostí

Další otázka byla zaměřená na osobní zhodnocení vlastních znalostí v oblasti kyberbezpečnosti. Většina respondentů považuje své znalosti v určitých mezích za dostatečné, přestože by ještě uvítali takových znalostí více, anebo jsou o svých znalostech zcela přesvědčeni. Přibližně čtvrtina odpovídajících však své znalosti za dostatečné nepovažuje a taková neznalost může mít vážné důsledky. A pouze jednoho respondenta otázka kyberbezpečnosti nezajímala, což málo vypovídá o jeho znalostech, avšak jeho lhostejný přístup k této otázce může být útočníky také zneužit.

5.2.3. Otázka č. 7 – Zdroje znalostí kyberbezpečnosti

Pokud by respondenti chtěli rozšířit své znalosti v této oblasti, pak by většina volila internet, protože dostupnost takových informací je nejvyšší a nejstálejší. Nemalá část respondentů by uvítala také vzdělávací kurzy na toto téma, případně literaturu z takového tématu. Pouze dva respondenti by nevěděli, kam se mají obrátit. Takové zjištění je pozitivní, jelikož bezradnost v oblasti hledání zdrojů vzdělávání ke kyberbezpečnosti nebyla zjištěna.

5.2.4. Otázka č. 8 – Osobní zkušenost s kyberútokem

Tato otázka zkoumá, zda odpovídající respondenti měli již osobní zkušenost s kyberútokem. Výsledky ukazují, že téměř dvě třetiny útok osobně takový útok zažilo (jedna třetina ne). Pokud člověk takový útok zažije, velice výrazně se u něho zvyšují šance, že si příště dá větší pozor a bude obezřetnější. Osobní zkušenost s útokem může mnohým pomoci s osobní opatrností na internetu do budoucna.

5.3. Sociální inženýrství (phishing)

5.3.1. Otázka č. 9 - Pojem phishing

Devátá otázka byla zaměřená na to zjistit, zda respondenti znají pojem phishing. Pojem je mezi respondenty dobře znám, protože více než tři čtvrtiny respondentů odpověděli, že tento pojem znají. Znalost pojmu jako takového může již určitým způsobem pomoci k obraně proti phishing, avšak pouhá znalost významu slova nedokáže nahradit komplexnější znalosti a zkušenosti, které však, jak je patrné z předchozích odpovědí, respondenti mají.

5.3.2. Otázka č. 10 – phishing – falešná identita – vydávání se za banku

Jen třetina osob odpovídá, že se útočníci vydávali za jejich banku. Zbytek útok v této konkrétní formě nezaznamenal. Avšak i přesto se našlo nemálo osob, u kterých došlo k pokusu využít jejich důvěry ke své bance a odcizit jim peníze, po čemž potenciálně může následovat i podkopání důvěry mezi klientem a bankou.

5.3.3. Otázka č. 11 – Forma útoku s podvrženou identitou banky

Další otázka se zaměřovala na konkretizaci formy útoku, kdy se podvodníci vydávali za banku. Jednoznačně nejčastější formou byla komunikace e-mailem. Hojně zastoupen byl i způsob skrze SMS, nicméně e-mail byl jednoznačně vybírán nejvíce. U jiných respondentů docházelo k takovým pokusům skrze telefonní hovor, sociální sítě, a dokonce i dopisem.

Jinak než prostřednictvím e-mailu dnes banky komunikují minimálně, tedy ostatní způsoby už se objevují spíše méně. U e-mailů je stejně jako u všech způsobů třeba si dát pozor.

5.3.4. Otázka č. 12-14 – Reakce na škodlivé e-maily

Tato sada otázek zkoumala, jak jsou respondenti seznámeni s nebezpečím, které by mohlo ze škodlivých e-mailů hrozit a jak se zachovají, přijde-li jim takový e-mail. Respondenti nejsou tak jednotní v otázce otevření e-mailu. Dá se připustit, že otevření mailu samotné ještě nemusí uživatele ohrozit, avšak existují způsoby, které i během otevření uživatele poškodit mohou, tedy asi třetina uživatelů by měla být poučena i o možnosti tohoto nebezpečí. V dalších otázkách se respondenti shodují, že v žádném případě se nesmí kliknout na odkazy a ani stahovat přílohy. Nicméně dva respondenti by odkaz otevřeli a jeden by dokonce stáhnul i přílohu.

5.3.5. Otázka č. 15-16 – Důvěra bankám v otázkách kyberbezpečnosti

Poslední dvě otázky ze sekce Phishing se zabývají důvěrou mezi klientem a bankou. V současné době většina respondentů poměrně důvěřuje své bance. Nelze říci, že klienti důvěřují zcela, jelikož největší část respondentů na stupnici od 1 do 5 označila stupeň 4. Důvěřují své bance, nicméně důvěra není stoprocentní. Je zde šance, že respondenti mají snadno otřesitelnou důvěru, která by případným útokem mohla být narušena. Následující otázka navazuje a zjišťuje, jestli by při případném úspěšném útoku respondenti změnili svou banku. Největší část si není jistá, ale spíše se přiklání k tomu, že by banku neměnili, avšak přibližně 25 % by svou banku nejspíše změnilo.

5.4. DDoS – Distributed Denial of Service

5.4.1. Otázka č. 17 - Pojem DDoS

U této otázky, naproti pojmu Phishing, pojem DDoS necelá polovina respondentů nikdy neslyšela. Polovina respondentů tento pojem zná.

5.4.2. Otázka č. 18-19 – Nedostupné internetové bankovnictví

Otázky č. 18 a 19 z této sekce jsou zaměřeny na zkušenosti odpovídajících s nedostupným internetovým bankovnictvím z důvodu útoku. Více než třetina respondentů má zkušenost s podobnou situací. Záměrem otázky č. 19 je zjistit, jak moc jsou takovým výpadkem klienti dotčeni. Nejvyšší koncentrace odpovědí se pohybuje ve středu stupnice;

tedy, že případný výpadek na klienty určitý dopad má, avšak jeho vliv není zásadní. Stupně, které odpovídají maximálnímu či minimálnímu vlivu, označil nepatrný počet respondentů.

