Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Sociální inženýrství

Bakalářská práce

Autor: Jiří Bönsch
Studijní obor: Aplikovaná Informatika

Vedoucí práce: Ing. Hana Švecová

Hradec Králové Duben 2021

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29.4.2021 .....
Jiří Bönsch

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Haně Švecové za odborné vedení práce a dobré rady, které pomohly práci vylepšit.

Anotace

Stále více se dostávají do povědomí útoky sociálního inženýrství. Jejich počet rok od roku narůstá a tím se stává toto téma stále aktuálnější. Předmětem této bakalářské práce je analýza připravenosti komerčních institucí a institucí veřejné správy vůči útokům sociálního inženýrství. Hlavním cílem bakalářské práce je analýza a ověření využívaných metod v praxi a vytvoření metodických doporučení. Bakalářská práce je rozdělena do dvou částí: teoretická a praktická část.

Teoretické část obsahuje charakteristiku sociálního inženýrství a přehled využívaných metod. Jsou vysvětleny hlavní principy sociálního inženýrství, nejčastější útoky a možnosti obrany proti sociálnímu inženýrství.

Praktická část je zaměřena na nejčastěji využívané metody v praxi podle provedeného šetření s následným stanovením bezpečnostních doporučení.

Annotation

Title: Social Engineering

Awareness of social engineering attacks is growing. Their number is increasing from year to year, making this topic even more relevant than it was ever before. This bachelor thesis is trying to examine readiness of institutions (both commerce and public administration) against these attacks. The main goal of the bachelor thesis is analysis and verification of the methods used in practice and the creation of methodological recommendations. The bachelor thesis is divided into two parts: theoretical and practical part.

The theoretical part contains the characteristics of social engineering and an overview of the methods used. The main principles of social engineering, the most common attacks and defense options against social engineering are explained.

The practical part is focused on the most commonly used methods in practice according to the survey with the subsequent determination of safety recommendations.

Obsah

Seznam obrázků

1 Úvod

V dnešní moderní době jsou kladeny stále větší nároky na bezpečnost. S rozvojem internetu je přístup k informacím velmi jednoduchý, na druhou stranu je však jejich ochrana stále složitější. Není proto překvapením, že se vyvíjí stále novější, lepší a pokrokovější metody pro ochranu dat.

V současnosti tak dochází k velkému množství technologických útoků, s postupem času je však velmi zřejmé, že nejslabším článkem obrany je stále častěji člověk. A to nemluvíme o případech špatného nastavení hardware nebo software zapříčiněného chybou nebo pouze nepozorností odborníků. Můžeme tak hovořit o prolomení ochrany zaměřené výhradně na člověka, které se říká sociální inženýrství. Útočník nemusí překonávat bariery obrany, pokud mu do systému umožní přístup samotný uživatel.

Útoky sociální inženýrství jsou zaznamenávány stále častěji, ne však z důvodu posílení obrany a jejich následného odhalení, ale z důvodu navyšování jejich množství. Je tedy nutné zjistit, zda se na tento typ útoků instituce v České republice připravují, jak se připravují a zda je tato hrozba brána vážně.

Bakalářská práce je rozdělena do části teoretické a praktické. V teoretické části je charakterizováno sociální inženýrství, jsou zde představeny principy útoků, využívané metody a možná obrana.

Praktická je zaměřena na analýzu současného stavu u soukromých a veřejných institucí s následným vytvořením přehledného seznamu metod, jejich analýzou a doporučeními pro použití daných metod při jejich zavádění do obrany, ať již stávající nebo nově vytvářené.

2 Cíl práce

Primárním cílem je analýza útoků a stanovení metod obrany proti sociálnímu inženýrství na základě provedeného zkoumání u soukromých a veřejných institucí.

Za účelem prozkoumání primárního cíle byly stanoveny dílčí cíle:

- charakterizovat sociální inženýrství z pohledu kybernetické bezpečnosti,
- analyzovat útoky v sociálním inženýrství,
- představit nejčastější hrozby sociálního inženýrství,
- analyzovat využívané metody v sociálním inženýrství,
- analyzovat využití sociálního inženýrství u soukromých a veřejných institucí,
- vytvořit přehled bezpečnostních doporučení proti útokům v oblasti sociálního inženýrství.

3 Metodika

Metodický postup pro tuto kvalifikační práci byl rozdělen do dvou částí (teoretické a praktické), které se sestávali z několika provázaných částí.

Metodika byla rozdělena na části: rešerše, analýza kybernetických útoků a charakteristika metod využívaných v sociálním inženýrství a v praxi.

Kvalifikační práce byla zaměřena na analýzu nejvyužívanějších metod v sociálním inženýrství s následným ověřením v praxi. Za tímto účelem byla provedena analýza a byly kontaktovány instituce ze soukromého sektoru i veřejného sektoru. Z důvodu ochrany osobních a interních dat organizací nejsou v této kvalifikační práci uváděna jména oslovených veřejných a soukromých institucí[1].

Z důvodu ochrany osobních a interních informací oslovených institucí nebylo možné detailněji specifikovat některé otázky, z toto důvodu bylo dotazování zaměřeno na otázky volnějšího charakteru (nepřímé otázky, konstruktivní otázky), které dále mohla instituce specifikovat podle vlastního uvážení. Otázky byly v rámci přehlednosti a funkčnosti rozděleny do dvou kategorií:

- metody zaměřené na povědomí uživatele
- metody technické

V průběhu komunikace s oslovenými institucemi byly položené otázky specifikovány a doplněny podle možností (informační bezpečnost, ochrana osobních údajů, přístup k utajovaným informacím) dané instituce.

[1]Oslovené instituce o to požádali během komunikace a byla to jedna z podmínek zisku informací.

Výsledkem jsou metody volně seřazené od nejpoužívanějších, rozdělené v již zmíněných dvou kategoriích. Každá metoda je pak vysvětlena, jsou představeny sjednocující znaky pro všechny instituce. To slouží účelu pochopení proč a jak je daná metoda využívána, a jak slouží k navýšení ochrany.

Problematika sociálního inženýrství je v České republice doposud velmi málo řešena v odborné literatuře a i u nás odborníci využívají zahraniční odbornou literaturu. Z toho důvodu bylo pro zpracování této bakalářské práce čerpáno převážně ze zahraničních zdrojů a literatury a při psaní byly využity obrázky, grafy či tabulky u kterých byl ponecháno původní znění, protože při doslovném překladu by mohlo dojít ke špatné interpretaci uváděných pojmů.

4 Teorie sociálního inženýrství

Sociální inženýrství je vážnou hrozbou se stále narůstajícím množstvím případů, je patrné,že se tento pojem dostal i do veřejného povědomí. To ale také znamená, že ho používají i lidé, kteří plně netuší o co se jedná a mohou tak šířit špatné informace. Z tohoto důvodu je velmi důležité začít definicí sociálního inženýrství, aby nemohlo dojít k mylným předsudkům a domněnkám. Stručně lze říci, že sociální inženýrství je koncept pojmenovávající psychologickou manipulaci subjektu za účelem získání informací nebo provedení akcí, které nejsou v jejich nejlepším zájmu. Tato zjednodušená a zkrácená definice je adekvátní pro rychlé pochopení, avšak pouze nastiňuje hloubku tohoto tématu. Pokud bychom hledali hlubší pochopení mohl by nám k tomu pomoci příběh představen v kapitole 10 knihy Kevina Mitnicka [1]. Tato kapitola zaměřená na sociální inženýrství představuje bezpečnostního konzultanta s přezdívkou „Whurley“ a jeho práci v Las Vegas, kde byl najat, aby vyzkoušel bezpečnost kasína. Je zde velmi dobře popsáno nejen sociální inženýrství v praxi a metody, které útočníci používají, aby dosáhli svého cíle, ale také myšlenkové pochody útočníka při přípravě i při samotném útoku. I když závěr Whurleyho práce pro kasíno nedopadl nejlépe byl tento útok velmi dobrým indikátorem skutečného útoku. Tento útok byl však pouze jedním možným útokem z mnoha, a dalo by se dokonce říci, že každý útok přesahující jistou úroveň sofistikovanosti je jedinečný. Při obraně je nutné se zaměřit nejen na samotný útok ale i na to, co mu předchází, pokud opravdu chceme pochopit pravou podstatu teorie sociální inženýrství a jeho hrozby.

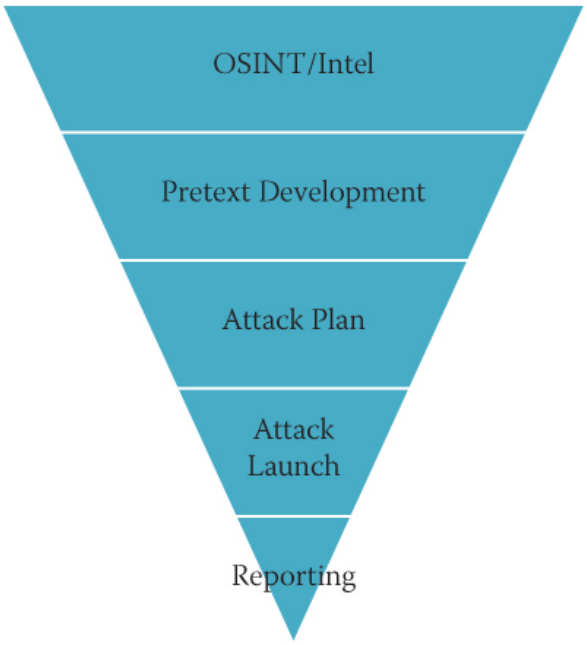
Závěrem krátkého úvodu do teorie sociálního inženýrství musíme podotknout, že slovo manipulace se sebou nese schizma špatnosti, a nejčastěji ho slyšíme ve spojení s negativními událostmi či situacemi. Z toho důvodu je velmi důležité si uvědomit, že ne každá manipulace

je špatná. Stejně tak ne každá instance sociálního inženýrství není nezákonná činnost či není ve prospěch společnosti. Specialisté sociálního inženýrství jsou mnohdy zaměstnáni ve firmách jako odborní poradci, konzultanti a testeři v informační bezpečnosti a jejich spolupráce je někdy vyžadována i orgány činnými v trestním řízení (policie, státní zástupce, soudy) a dalšími státními institucemi.

4.1 Rozbor útoků sociálního inženýrství

Tato kapitola se zabývá rozborem útoku a to specificky pomocí pyramidy sociálního inženýrství představené Christopherem Hadnagym v knize Social Engineering [2]. Pyramida SI[2] představuje reprezentaci častých faktorů které se opakují při útocích, jak je author Chrystopher Hadnagy vypozoroval během svého profesního odborného působení v oblasti sociálního inženýrství. Pyramida je pak dále upravena pro pochopení a využití na ochranu proti těmto útokům a pro využití specialisty na simulování útoků. Je však důležité si uvědomit, že velikost bloku odpovídá časové náročnosti, kdy útočník stráví více času přípravou na útok, než samotným útokem. Většina útoků sociálního inženýrství nelze připravit za pár minut, mnohdy trvá příprava dny, měsíce nebo i roky. Je tedy zřejmé, že ne každý útok sociálního inženýrství se bude řídit přesně krok po kroku dle této pyramidy. Je možné, že některé části pyramidy budou přeskočeny nebo nahrazeny značnou sérií improvizací, avšak pomocí této pyramidy můžeme útoky v sociálním inženýrství rozdělit na menší, jednodušeji popsatelné části pro jednodušší pochopení sociálního inženýrství. Jelikož jsme se již seznámili s příběhem „Whurleyho [1]“, z tohoto důvodu je v dalších částech této kvalifikační práce využíván pro lepší vysvětlení modelu pyramidy od Ch. Hadnagymo, který je zobrazen na obr. 1 [2].

[2]SI – Sociální inženýrství.



Obr. 1: Pyramida SI

Zdroj: [2]

4.1.1 OSINT/Intel

OSINT je zkratka pro open source inteligence, neboli volně dostupné zdroje. Tento krok je tedy sběr informací o cíli.

„V současnosti je hlavní pozornost zaměřena na elektronická média (především internet). Základním a zcela zásadním rozdílem oproti jiným oblastem věnujícím se získávání informací je práce se všemi dostupnými informačními zdroji -tedy i s takovými, které nejsou označovány jako relevantní ve vědecké sféře. V rámci OSINT jsou běžně vytěžovány například i takové informační zdroje jako jsou blogy, diskusní fóra, newsgroups nebo (zejména v poslední době) sociální média. Tyto zdroje mohou poskytnout velmi aktuální a cenné údaje a informace. Zároveň však vzniká problém s velkým objemem takových dat a jejich problematickým zpracováním v reálném čase. Dále tyto informační zdroje kladou vysoké nároky na následnou analýzu a ověření, přičemž může snadno dojít k dezinterpretaci takových informací.“ [3]

I když se toto na první pohled může zdát jednoduché a rychlé, opak je pravdou. Chrystopher Hadnagy poukazuje na fakt, že v dnešní době není problém najít informace, problém je určit která informace je důležitá [2]. Nelze pouze říct: „potřebuji všechny informace“. Je tedy často nutné zaměřit sběr informací na specifickou oblast, podle typu cíle nebo podle očekávané interakce s cílem, popřípadě podle typu útoku. Také schopnost poznání, která informace je důležitá či není je umění.

Příkladem si zde uvedeme běžný příklad phishingu pomocí podvodných emailů. Málokdo odpoví na email, který po něm bude vyžadovat informace o jeho bankovním účtu, obzvláště, když je navíc od neznámého odesílatele a týká se banky, o které nikdy neslyšel. Situace je však jiná, pokud příchozí email pochází z domény, která se o jedno lehce přehlédnutelné písmeno liší od jeho banky a i email samotný kopíruje vzhled emailu jeho banky. Ve „Whurleyho [1]“ případě je hned v úvodu kapitoly jasně psáno, že nejdříve sbíral informace z domova, pak i na samotném místě činnosti a to od zaměstnanců nebo finančního auditora.

Existuje mnoho způsobů sbírání informací, někdy stačí pozorně poslouchat nebo si při prohlídce všímat detailů, jindy je potřeba prohledat sociální sítě nebo registry budov či internetových stránek [2]. Neexistuje člověk či organizace, o které nelze najít záznam na internetu, je pouze nutné informace najít. U některých případů je to pouze těžší než u jiných. Proto je potřeba uvědomit si, že kdokoli se může stát cílem sociálního inženýrství a připustit si rizika z toho vznikající. A to se stále bavíme pouze o OSINTU, volně dostupných informacích. Pokud útočník útok myslí vážně, je rozumné uvažovat možnost, kdy takto volně získané informace použije k získání informací, které volně dostupné nejsou, ať už je to pomocí podvodného telefonátu, nelegálního přístupu k souborům nebo jako v případě „ Whurleyho [1]“ vyzpovídáním osob, o kterých ví, že v místě

jeho útoku pracují nebo s ním spolupracují. Uvědomme si tedy, že útočník má k dispozici značné množství informací ještě před tím, než vůbec samotný útok započne a my, jako napadená strana, zatím ani netušíme, že jsme cílem útoku a je potřeba se bránit. Hlavně tento rozdíl v přípravě na útok činí Sociální inženýrství tak nebezpečným. Jedinou obranou vůči tomuto kroku útoku je limitovat množství volně dostupných informací a dobře zabezpečit přístup k ostatním.