5.4.3. Otázka č. 20-21 – Délka výpadku z důvodu útoku a důvěryhodnost banky

V otázce č. 20 jsou respondenti vyzváni, aby se pokusili odhadnout dobu, po kterou bylo elektronické bankovnictví nedostupné. Velká většina respondentů nedokázala čas určit, nebo takový výpadek nezažila. Pokud odpovídající výpadek zaznamenali a byli schopni určit čas, tak nejvíce odpovědí připadlo k době 1-3 hodiny výpadku bankovnictví. Dále pak výpadek v čase mezi 3-24 hodinami označilo 6,5 % odpovídajících a nakonec jen 4 respondenti označili čas do jedné hodiny. Výpadek, který banka zvládne napravit do několika hodin je tedy klienty považován za únosný, neboť i přes zkušenosti s takovými výpadky by většina klientů banku neměnila a zároveň ani neztratila důvěru v banku, na což se tázala otázka č. 20. Pro více než tři čtvrtiny respondentů by banka zůstala i po takovém výpadku z důvodu útoku důvěryhodnou, neboť situaci dokáže zvládnout a napravit v čase, který klienty nijak nepoškodí. Jen necelá čtvrtina by důvěru v banku po takovém útoku ztratila.

5.5. Prevence proti kybernetickým útokům

5.5.1. Otázka č. 22-23 – Varování bankou před kyberútoky a způsob varování

Velice povzbuzující odpovědi respondenti odeslali v otázkách, které se týkají současné prevence bank vůči klientům ve věcech kyberbezpečnosti. Z 93 respondentů 79 odpovědělo, že je jejich banka ohledně podvodů a nebezpečí na internetu varovala. Nicméně stále zbývá 15,1 % respondentů, které banka před kyberútoky nevarovala. 15 % neinformovaných klientů je v takto citlivé oblasti poměrně vysoké číslo. Banky využívají různé způsoby předávání informací klientům a respondenti jsou v otázce č. 23 vyzváni, aby vybrali, které to jsou. Nejčastějším je tentýž způsob, který útočníci využívají k pokusům o podvodné jednání, tedy e-mail. Taková shoda je přinejmenším alarmující, jelikož zde vzniká možnost, že útočníci využijí tohoto způsobu komunikace banky a zneužijí proti klientům. Dalšími způsoby, které respondenti nejvíce označili, je internetové bankovnictví (na počítači i v telefonu). Méně používané jsou pak webové stránky, SMS zprávy a jiné,

5.5.2. Otázka č. 24 - Nahlášení útoku bance

Poslední otázka v celém dotazníku se týká nahlášení podvodu bance. Zde se graf rozdělil téměř na dokonalé třetiny, kdy největší část zvolila, že takový útok hlásí své bance vždy. Druhá největší skupina uvedla, že útoky nehlásí nikdy a nejmenší část, že jen za určitých okolností. Pro banku je jistě velice užitečné, že největší část respondentů označila možnost, že útoky hlásí vždy. Bylo by velmi vhodné, kdyby banky poučili zbytek klientů, že hlásit útoky je základním krokem k jejich předejití; nahlásit útok znamená upozornit banku na existenci nebezpečí, které banka může začít řešit a případně informovat své klienty.

6. Závěr

Praktická část této bakalářské práce je zaměřena na klienty bank různého věku a různého zaměstnání. Během tohoto zkoumání je žádoucí, aby bylo dosaženo různorodosti respondentů, protože bezpečnost na internetu se týká všech, kteří se v online prostoru pohybují. Ať už odpovídající pracuje, studuje, nebo dělá oboje, tak je klientem nějaké banky a musí být na pozoru, neboť nebezpečí na internetu může hrozit komukoliv a kdykoliv.

Velká část respondentů považuje znalosti z oblasti kybernetické bezpečnosti za důležité, dokonce velmi důležité. Své vlastní znalosti pokládají za dostatečné, avšak rádi by se i něco přiučili. Mají zájem i o nabytí dalších znalostí. Vědí, kam se podívat a kde znalosti hledat. Spousta z nich se již osobně setkala s kybernetickým útokem. Taková zkušenost může poškozeného motivovat k vzdělávání a k rozvoji svých znalostí, avšak často mohou být útoky prováděny různým způsobem a zkušenost s jedním neznamená, že oběť nepodlehne druhému.

Respondenti jsou obeznámeni s názvy útoků, znají jejich názvy a vědí, o co se jedná. Pokud například narazí na podezřelý e-mail, uvědomí si, že jakákoliv interakce s ním je nebezpečná. Velká většina se zatím nesetkala s tím, že by se podvodník vydával za banku. Klienti důvěřují svým bankám v otázce bezpečnosti, avšak nezanedbatelná část z nich má důvěru velmi křehkou. Téměř čtvrtina by důvěřovat přestala, kdyby se banka stala obětí útoku (nejen DDoS). Pokud by se sami klienti nebo někdo jejich známý stal obětí podvodu, téměř 25 % z nich by zvažovalo přechod k jiné bance a 37 % respondentů si není jisto, pravděpodobně by záviselo na konkrétní situaci.

Prevence proti podvodům ze strany banky probíhá často v různých formách a odpovědi v šetření tomu odpovídají, neboť více než tři čtvrtiny dotazovaných jsou svou bankou na podvody upozorňovány, nejvíce však jsou upozorňováni formou e-mailu. Taková forma prevence může ale skrývat určité riziko. Pokud by útočníci napodobili takové e-maily a využili jich, mohli by se tím klienti ocitnout v nebezpečí. I přes to, že klienti znají pojmy jako jsou DDoS a phishing, tak počet útoků v kyberprostoru neustále roste, a to patrně proto, že útoky bývají úspěšné, jinak by se o ně útočníci nepokoušeli.

Velice důležitým prvkem a klíčem ke zlepšení celé situace je komunikace mezi klientem a bankou. Téměř 32 % dotazovaných by pokus o podvod své bance nenahlásilo a jen 26 % respondentů hlásí takový útok někdy. Každé nahlášení přitom může být pro banku důležité. Čím více útoků bude bance nahlášeno, tím lépe může banka reagovat a podle toho varovat klienty. Banka uvádí možnost podvod nahlásit, avšak ne dostatečně důrazně. Pokud

by vedla své klienty k větší interakci s ní, pak by sama mohla mít lepší přehled o útocích, které jsou denně vedeny proti jejím klientům a zároveň tím i upevnit důvěru klientů ve svou schopnost ochránit je. Na důvěře mezi klientem a bankou stojí jeden z nejdůležitějších pilířů ekonomiky státu – celé bankovnictví. Je potřeba o tuto důvěru pečovat a snažit se o její růst. Posílením důvěry a zlepšením komunikace mezi bankou a klientem lze snížit nebezpečí podvodů a zároveň posílit velice podstatnou část ekonomiky státu.

7. Seznam použitých zdrojů

1. AAG, The Latest 2023 Cyber Crime Statistics (updated July 2023) [online]. [cit. 22.07.2023]. Dostupné z: https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=With%20an%20average%20of%2097,their%20data%20leaked%20every%20second.
2. AVAST, Co je sociální inženýrství? Jak ho rozpoznat a zabránit útokům [online]. [cit. 22.07.2023]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering
3. KYBEZ, Jaké jsou nejčastější typy kybernetických útoků? [online]. [cit. 22.07.2023]. Dostupné z: https://kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/
4. IBM, What is phishing? [online]. [cit. 22.07.2023]. Dostupné z: https://www.ibm.com/topics/phishing
5. IBM, What is smishing? [online]. [cit. 22.07.2023]. Dostupné z: https://www.ibm.com/topics/smishing
6. Policie České republiky, Vishing a spoofing [online]. [cit. 23.07.2023]. Dostupné z: https://www.policie.cz/clanek/vishing-a-spoofing.aspx
7. Legislativa.cz, Kybernetický útok (kyberútok). Definice, typy, následky a prevence [online]. [cit. 23.07.2023]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
8. AVAST, Malware [online]. [cit. 23.07.2023]. Dostupné z: https://www.avast.com/cs-cz/c-malware
9. IBM, What is malware? [online]. [cit. 22.07.2023]. Dostupné z: https://www.ibm.com/topics/malware
10. Bundesamt für Sicherheit in der Informationstechnik, Ransomware – Vorsicht vor Erpressersoftware [online]. [cit. 22.07.2023]. Dostupné z: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html#:~:text=Der%20Begriff%20Ransomware%20steht%20f%C3%BCr,(englisch%3A%20Ransom)%20verlangt.
11. Sprava-site.eu, Scareware [online]. [cit. 22.07.2023]. Dostupné z: https://www.sprava-site.eu/scareware/
12. AVAST, Spyware 2023 Copyright AVAST Software s.r.o. [online]. [cit. 23.07.2023]. Dostupné z: https://www.avast.com/cs-cz/c-spyware

13. HornetSecurity, Was sind Trojaner? Wir erklären die Funktionsweise von Trojanern. [online]. [cit. 23.07.2023]. Dostupné z: https://www.hornetsecurity.com/de/wissensdatenbank/trojaner/
14. Univerzita Hradec Králové, Phishing a rizika s ním spojená [online]. [cit. 23.07.2023]. Dostupné z: https://www.uhk.cz/cs/univerzita-hradec-kralove/uhk/celouniverzitni-pracoviste/oddeleni-informacnich-technologii/it-poradna/elektronicka-posta-a-sluzby-office-365/phishing
15. AVAST, Was ist ein Distributed Denial of Service (DDoS)-Angriff und wie funktioniert er? [online]. [cit. 10.10.2023]. Dostupné z: https://www.avast.com/de-de/c-ddos
16. Cloudflare, What is a DDoS attack? [online]. [cit. 15.10.2023]. Dostupné z: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
17. Internetem bezpečně, Botnet [online]. [cit. 15.10.2023]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/
18. iRozhlas, DDoS kybernetické útoky jsou hlavně nepříjemné. Útočníci nechtějí ukrást data, říká ředitel kyberúřadu [online]. [cit. 15.10.2023]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/ddos-hackeri-kyberneticke-utoky-data_2309042328_job
19. AVAST, Was ist ein Botnet? [online]. [cit. 15.10.2023]. Dostupné z: https://www.avast.com/de-de/c-botnet
20. Cloudflare, Application layer DDoS attack [online]. [cit. 04.11.2023]. Dostupné z: https://www.cloudflare.com/en-gb/learning/ddos/application-layer-ddos-attack/
21. Cloudflare, HTTP flood attack [online]. [cit. 04.11.2023]. Dostupné z: https://www.cloudflare.com/en-gb/learning/ddos/http-flood-ddos-attack/
22. A10 Networks, Inc., What is a Protocol DDoS Attack? [online]. [cit. 04.11.2023]. Dostupné z: https://www.a10networks.com/glossary/what-is-a-protocol-ddos-attack/
23. Cloudflare, What is BGP hijacking? [online]. [cit. 04.11.2023]. Dostupné z: https://www.cloudflare.com/en-gb/learning/security/glossary/bgp-hijacking/
24. Cisco Systems, Inc., BGP Route Hijacking [online]. [cit. 04.11.2023]. Dostupné z: https://www.thousandeyes.com/learning/glossary/bgp-route-hijacking
25. Catchpoint Systems, Inc., BGP Hijacking [online]. [cit. 04.11.2023]. Dostupné z: https://www.catchpoint.com/bgp-monitoring/bgp-hijacking

26. Noction, BGP Hijacking overview. Routing incidents prevention and defense mechanisms. (Updated) [online]. [cit. 04.11.2023].
Dostupné z: https://www.noction.com/blog/bgp-hijacking
27. Cloudflare, SYN flood attack [online]. [cit. 04.11.2023].
Dostupné z: https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/
28. GeeksforGeeks, TCP 3 – Way Handshake Process [online]. [cit. 04.11.2023].
Dostupné z: https://www.geeksforgeeks.org/tcp-3-way-handshake-process/
29. NETSCOUT, Volumetric DDoS Attacks [online]. [cit. 04.11.2023].
Dostupné z: https://www.netscout.com/what-is-ddos/volumetric-attacks#signs
30. Cloudflare, DNS amplification attack [online]. [cit. 04.11.2023].
Dostupné z: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/
31. Cybersecurity and Infrastructure Security Agency, DNS Amplification Attacks [online]. [cit. 04.11.2023].
Dostupné z: https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks
32. RFC-editor, BCP 84, RFC 8704, Enhanced Feasible-Path Unicast Reverse Path Forwarding [online]. [cit. 04.11.2023].
Dostupné z: https://www.rfc-editor.org/info/rfc8704
33. Cloudflare, What is blackhole routing? [online]. [cit. 04.11.2023].
Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/
34. Imperva, Rate Limiting [online]. [cit. 04.11.2023].
Dostupné z: https://www.imperva.com/learn/application-security/rate-limiting/#:~:text=Rate%20limiting%20mitigates%20DDoS%20threats,sometimes%20millions%20of%20IP%20addresses.
35. Cloudflare, What is Anycast? | How does Anycast work? [online]. [cit. 04.11.2023].
Dostupné z: https://www.cloudflare.com/learning/cdn/glossary/anycast-network/
36. Největší banky v Česku. Nové žebříčky podle klientů a peněz [online]. [cit. 02.03.2024].
Dostupné z: https://www.penize.cz/osobni-ucty/440001-nejvetsi-banky-v-cesku-zebricek-podle-poctu-klientu-a-spravovanych-penez