4.1.2 Pretext Development

Pretext Development je tvorba záminky pod kterou útočník operuje. Oklamat cíl není snadné a tak musí útočník využívat všechny možné způsoby pomoci. Jeden z nejlepších triků sociálního inženýra je nenechat cíl přemýšlet. Lidský mozek je geniálně vyvinutý a složitý orgán. To však neznamená, že je dokonalý, jak popisují knihy „Thinking, fast and slow“ od Daniela Kahnemana, nebo „Influence: The Psychology of Persuasion“ od Roberta B. Cialdiniho [4] [5]. Náš mozek lze ovlivňovat s překvapivou snadností za využití správných technik nebo kognitivních „chyb“. Jednou z těchto „nedokonalostí“, které sociální inženýři rádi využívají je jeho „lenost“. Mozek se snaží šetřit svoji práci na opravdu důležité věci a proto se snaží co možná nejvíce automatizovat. Jeho činnost vytváří „podprogramy“, kterým říkáme zvyky. Příkladem nám může být řízení auta, činnost která ze začátku není jednoduchá, ale s postupem času ji mozek zautomatizuje natolik, že si mnohdy ani sami neuvědomujeme, co všechno současně vykonáváme. Tato funkčnost je pak vyvážena situacemi, kdy např. přijdeme do místnosti, a nemůžeme si vzpomenout, proč jsme přišli, což je dáno tím, že náš mozek přemýšlel nad jinými myšlenkami, které byly s největší pravděpodobností důležitějšími než myšlenkové pochody spojené s místem a cestou do dané místnosti. Součástí této lidské činnosti, v našem případě zvyku, však není zapamatování si, proč jsme do dané

místnosti šli. Dalo by se říci, že tyto zvyky byly vytvořeny, aby mozek ušetřil svoji činnost během „denní rutiny[3]“.

Pokud se tedy útočníkovi povede, aby jeho útok spadal do takzvané „denní rutiny“, má mnohem větší šanci na úspěch. Využije totiž faktu, že není možné využít naši nejlepší ochranu, protože nebude možné nad útokem přemýšlet, ale budeme okamžitě jednat.

Pokud si tedy položíme otázku: Jakým způsobem by metodu využil útočník pro dosažení výše uvedené situace na příkladu? Odpovědí na tuto otázku je právě Pretext Development. Útočník při využití této metody využije všechny zjištěné informace z OSINTu právě k tomu, aby vytvořil věrohodnou záminku k útoku. Útočník však nebere v potaz pouze zjištěné informace, ale i předpokládané problémy. Tuto situaci popisuje Ch. Hadnagy, kde detailněji rozvádí činnost tvoření přesvědčivého (věrohodného) pretextu [2]. Věrohodný pretext by měl podle Ch. Hadnagyho odolat před očekáváním, které je na něj kladeno. Pokud se na pretext začne někdo ptát, tak zkušený sociální inženýr je vždy připraven odpovědět, nezkušený sociální inženýr je však svou nepřipraveností a neznalostí snadno odhalen. Pokud útočník vytvoří pretext, ale pak není schopen zodpovědět základní otázky, které by pravá osoba v jeho situaci znala, bude podezříván či úplně odhalen.

Existují však i situace, kdy se útočníka nikdo na žádné otázky ptát nebude. I tam však útočník využívá pretextu, právě aby této situace dosáhl. Tímto příkladem může být ochranka, která se přece nebude ptát někoho, kdo je oblečen jako uklízeč a vytírá podlahu, jestli opravdu uklízí. Naopak, často jim dokonce unikne důležitý detail, například že uklízeč má suchý mop. V mozku totiž existuje předsudek o uklízečích, a to že uklízí. Proto, když ho vidíme uklízet, tak si ho dále nevšímáme. Toto je další nedokonalost lidského myšlení, kterou

[3]Denní rutina – opakující se běžné denní aktivity [6]

sociální inženýři s oblibou využívají. Samostatná záminka musí být tedy z pohledu útočníka zkonstruovaná tak, aby byla věrohodná pro dané prostředí. Pokud uvidíme po budově právnické firmy chodit klauna, asi nám to bude divné. Ale kolem cirkusu by se nad ním nikdo ani nepozastavil.

Je vhodné uvědomit si, že záminka může sloužit jen jednomu účelu, například dostat se do budovy, a poté ji útočník zahazuje a používá dále jinou. Lze předpokládat, že čím více dochází ke zvyšování složitosti útoku, tím více záminek bude využito a tím více existuje možností selhat. I když jsme si zde představovali dosti přehnané případy z důvodu snadného pochopení, využívání záminek je naprosto běžné a dané záminky jsou málokdy takto jasné.

Otázka potom zní, jak se proti využívání pretextu bránit. Zde již můžeme uplatňovat obranu efektivněji, je zde několik možností. Například můžeme seznámit personál s možnostmi tohoto útoku a provádět školení, která by je měla připravit. Další možností je sestavit systémy a ochranu tak, aby tyto lidské slabiny byly brány v potaz.

Na závěr podkapitoly se opět podíváme na „ Whurleyho [1]“ útok. Již při získávání informací použil „Whurley“ záminku zisku pozice ve finančním sektoru Las Vegas aby vymámil informace o cíli od finančního auditora pracujícího pro cíl. A záminku auditora pak znovu používá při samotném útoku.

4.1.3 Attack Plan

V další části sociálního inženýrství si již útočník zjistil dostatek informací o svém cíli a má připravenou záminku či záminky, se kterými bude pracovat, a cílem je tedy sestavení vlastního plánu útoku. Je však velmi důležité pochopit, co je cílem útoku a jakých výsledků chtějí útočníci dosáhnout či jaký nevhodnější čas pro útok

zvolit, popřípadě jaká omezení jsou s útokem spojena [2]. Dalším bodem, na který můžeme poukázat, je možnost mít někoho připraveného pro nouzovou pomoc nebo rozptýlení [2].

Pro plánovaný útok je ideální vytvořit hrubý plán bez zbytečných detailů, protože jak říká Erwin Rommel: „Žádný plán nepřežije kontakt s nepřítelem“ [7]. Dobrý sociální inženýr by měl prokázat schopnost umění improvizace. To, co bychom mohli považovat za na první pohled taktiku spoléhající z části na nepřipravenost, může být ve skutečnosti velmi reálná a efektivní strategie. V reálné situaci totiž není možné spoléhat na to, že máme k dispozici veškeré informace. Naopak by tento předpoklad mohl vést k neúspěchu. Také není možné při plánování brát v potaz nezměrné množství faktorů a detailů, které budou ovlivňovat samotný útok. Bohužel, nebo snad bohudík, se stává i to, že celý útok selže na tom, že daná osoba má špatnou náladu a snaží se podvědomě znepříjemnit den ostatním nekompromisním dodržováním předpisů nebo dokonce přesahováním nároků těchto předpisů. Na druhou stranu, útok, který by za normálních okolností musel selhat, se za specifických okolností může úspěšně uskutečnit. Zmíněná osoba v tomto případě může odcházet ze společnosti, a tak ji již tolik nezáleží na dodržování postupů. Kolem tohoto lidského faktoru je nemožné plánovat, útočník se s uvedenou situací musí vyrovnat. Do stejné kategorie budou spadat i zcela náhodné situace. Zdatný útočník si však může podobných situací všimnout a využít tyto situace ve svůj prospěch.