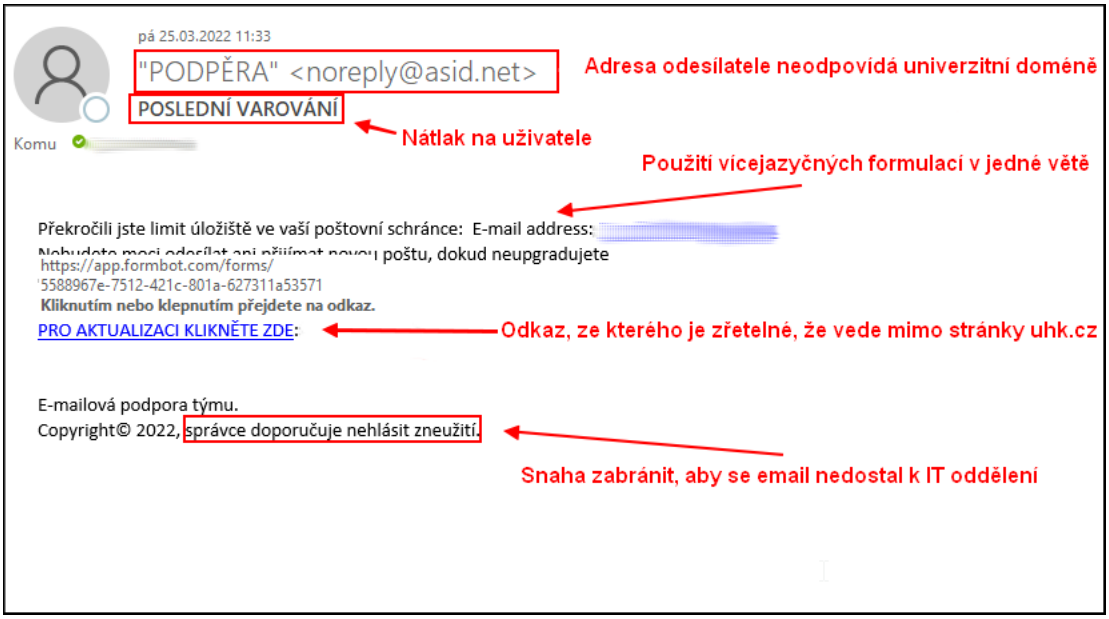
8. Přílohy

Příloha 1. - http://generator-citaci.cz/?caf&&query=Generators&afdToken=ChMIuKKa6-mmgAMVCIT9Bx1XLg-cEm0BJ3TYYcIFGnnMBLI9FbNO4HzkiuXB77yDd2cq2p5ZMzfsdfal0UlEwaxHyZx7ojTvuuCQMiTedOlInRixca891jQkPrBznL-ZUFNTttHrr3o2ydzxfvRqDz0bgNDCLgoYheFTXq&pcsa=false&nb=0&nm=14&nx=174&ny=43&is=700x480

9. Obrázky

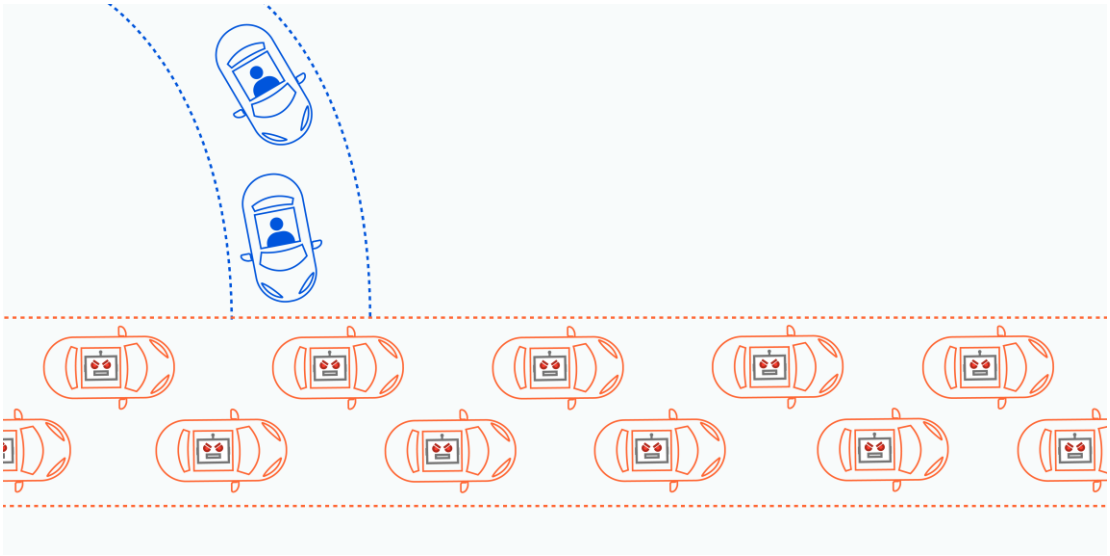
Obrázek č.1 – Prvky phishingového e-mailu

Zdroj:https://www.uhk.cz/cs/univerzita-hradec-kralove/uhk/celouniverzitni-pracoviste/oddeleni-informacnich-technologii/it-poradna/elektronicka-posta-a-sluzby-office-365/podezrele-e-mailove-zpravy



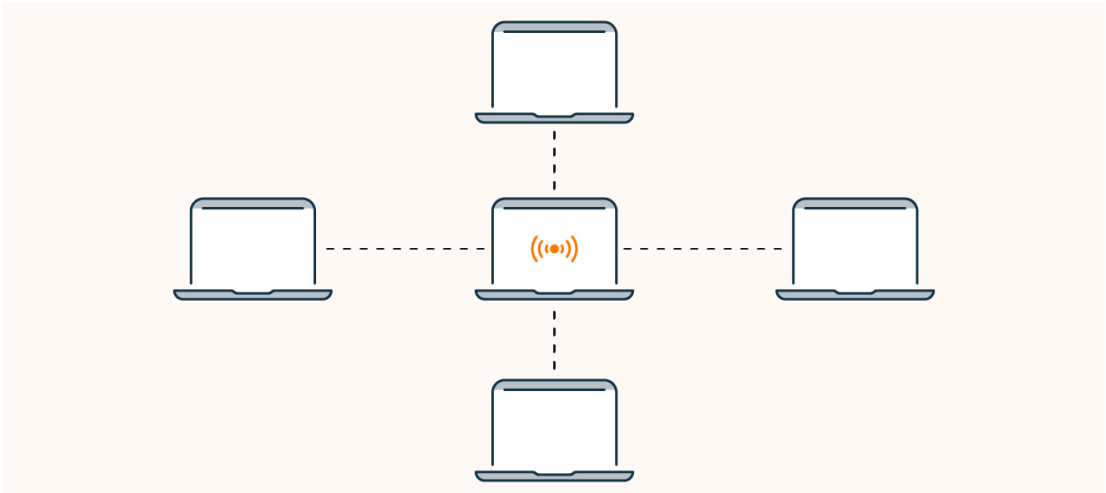
Obrázek č.2 – DdoS útok jako automobilová doprava

Zdroj: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack//ddos_attack_traffic_metaphor.png



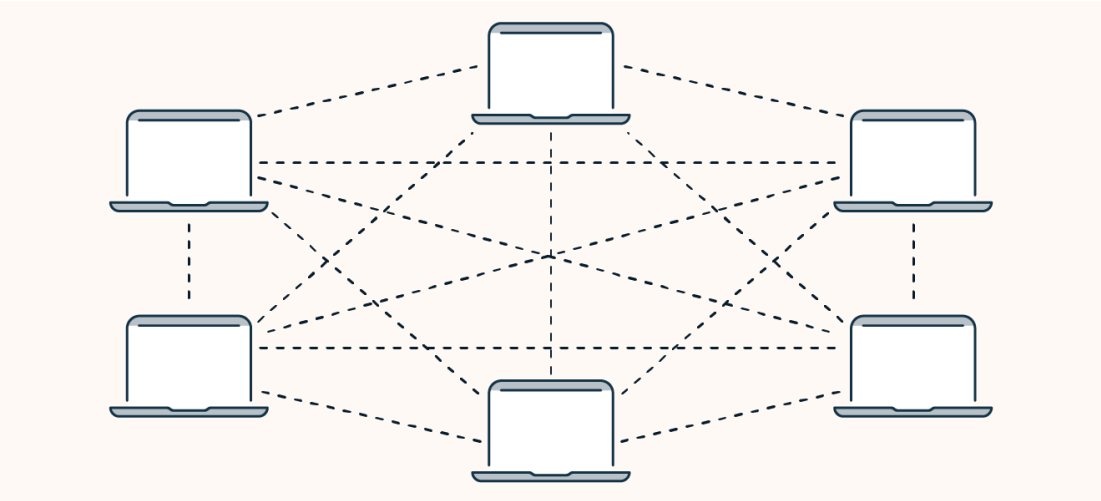
Obrázek č.3 – Centralizovaná kontrola botnetu

Zdroj: https://www.avast.com/de-de/c-botnet



Obrázek č.4 – Decentralizovaná kontrola botnetu

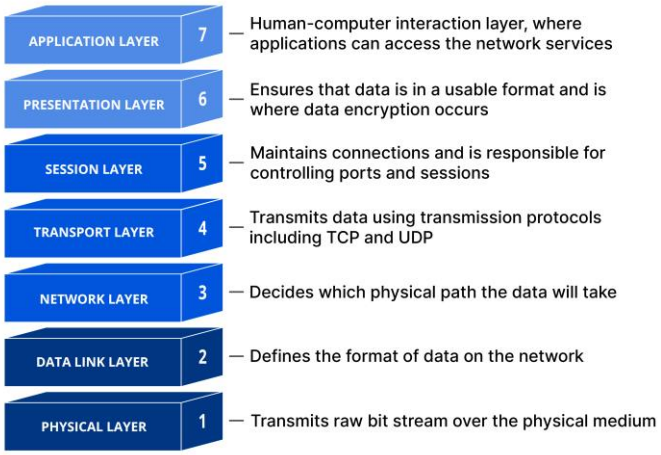
Zdroj: https://www.avast.com/de-de/c-botnet



Obrázek č.5 – ISO/OSI layer model

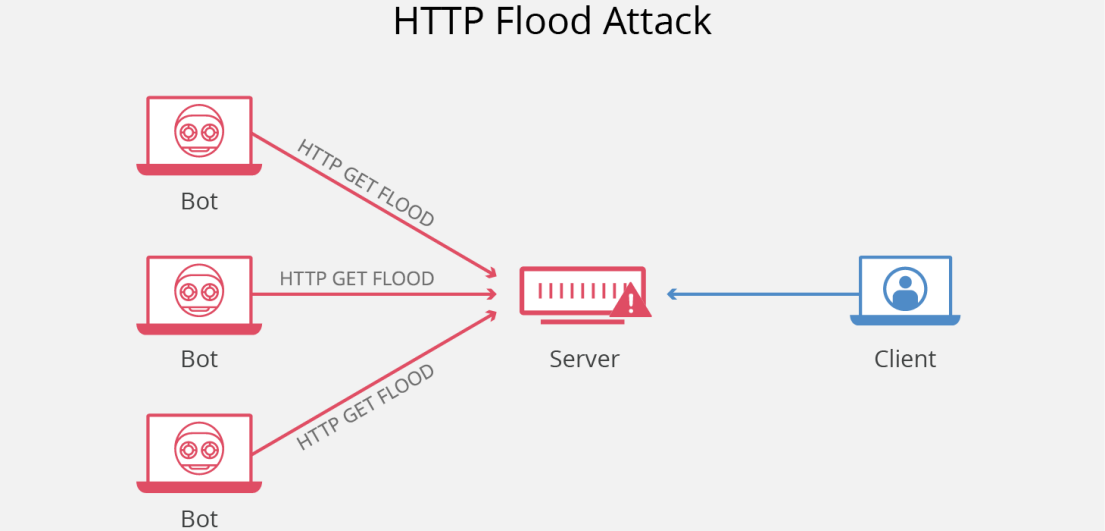
Zdroj:

https://cfassets.www.cloudflare.com/slt3lc6tev37/6ZH2Etm3LlFHTgmkjLmkxp/59ff240fb3ebdc7794ffaa6e1d69b7c2/osi_model_7_layers.png



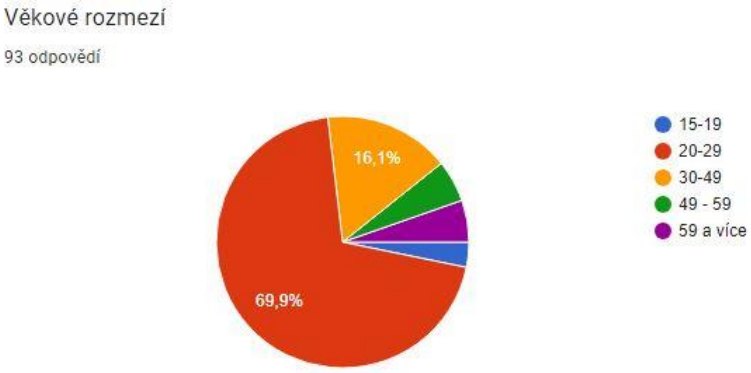
Obrázek č.6 – HTTP Flood (typ GET) útok

Zdroj: https://www.cloudflare.com/img/learning/ddos/http-flood-ddos-attack/http-flood-attack.png