Ve „Whurleyho [1]“ případě je plánování popsáno minimálně. Můžeme z dalšího textu vyvodit, že plánování bylo nedostatečné nebo alespoň neúplné. „Whurley“ sám sebe popisuje jako příliš sebevědomého a i množství situací, kdy se musí spolehnout na rychlou improvizace tomuto faktu nasvědčuje.

4.1.4 Attack Launch

Pokud byl již proveden sběr informací, je připravená vhodná záminka k útoku, byl vytvořen plán a vybrán i konečný cíl útoku, je možné plánovaný útok uskutečnit. Představíme si tedy nejčastější vektory útoků sociálního inženýrství a metody manipulace v nich využívané. Podrobnějším informacím o jednotlivých typech útoků bude věnována vlastní kapitola 4.2.

Prvním zmínkou je fyzický útok, také zvaný impersonace, uvažován v těchto mezích: útočník se snaží osobně překonat ochranu a to většinou předstíráním. Příkladem nám může být „Whurleyho [1]“ útok, kdy se pomocí sociálního inženýrství dostal přes ochranku a později předstíral že je z interního auditu aby se mohl volněji pohybovat po budově.

Další a možná známější metodou je phishing. Phishing je útok realizovaný přes email a jeho nejznámější formou je email od „Nigerského prince“ [2]. V tomto případě se pomocí emailu útočník snaží získat peníze, avšak phishing lze použít i pro zisk informací nebo pro přenos škodlivého softwaru.

Vishing je pak forma útoku přes telefonní hovor [2]. Dříve používaná spíše pro zisk informací nebo přístup do systému, v dnešní době, kdy existuje možnost uzavření smluv po telefonu, se tento typ útoku stává mnohem závažnějším.

Smishing je obdoba phishingu tentokrát však přes SMS. I když jsou si tyto útoky do jisté míry podobné, při bližším pohledu se zde nacházejí značné rozdíly v přístupu a struktuře. U phishingu musí být email koncipován s porozuměním, že mu bude věnován dostatek času. Většinou si emaily čteme v klidu, často pro ně dokonce máme vyhrazený časový úsek. U smishingu je naopak nutno uznat fakt, že SMS řešíme v okamžiku, kdy přijdou. Většinou také co nejrychleji,

protože přerušují jinou činnost, ke které se chceme vrátit. To na útok klade jiné nároky ale také mu dává nové možnosti.

I když známe, jaké druhy útoků sociální inženýrství jsou využívány, neznamená to, že je umíme zastavit. Daniel Kahneman ve své knize představuje fungování lidského myšlení, které může být zneužito k manipulaci [4]. Chceme-li tuto manipulaci opravdu prozkoumat, musíme však tyto informace sloučit s postupy, které jsou k manipulaci často využívány a také ukázat, jak jsou postupy používány, aby byly co nejvíce efektivní. Robert B. Cialdini za tímto účelem charakterizuje jak je možné zmanipulovat cíl za použití na pohled jednoduchých avšak velmi efektivních technik [5]. Těmto technikám a principům je opět věnována vlastní kapitola 4.3, kde je detailněji vysvětleno a upřesněno využití technik sociálního inženýrství v konkrétních příkladech (kontextu).

4.1.5 Reporting

Tato část je zaměřena na vyhodnocení provedeného útoku a následnou tvorbu hlášení, které má fungovat jako zpětná vazba k tomuto útoku. Rozhodně se tak netýká normálních útoků. Útočníci podávají někomu dalšímu hlášení pouze, pokud na útok byli najati, jako v případě „ Whurleyho [1]“. Část hlášení se tedy týká specialistů na ochranu, kteří byli najati na takzvaný „pentest“. Pentest je simulovaný útok, který může být dle požadavků celý založen na sociálním inženýrství, obsahovat ho, nebo se mu naopak vyhnout. Je jisté, že takto uměle zadané okolnosti ovlivní přenositelnost výsledků ke skutečnému útoku, mnohdy se však zadavatel snaží posílit jen určitou oblast své ochrany [2]. Je důležité, aby slabiny nalezené v rámci útoku byly specialistou provádějícím tento útok zaznamenány a aby bylo z těchto slabin sestaveno hlášení, kde specialista nalezenou slabinu nejen dopodrobna popíše ale také může doporučit, jak jednotlivé slabiny odstranit nebo alespoň minimalizovat [2]. Proto, i

když je tomuto hlášení věnována nejmenší část pyramidy, je kriticky důležité.

Ve „Whurleyho [1]“ případě je hlášení stejně jako v pyramidě věnována pouze malá část na závěr. Je nutné podotknout, že zaměstnavatel nebyl s „Whurleyho“ výsledky spokojen. Ne však kvůli špatně provedenému útoku ale protože naopak ukázal skutečnou zranitelnost kasina a kasino by tak mohlo přijít pod hledáček státních orgánů.

4.2 Typy útoků

Jak již bylo v předchozích kapitolách uvedeno, v rámci sociálního inženýrství můžeme rozlišovat několik typů útoků. Jelikož jsme si již představili a charakterizovali jednotlivé části útoku sociálního inženýrství, je načase, aby jsme si blíže přiblížili jednotlivé typy, ukázali, jak se od sebe liší a v čem je jejich hlavní hrozba. Předem je však dobré znát, že v rámci útoku sociálního inženýrství není neobvyklé, aby jednotlivé typy útoku zde představené na sebe navazovaly. Zlepšuje se tak totiž jejich efektivnost. Příkladem můžeme představit kolaboraci vishingu a phishingu, kde útočník po předchozím zjištění členství cíle v určitém systému nejdříve po telefonu získá dodatečné informace. Útočník také upozorní cíl na „chybné informace“ v systému, aby mohl cíli přirozeně navrhnout cestu nápravy této situace přes email, kde zašle odkaz na stránky pro korekci těchto „špatných informací“. Útočník má takto záminku zaslat phishingový email s odkazem, kde cíl nebude přemýšlet o validitě emailu, jelikož ho očekává, a zároveň bude cíl takto mnohdy ochoten zadat více informací, než by byl ochotný zdělit po telefonu při samotném vishingu.

4.2.1 Phishing

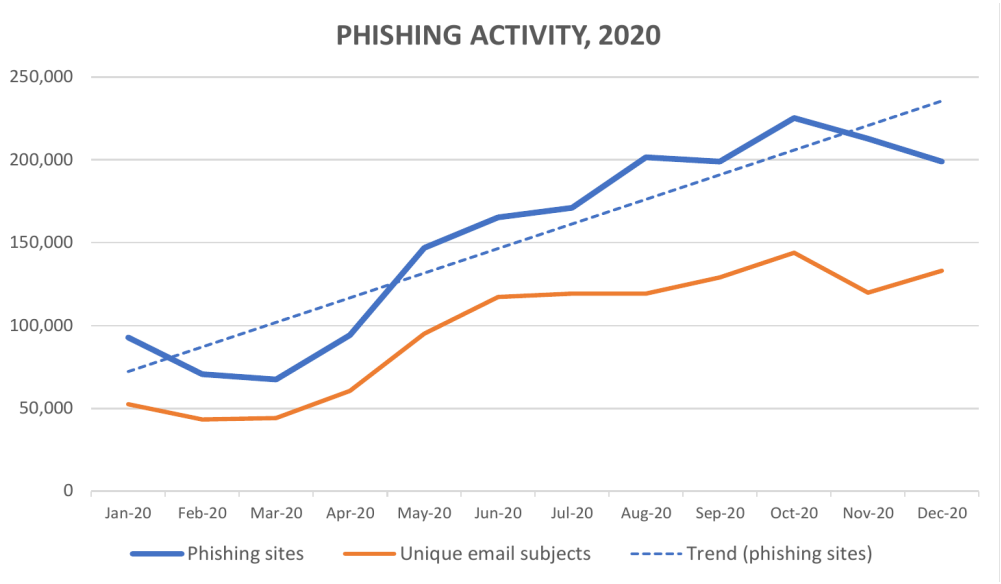
Phishing je metoda útoku s cílem získání osobních informací, manipulace nebo získání přístupu do uzavřeného systému za pomocí emailové komunikace [2]. Stejně jako mnoho dalších útoků z kategorie sociálního inženýrství, phishing využívá k úspěchu nepozornost, neznalost a nebo samotnou psychologickou dispozici jedince. Jedním z typických příkladů phishingu je HOAX[4]. To je mail, který je zasílán uživatelům a vyžaduje zadání přihlašovacích údajů k internetovému bankovnictví. Je samozřejmostí, že pokud přijde mail, kde se nás bude někdo neznámý ptát na přihlašovací údaje k bankovnímu účtu, budeme podezřívaví a nebudeme odpovídat. Co když však přijde email od naší banky s tvrzením, že se stala chyba a musíme se přihlásit přes přiložený odkaz, aby se ji mohli pokusit napravit?