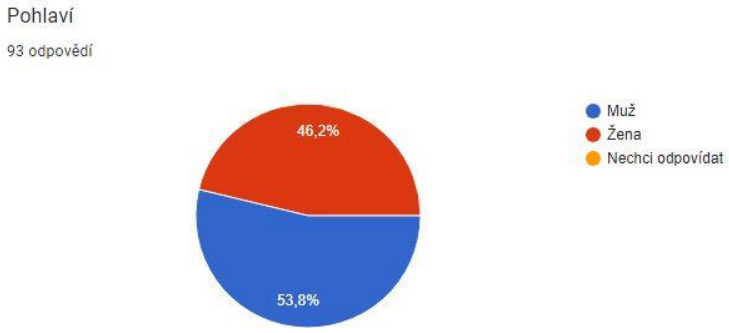
10. Seznam grafů

Graf č.1 – graf věkového rozmezí



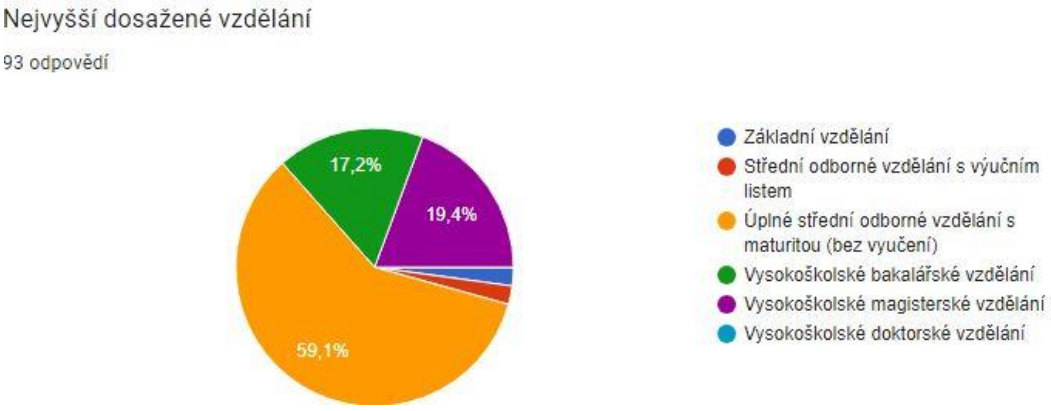
Zdroj: dotazníkové šetření

Graf č.2 - pohlaví



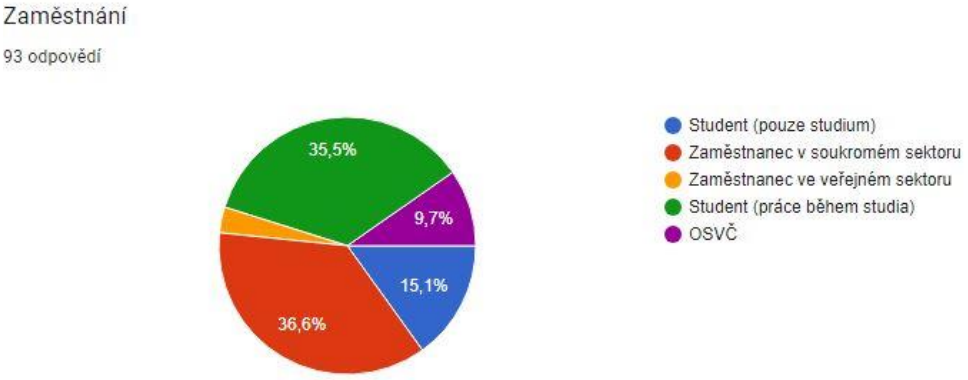
Zdroj: dotazníkové šetření

Graf č.3 – nejvyšší dosažené vzdělání



Zdroj: dotazníkové šetření

Graf č.4 - zaměstnání



Zdroj: dotazníkové šetření

Graf č. 5 – důležitost základních znalostí z oblasti kyberbezpečnosti v dnešní době

Zdroj: dotazníkové šetření

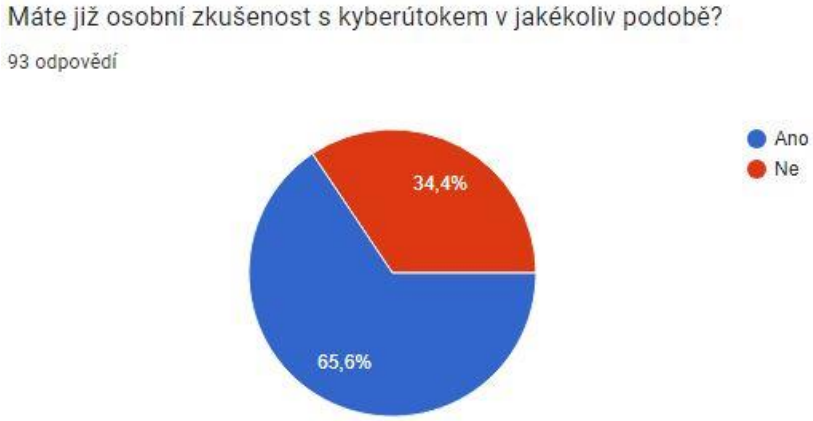
Graf č.6 – považují respondenti své znalosti za dostatečné?

Zdroj: dotazníkové šetření

Graf č. 7 – zdroje k prohloubení znalostí o kyberbezpečnosti

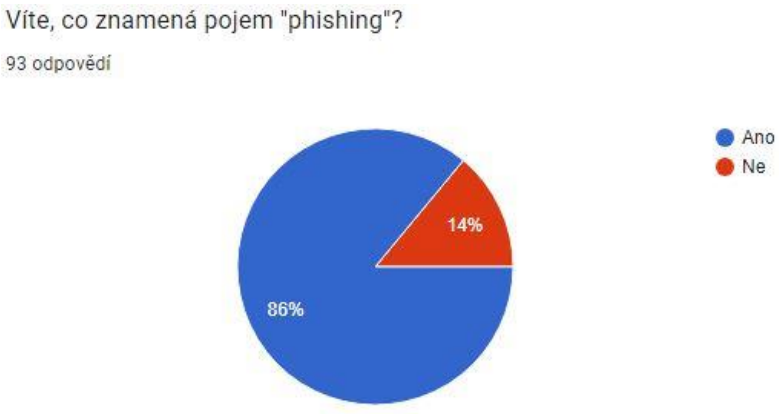
Zdroj: dotazníkové šetření

Graf č.8 – osobní zkušenost s kybernetickým útokem



Zdroj: dotazníkové šetření

Graf č.9 – pojem phishing

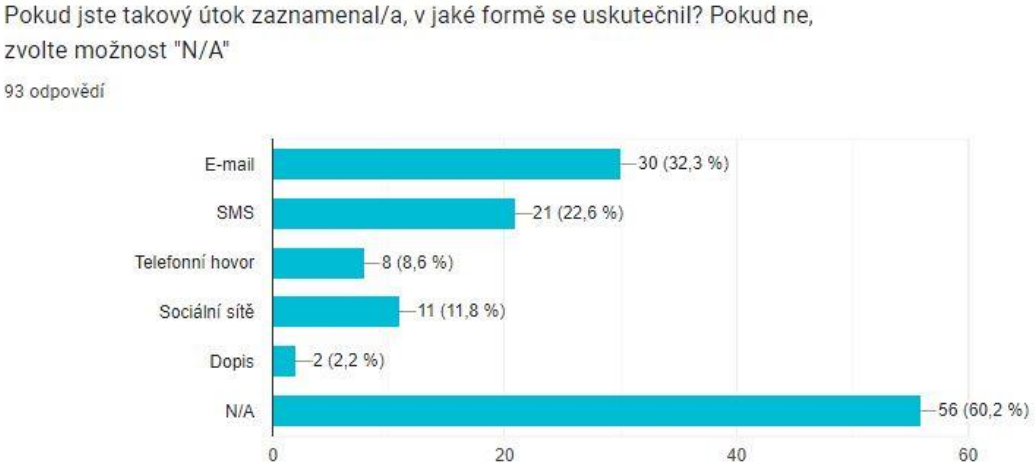


Zdroj: dotazníkové šetření

Graf č. 10 – osobní zkušenost s podvodem, kdy se útočník vydával za banku

Zdroj: dotazníkové šetření

Graf č.11 – způsob uskutečnění útoku vydáváním se za banku



Zdroj: dotazníkové šetření

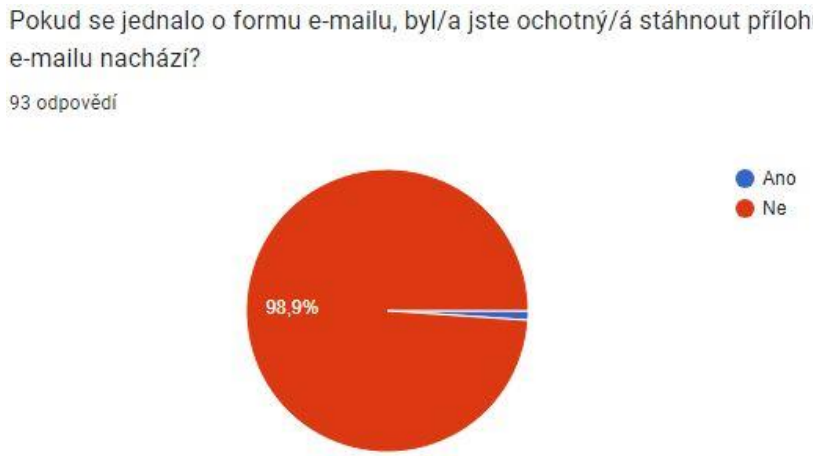
Graf č.12 – otevřeli by respondenti podežřelý email?