Pokud však odesílatelem není naše banka ale útočník, odkaz obsažený v emailu bude podvodný. Pokud na něj klikneme, pravděpodobně se dostaneme na stránku, která bude vypadat identicky se stránkou naší banky. Zde se pak objevují dvě možnosti. V lepším případě stránka selže v okamžiku,kdy získá požadované udaje. Tak můžeme okamžitě poznat že něco není v pořádku. V horším případě narazíme na variaci MITM[5] útoku, kdy nás stránka přesměruje na pravou, takže si ani nevšimneme napadení.

Princip phisnigu je tedy založen na falešné identitě s cílem získání důvěry uživatele pro získání požadovaných soukromých, osobních a citlivých informací za účelem možného obohacení. Tento typ útoku klade velmi malé nebezpečí na útočníka a tak nemůže být překvapením, že phishingové formy útoků jsou nejrozšířenější formou

[4]HOAX – podvody, které zneužívají uživatele k získání cenných informací. Útočníci jsou obecně finančně motivovaní a budou používat různé metody útoku včetně phishingu, vishingu, pop-up oken a sociálních médií. [8]

[5]MITM – Man-in-the-middle – styl útoku kdy útočník získává informace monitorováním komunikace mezi obětí a cílem oběti. [9]



Obr. 2: Phishingová aktivita

Zdroj: [10]

útoků v sociálním inženýrství [2]. Jeho četnost navíc rok od roku narůstá a tak můžeme předpokládat, že tento trend a oblíbenost útoku ze strany hackerů bude mít rostoucí tendenci [10]. Statistiku počtu útoků v oblasti phishingu za rok 2020 můžeme vidět zobrazenou na obr. 2.

Nebezpečí Phishingu

Jak již bylo naznačeno, hlavní nebezpečí phishingu spočívá v jeho nenápadnosti. Pro lepší pochopení problematiky phishingu si můžeme demonstrovat funkčnost na třech případech.

Pokud najdeme přední dveře budovy vytržené z pantů, již z dálky s jistotou víme, že se do budovy někdo vloupal.

Kdyby byla provedena destruktivní manipulace pouze na zámku, například vyvrtání, vloupání poznáme až když přijdeme ke dveřím blíže.

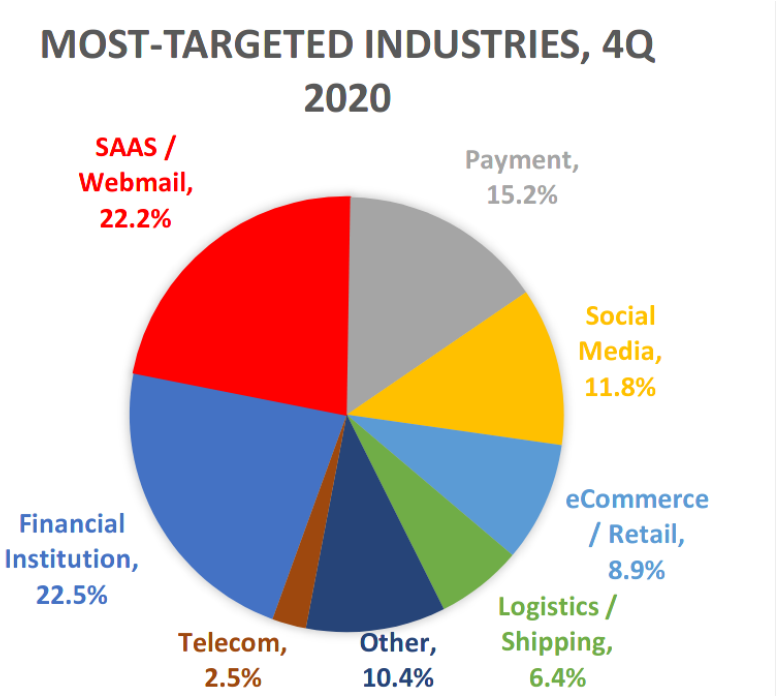
Pokud však nastane situace, kdy byl zámek otevřen nedestruktivní metodou, nemusíme si ani všimnout, že byla bezpečnost budovy

narušena. Odezva na vloupání je pak buďto delší a nebo v nejhorším případě žádná, pokud si vloupání vůbec nevšimneme.

Phishing se bohužel podobá nejvíce třetímu případu, kdy si cíl útoku mnohdy nemusí uvědomovat, že byl napaden a tak nemůže podstoupit kroky, aby zamezil následkům útoku. Tato skutečnost platí dvojnásobně u útoků s cílem získání přístupu do systému, kde si útočník po prvotním úspěšném průniku může najít nebo dokonce vytvořit další slabiny, které mu umožní návrat do systému a to i pokud byl prvotní útok později odhalen a bylo zamezeno útočníkovu přístupu prvotní metodou [1].

Je tedy velmi důležité útoky v podobě phishingu nepodceňovat. Pokud bychom se zeptali populace, s jakým typem klamavých emailů se doposud setkali, tak většina z dotázaných poukáže na případ emailu „Nigerijského prince“, který musel dostat zlato ze země a žádal o pomoc většinou malou dotací se slibem následného rozdělení o své bohatství jako odměnu za pomoc. Tento stereotyp je bohužel tak známý, že velmi zlehčuje pro běžnou populaci nebezpečí phishingu. Panuje totiž představa, že nikdo na tak jasně podvodný email nebude odpovídat a nemá tedy cenu phishing brát jako významnou hrozbu. Výše uvedené je možné dále demonstrovat na dalším příkladu, kdy je potvrzeno, že opak je pravdou. Jako nejvhodnějším příkladem se jeví poučení ze situace okolo COVID-19. Autoři článku „Why is phising still succesfull“ [11], popisují situace, kdy vědci zaznamenali nárůsty útoků phishingu spojených s pandemií COVID-19. Google například zaznamenal zastavení přes 250 milionů COVID-19 spam a phishing emailů [11].

Data z roku 2019 také ukazují, že 88 procent tázaných společností utrpělo v daném roce nějaký typ phishingového útoku a úspěšné útoky také způsobili minimální škodu 3,5m dolarů [11]. To dokazuje, že je důležité o nich mluvit, zkoumat, rozpoznávat a hlavně zvyšovat



Obr. 3: Nejvíce napadaná odvětví průmyslu

Zdroj: [10]

ochranu v podobě prevence v oblasti informační bezpečnosti. Data z konce roku 2020 poukazují na nárůst phishingové aktivity, dokonce její zdvojnásobení během tohoto roku jak můžeme vidět na obr. č. 2 v této kapitole [10]. Dalšími důležitými daty, které můžeme získat jsou oblasti, ve kterých dochází k nejvíce útokům pomocí sociálního inženýrství jak zobrazuje obr. č. 3.