Zdroj: dotazníkové šetření

Graf č. 13 – otevření odkazu

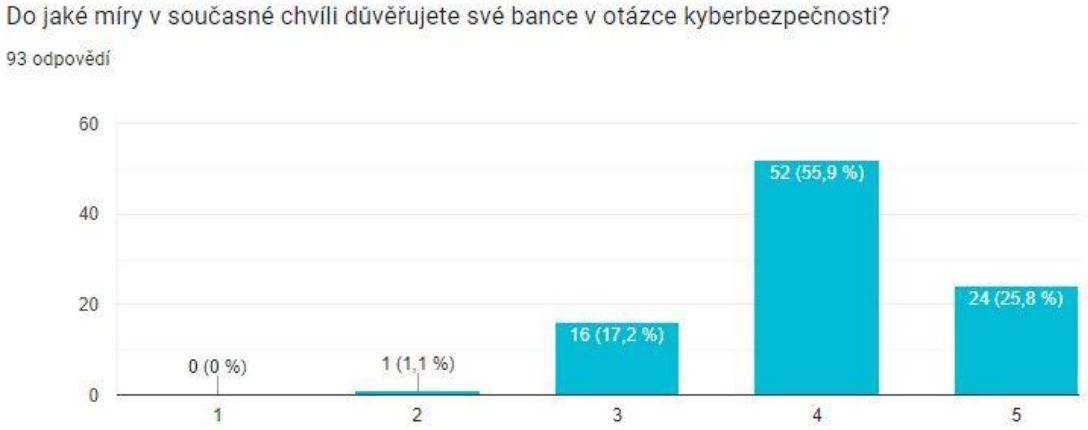
Zdroj: dotazníkové šetření

Graf č. 14 – stáhnutí přílohy



Zdroj: dotazníkové šetření

Graf č. 15 – důvěra respondentů jejich bankám v otázce kyberbezpečnosti

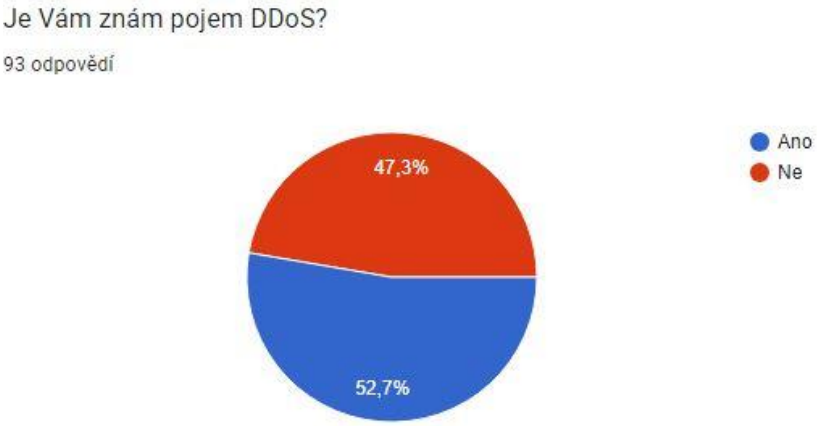


Zdroj: dotazníkové šetření

Graf č. 16 – přechod k jiné bance v případě útoku

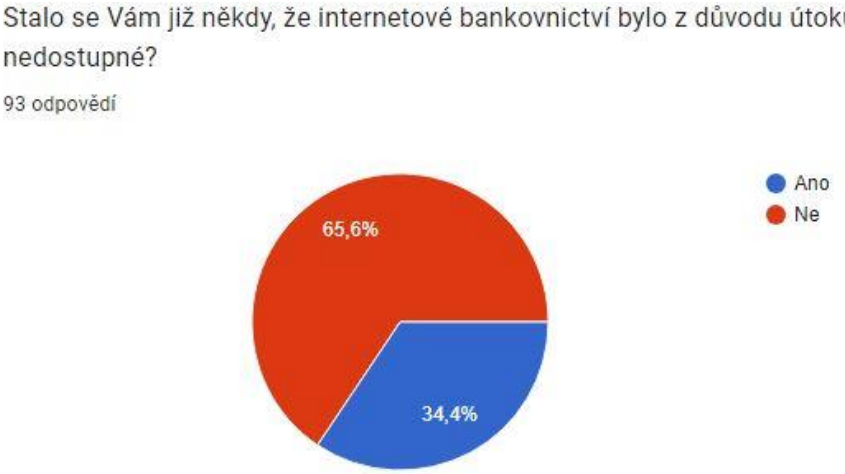
Zdroj: dotazníkové šetření

Graf č. 17 – pojem DDoS



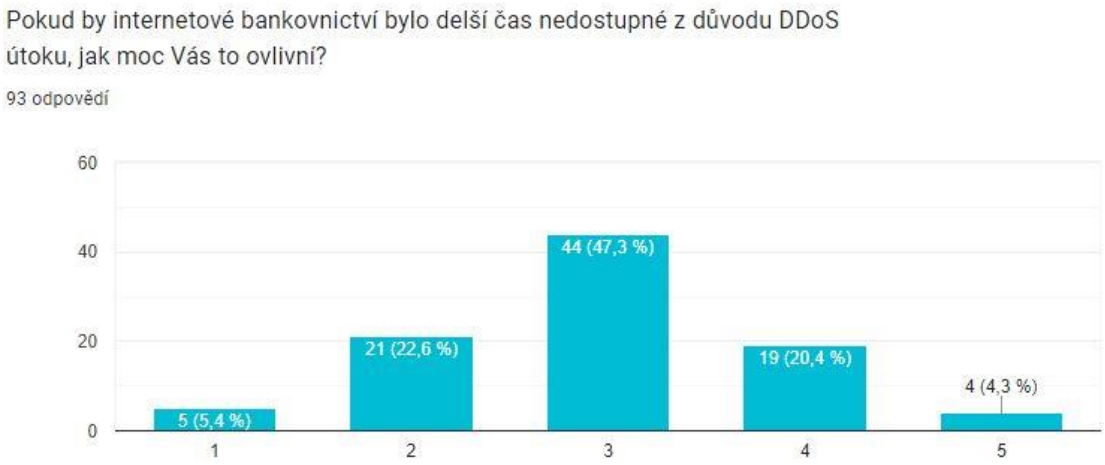
Zdroj: dotazníkové šetření

Graf č. 18 – nedostupné internetové bankovnictví z důvodu útoku



Zdroj: dotazníkové šetření

Graf. č 19 – vliv na klienty z důvodu nedostupného el. bankovnictví



Zdroj: dotazníkové šetření

Graf č. 20 – délka výpadku bankovnictví z důvodu útoku

Zdroj: dotazníkové šetření

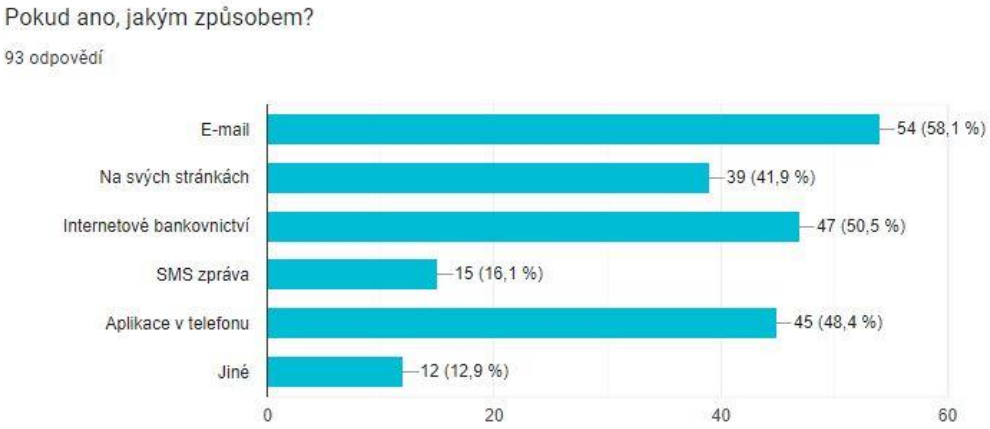
Graf č. 21 – ztráta důvěry v banku

Zdroj: dotazníkové šetření

Graf č. 22 – varování ohledně kyberútoků

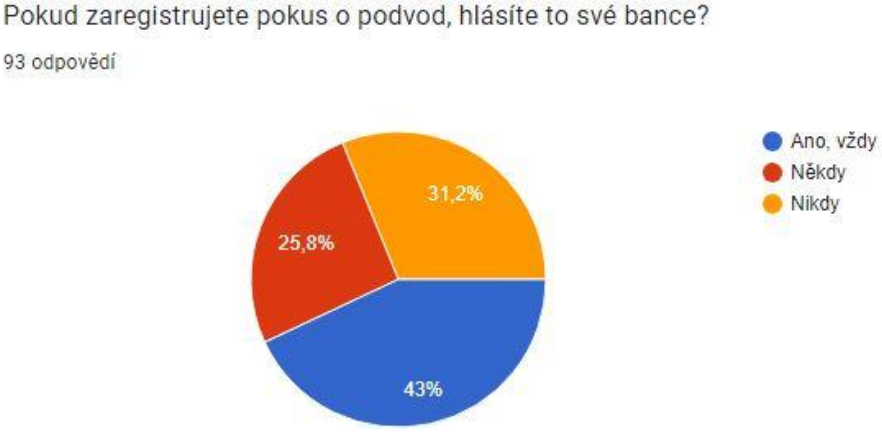
Zdroj: dotazníkové šetření

Graf č. 23 – forma varování bank ohledně kyberútoků



Zdroj: dotazníkové šetření

Graf č. 24 – oznámení pokusu o útok bance



Zdroj: dotazníkové šetření