COVID-19 navíc způsobil ještě jedno nové bezpečnostní riziko, lidé byli donuceni pracovat převážně z domova(HO)[6]. Můžeme pozorovat nejen oportunistické chování útočníků spjaté s využíváním COVID-19 jako materiálu pro phishingové emaily, ale také bezpečnostní rizika nově vzniklá kvůli práci z domova [12]. Firmy dlouhodobě zlepšovali bezpečnost interních sítí, takže jednoduché hackerské nebo phishing útoky byly zaznamenány a odvráceny bez toho, že by si je běžný zaměstnanec vůbec uvědomil. Zaměstnavatelé při vypuknutí pandemie byli nuceni převést své zaměstnance na HO, aniž by byli

[6]HO -Home Office, práce z domova

připraveni na problémy s tím spojené. Zaměstnanci mnohdy pracovali na domácí síti bez zabezpečeného přístupu interní sítě zaměstnavatele, navíc na vlastních zařízeních. Dalo by se tedy očekávat že chování zaměstnanců v domácím prostředí bude uvolněnější vlivem domácího prostředí, avšak jejich ochrana dramaticky klesla. Zaměstnavatelé na vzniklou situaci reagovali až v následujících týdnech po vypuknutí pandemie COVID-19.

Mnozí zaměstnanci využívají nezabezpečených hesel např. PIN k bankovní kartě, datum narození či rodné číslo. Právě tyto údaje jsou lehce zneužitelné a vznikly různé statistiky, které se zobrazují seznamy nejvyužívanějších hesel [13]. Většina firem také stále využívá jako jedinou nutnost k přihlášení heslo neboli jedno-faktorové přihlášení [12]. To je z hlediska bezpečnosti v současné době už považováno za nedostačující, obzvláště v dané situaci. Tato hesla jsou v mnoha případech jednoduše odhadnutelná nebo dokonce tvořená automaticky podle firemních pravidel. Příkladem může být jméno spojené s číslem pracoviště, kdy je možné tyto informace jednoduše dohledat nebo získat pomocí sociálního inženýrství. Tyto statistiky dále zobrazují, že 39% zaměstnanců používá stejné heslo pro všechny programy a účty související s prací a až 51% své heslo sdělilo kolegům [12].

Principy funkčnosti

Odpovědět na otázku, proč phishing funguje, není vůbec jednoduché. Phishing totiž není tak zřejmý, jak by se mohlo na první pohled zdát. Klasické hackerské útoky na systémy se mnohdy zaměřují na jednu specifickou slabinu, kterou využijí ve svůj prospěch, ať už to je k vytvoření jiné slabiny a poté s efektem laviny prolomení celkové obrany, nebo pouze k získání informací z určité části systému, do které byl pomocí slabiny získán přístup. Tyto slabiny lze dobře analyzovat, zdokumentovat a pokud byly nalezeny, tak ve většině

případů není problém je opravit. Slabiny se totiž nachází v systémech, které jsme my lidé plně vytvořili a kolektivně jim rozumíme, i když mnoho slabin vzniká chybou na úrovni jednotlivce. A tímto se dostáváme k hlavnímu problému. U klasické obrany systémů není problém jednoduše posílit a odstranit nalezené slabiny. Phishing je z velké části zaměřen na člověka a jeho kognitivní schopnosti. Přesněji, phishing je zaměřen na psychologické a kognitivní impulsy a chyby, které nejsou pod naší vědomou kontrolou. Pomineme-li technické pomocníky, kteří odbourávají nejjednodušší druhy phishingu, celý zbytek obrany je plně na bedrech člověka. Lidstvo dostalo člověka na měsíc, pomalu se připravuje kolonizovat další planety v naší sluneční soustavě a dokonce vysílá družice pro zkoumání vesmíru mimo naši sluneční soustavu. I tak však na Zemi existují místa, která nejsou plně prozkoumána. Stejně tomu tak je s psychologií a zkoumáním lidského mozku, i přes to, že toho víme mnoho, existuje velké množství podstatných detailů, které neznáme nebo dokonce interpretujeme špatně. A i když víme, že některá část nefunguje tak, jak bychom chtěli, máme jen málo možností, jak je změnit. A oproti vylepšení systému, který je v rámci dnů či měsíců, nám může úprava trvat roky, nebo se nemusí zdařit vůbec. I proto je tak důležité zkoumat phishing a sociální inženýrství, protože nám pomáhají ukázat zranitelnost a nedokonalost vlastní mysli. A první krok úpravy k lepšímu je poznat, že je něco špatně.

Dodatečné dělení

Útoky phishingu lze pro zpřehlednění dále rozdělit podle cíle samotného útoku. Jistě není překvapující, že samotná podstata útoku ale i jeho složitost, provedení či nebezpečí záleží na tom, jak velké množství lidí se snažíme útokem zaměřit. Stejně jako jsou v dnešní době politické či komerční kampaně zaměřené na určitou skupinu jedinců, tak i phishingové útoky jsou sestaveny tak, aby byli co

nejefektivnější oproti jejich cílové skupině. To je sice činí absolutně neúčinné při útoku na jinou skupinu, to však útočníkům nevadí. Naopak je překvapivé, že útočníci specializující se na phishingové útoky se naučili i tento fakt používat ve svůj prospěch.

Můžeme tedy útoky dělit do těchto 4 skupin:

- Jednoduché útoky
- Složité útoky
- Spear Phishing
- Whaling

Jednoduché útoky

Stejně jako se vším, i u vysvětlování útoků phishingu je dobré začít od nejjednodušších, nejrozsáhlejších a v našem případě i nejznámějších útoků. Jsou to útoky typu Nigerisjký princ, COVID-19 nebo „odpovězte na tento email a vyhrajte“. Společným znakem těchto útoku je jejich nevázanost na jedince a poměrně nízká sofistikovanost. Jejich účelem je pokrýt co největší množství populace. Jsou to útoky zaměřené na množství, ne na kvalitu. I zde si však musíme dávat pozor, ve speciálních případech stačí pouze kliknout na odkaz nebo stáhnout jediný soubor.

Asi největší ironií je, že těmto útokům napomáhá jejich jednoduchost. Jak již bylo naznačeno dříve, útočníci začali čím dál více pracovat s tendencí lidí neodpovídat na emaily, které jsou naprosto jasně falešné. To však funguje jako filtr pro útočníky, kteří se v rámci času naučili strukturovat útoky takovým stylem, aby na ně odpovídali jen jedinci, kteří jsou na tento typ útoku náchylní. Tato filtrace tedy pomáhá útočníkům ušetřit čas. Vysílání tisíců až milionů emailů produkuje jen desítky odpovědí u kterých je však šance úspěchu maximalizována.

Závěrem je vhodné podotknout, že díky pokroku ve spam-filtrech a umělé inteligenci, která automaticky odpovídá na podvodné emaily za účelem maření času útočníku, se četnost těchto útoků rok od roku snižuje. Příkladem je snížení z roku 2019 do roku 2020 o 42 procent [14] [15].

Složité útoky

Složitost spočívá v práci, kterou musel vynaložit útočník, aby napodobil jinou již existující entitu a tím zmátl cíl útoku. Pokud jsme tedy u jednoduchých útoků řešili emaily, na které čekal útočník odpověď ze strany uživatele nebo v nich byl již obsažen škodlivý odkaz, u složitějších útoků se k tomuto přidává navíc ještě vrstva maskování.

Velmi oblíbenou taktikou útočníků je totiž předstírání, že jsou velké organizace s dobrou reputací nebo jsou s ní alespoň asociováni. Je totiž velmi jednoduché ignorovat email, který požaduje informace zaměřené na získání osobních údajů, když přichází z neznámé adresy. Nebo email, ve kterém útočník požaduje dodatečné informace k doručení zásilky od služby, která je nám neznámá. Chování však bude jiné, pokud odesilatelem emailu se zdá být známé jméno, kde je v současné době zasílání emailů standardem, např. Google, Amazon či Česká pošta. I člověk s velmi dobrou znalostí informační bezpečnosti však může být oklamán, pokud se sejdou správné okolnosti v jeho neprospěch. Pokud například byl očekáván balík, který měl přijít již včera a najednou mu přijde email od PPL s tím, že je nutné doplnit dodatečné informace, aby mu mohl být balík doručen, tak uživatel nebude váhat a informace doplní doufajíce v urychlené doručení. Toto je sice velmi specifická situace, která může nastat jen s velmi malou pravděpodobností, důležitým faktorem ale je, že pravděpodobnost není tak malá, aby byla zanedbatelná. I uživatel mající velmi dobré znalosti v oblasti informační bezpečnosti

může v daný okamžik a v dané situaci podlehnout,což je přesně myšlenka složitějších útoků. Demonstrujícím příkladem může být událost, kterou řešil Google. Společnost Google má velmi dobrou pověst a proto existuje značné množství útoků, které předstírají, že jsou asociovány přímo s touto firmou. Pokud si však uživatel pořádně prohlédne stránku na kterou ho v emailu odkazují, zjistí že to není GOOGLE s dvěma o ale G00GLE s dvěma 0(nulami).

Tyto útoky mají menší pole působnosti než ty jednoduché, bohužel však bývají zákeřnější. I když ze začátku bylo používáno pouze odkazovaní na chybnou stránku k zisku údajů, dnes jsou konfigurovány odkazy tak, že po přihlášení na chybnou stránku, která vypadá stejně jako ta pravá, vás tato podvodná stránka přesměruje na tu pravou. Stane se tedy situace, kde si uživatel vůbec nemusí uvědomit, že by bylo něco špatně. Toto je velmi nebezpečné hlavně u internetového bankovnictví, kdy můžeme dát útočníkům přístup k našemu bankovnímu účtu i přes to, že používáme dvoustupňovou (více-faktorovou) autorizaci.

Spear Phishing

Ještě náročnějším typem útoku je pak spear phishing. Tam, kde se předchozí útoky soustředily na různě velké skupiny uživatelů, spear phishing je soustředěn pouze na jeden jediný cíl. A co ztrácí na univerzálnosti a šířce použití, to získává na efektivitě a nebezpečnosti. Představme si email, který je vytvořen specificky pro nás. Email, kde útočník strávil týdny až měsíce hledáním jakékoli informace, která je o nás dostupná. Email, vytvořený útočníkem za jediným účelem, prolomit naši obranu. Tohle je spear-phishing. V dnešní moderní bodě je až překvapivé, jak jednoduché je nalézt informace o jedinci, pokud útočník ví ,kde a jak hledat. A díky globalizaci je tato činnost stejně jednoduchá jak pro útočníka, který

se nachází ve vašem městě, tak pro útočníka na druhé straně planety.

Pokud by si někdo myslel, že spear-phishing je díky množství vynaložené práce vzácný a málo využívaný útok, podívejme se na data. Podle statistik ze Security Boulevard, 88% tázaných organizací se setkalo s tímto druhem útoku za rok 2019, 46% se pak setkalo s vydíráním spojeným s tímto útokem [16]. Tam, kde jednoduché phishing útoky jsou úsměvné a složité útoky nejsou až tak velký problém, pokud si člověk dává velký pozor, spear-phishing ukazuje pravou hrozbu. Je to asi jako rozdíl mezi generickým oblekem prodávaným v obchodě a značkovým oblekem šitým na míru.

Whaling

Tento specializovaný termín se používá pro specifickou kategorii spear-phishingu, a to spear-phishing zaměřený na vysoce postavené či důležité cíle. Přirovnání k lovu velryb je opravdu přesné. Je pravdivou skutečností, že i když má firma velmi dobře postavenou obranu proti sociálnímu inženýrství a phishingu specificky, vysoce postavení zaměstnanci tato opatření často ignorují, protože se na ně „nevztahují“. A tato chyba je o tolik horší, uvědomíme-li si fakt, že takto vysoce postavené osoby mají přístup k velkému množství citlivých dat. Často mají privilegované přístupy do firemních systémů a jsou v pozici moci, kterou může útočník použít k útoků na další části firmy. Existence whalingu nám tedy ukazuje, že sebelepší opatření proti phishingu budou neúčinná, pokud se nebudou dodržovat. A pokud by snad někdo argumentoval, že nedodržování principů od malé skupiny jedinců neohrožuje celou skupinu, můžeme jim připomenout situaci ohledně COVID-19.

4.2.2 SmiShing

Smishing byl méně používaný způsob útoku sociálního inženýrství. Tyto podvodné SMS jsou z velké části podobné phishingu, vyznačují se však svojí stručností a způsobem manipulace cíle. Stejně jako je jiný přístup k vyřizování emailů a SMS, tak jsou jiné požadavky na tyto útoky. Smishing je tedy stručnější, více reaktivnější forma útoku.

Nebezpečí Smishingu

Smishing může kompromitovat mobilní zařízení. To v minulosti asi nebyl moc velký problém, avšak novodobé mobilní zařízení se stávají pro náš život stále důležitějšími. Nejen že mnoho zaměstnavatelů povoluje využívání vlastních telefonů pro pracovní činnost ale novodobá integrovanost přihlašování v rámci 2-fázové autentizace nebo internetové bankovnictví z aplikace činí mobilní zařízení stále lákavějším cílem. Pokud se tedy útočníkovi podaří ovládnout mobilní zařízení cíle, získá přístup nejen k emailům a fotografiím uložených na zařízení ale může také vzdáleně zapnout kameru či mikrofon nebo využít zařízení jako přístup do zabezpečené sítě [2]. Kevin Mitnick tento problém rozvádí dál, a ukazuje, jak jediné prolomené zařízení dokáže kompromitovat zabezpečení celé sítě [17]. S příchodem zařízení ovládaných hlasem se zvýšila pravděpodobnost útoků na uvedená zařízení, protože tato zařízení mohou neustále poslouchat prostor, ve kterém se nachází a pokud se k nim dostane útočník, může z nich bez větších problémů tento odposlech získávat. Takové zařízení nacházející se v zasedací místnosti, nebo na stole ředitele velké firmy je pak značná bezpečnostní hrozba.

Principy funkčnosti

Mnoho principů je zde stejných jako u phishingu, liší se hlavně v tom, jak obyčejný uživatel přistupuje k mobilnímu zařízení. Smishing má tendence být stručnější, využívat zkrácené URL, jelikož je skoro nemožné si je nechat rozepsat a málokdo se s o to bude vůbec snažit,

a hlavně využívat postupy vyžadující méně kroků ke splnění od cíle, protože příliš složité požadavky na cíl způsobí ztrátu jeho motivace je splnit [2]. Toto by se mohlo zdát jako jakýsi méně propracovaný phishing ale není tomu tak. Pokud například útočník využívá podvodné stránky pro získání přihlašovacích informací, musí být stejně propracované jako u phishingu. Útočníci zde pouze korektně využívají tendence a zvyky běžných uživatelů mobilních zařízení. Jsme totiž zvyklí, že SMS jsou stručnější. Také jsme zvyklý vyřídit SMS okamžitě, většinou protože jsou přerušením již probíhající činnosti ke které se chceme vrátit. Z těchto důvodů je stručnost smishingu a jejich urgentnost jistou výhodou pro útočníka, protože na nás tvoří tlak konat a nepřemýšlet nad tím, co vlastně děláme. Pokud je však SMS moc dlouhá nebo jsou vyžadované kroky moc zdlouhavé, hrozí že ji odložíme na později a máme tak čas přemýšlet o ní, až se k ní vrátíme ve vhodnějším čase. Obranou nám tedy zde může být vypůjčení metod od emailů. Musíme věnovat každé SMS dostatek času a zbytečně nespěchat a přehlížet tak detaily nebo související skutečnosti, které by nám pomohly falešnost odhalit.

4.2.3 Vishing

Vishing lze velmi zjednodušeně popsat jako phishing, ale po telefonu. Zní to velmi jednoduše, i zde se ale nachází nástrahy, které si musíme představit. Volání po telefonu je totiž velmi odlišné od čtení emailů a to znamená, že i obrana a útok se značně liší, a to i přes to, že cíle vishingu jsou téměř stejné jako cíle phishingu. Cílem je tedy získat informace nebo manipulovat cíl pro provedení nějaké akce, která není v jeho nejlepším zájmu. Vishing se však výrazně liší mírou pasivity, nebo spíše aktivity útoku. Tam kde phishing je pasivní a po sestavení a odeslání nemá útočník šanci s cílem jinak interagovat a je tedy pasivní, vishing dává útočníkovi zpětnou vazbu během samotného útoku. Z tónu hlasu a výběru slov totiž může útočník

poznat informace, které ho donutí pozměnit přístup útoku aby dosáhl lepších šancí úspěchu.

Nebezpečí Vishingu

Hlavní účel vishingu se pohybuje okolo získávání a verifikace informací. Christopher Hadnagy například ukazuje, jak pomocí vishingu potvrdit informace již získané v OSINTu, získat nové informace ale hlavně a možná i překvapivě, jak pomocí vishingu kompromitovat bezpečnost celého systému [2]. I když přes vishing nejde poslat kompromitující soubor, i tak lze pomocí dobře sestaveného útoků získat přístup do systému. Někdy stačí zjistit login a heslo, jindy je potřeba pomoc cíle, například telefonické podpory dané společnosti, aby nám pomohla nastavit vzdálený přístup. To vše však znamená, že ač se vishing může zdát neškodným, opak bývá pravdou.

Třešničkou na pomyslném dortu pak můžeme brát skutečnost, že po telefonu lze v České republice uzavírat legálně platné smlouvy, a to již od roku 2012. Toto kontroverzní téma vyvolalo hned několik změn zákona. Ministerstvo spravedlnosti se například v roce 2019 pokoušelo tuto možnost zrušit. Uzavírání smluv po telefonu je však stále možné a je tedy nutné toto nebezpečí brát v potaz. Pro více informací je možné nahlédnou do Nového občanského zákoníku, paragraf 1820 a dále [18].

Principy funkčnosti

Hlavní výhoda vishingu spočívá v jeho rychlosti. U emailu má člověk čas se zastavit a přečíst si detaily znovu, u telefonního hovoru tato možnost však není. Proto je u vishingu menší důraz na detaily a větší na samotnou manipulaci a ovlivňování. To však neznamená, že vishing lze uskutečnit bez jakékoli přípravy. OSINT je stejně důležitý jako u jiných útoků a dobře vytvořený pretext bude útočníkovi značně usnadňovat útok.

Navíc je zde oproti phishingu mnohem jednodušší využití emocí a manipulačních technik, popsaných v dalších kapitolách. Pokud se útočníkovi povede takto manipulovat cíl, často je ochoten vydat informace nebo dokonce provést akce, které jsou jasně proti jeho nejlepšímu zájmu, jen aby útočníkovi pomohl. Rychlost takového útoku značně stěžuje obranu, možnosti však existují. Chistopher Hadnagy například popisuje případ, kde byl systém postaven tak, aby nebylo možné přes vishing z cíle útoku cokoli získat, jelikož systém samotný nepovolil přístup, dokud do něj nebyly zadané potřebné informace, ke kterým cíl sám o sobě neměl přístup [2]. Také různá školení a už samotné seznámení s možností vishingu zvyšují bezpečnost.

4.2.4 Fyzický útok

Jako fyzický útok sociálního inženýrství můžeme klasifikovat takové útoky, kde se útočník musí fyzicky dostat k cíli [2]. Příkladem může být třeba snaha dostat se k určitému počítači, serveru či korespondenci nacházející se v dané lokaci za účelem dalšího využití. Je zřejmé, že útočník se vystavuje značnému nebezpečí, pokud se pokusí tento typ útoku provést, proto bývá jednou z posledních možností a je rozhodně vzácnější, než ostatní typy útoků, které již byly zmíněny. Tento typ útoku však má před jinými i jisté výhody, takže rozhodně nelze brát pouze jako poslední možnost zoufalého útočníka. Není neobvyklé, že z internetu výborně zabezpečené servery či celé sítě jsou minimálně zabezpečené zevnitř. A pokud se tedy útočníkovi nepodaří útok zvenčí, útok zevnitř má mnohem větší šanci úspěchu. Záleží tedy jen, jestli útočník identifikoval při sběru informací nějakou slabinu a jak ji může využít. Druhou a podstatnou výhodou je maximalizace zpětné vazby při samotném útoku. Nový zisk informací nonverbálních, které opět pomáhají útočníkovi k rychlým opravám v jeho přístupu k útoku, spojený s ostatními

informacemi činí tento útok velmi náročným ale také flexibilním a účinným. Pokud se tedy podíváme na všechny typy útoků které jsme si zde již představili, fyzický útok je sice nejrizikovější ale také poskytuje zkušenému útočníkovi nejvíce možností úprav dle nových informací, získaných přímo při útoku. Také celkové spektrum informací poskytuje největší možné využití manipulačních technik.

Nebezpečí Fyzického útoku

Jak jsme již představili v předchozí části, vnitřní ochrana sítí, či počítačů je téměř vždy menší, než ochrana zvenčí. To dává smysl, jelikož se počítá s běžným užíváním a nadbytečná ochrana by mohla zhoršovat tento primární cíl. Navíc existují jiné ochrany, které by nás měly chránit před vnitřním útokem, například ochranka na vrátnici, nebo zamčené dveře do místnosti, kde se nachází servery. Cílem útočníka je tedy aby obešel tyto ochrany. Sociální inženýr však nebude používat hrubou sílu, aby otevřel zamčené dveře, jeho preferovanou metodou je přesvědčit někoho jiného aby mu dveře otevřel a ještě mu je podržel při vchodu dovnitř. Tento typ útoku navíc umožňuje útočníkovi využívat snad všechny triky, které mu sociální inženýrství nabízí.

Na co je však potřeba se zaměřit, je dopad úspěšného útoku. Pokud se útočníkovi povede dostat do systému přes phishing, je stále omezen možnostmi systému. A tak si sice přečte emaily uložené na serveru ale klasická pošta, či cokoli mimo napadený systém mu zůstane skryté. Při fyzickém útoku však má útočník mnohem více možností. Pokud se tedy útočníkovi povede dostat přes ochrany až k svému cíli, může vytvořit slabiny pro přístup z venčí. Může pořídit fotky nebo videa o čemkoli, k čemu se dostane. V nejhorším případě může také uplatnit odposlouchávací či nahrávací zařízení, která buďto budou posílat data mimo, nebo nahrávat na interní paměť pro

pozdější vyzvednutí. Není přehnané říci, že toto je nejzávažnější útok sociálního inženýrství.

Principy funkčnosti

Představíme si zde principy, které je potřeba blíže charakterizovat, aby jsme pochopili principy fungování útoku. Principy funkčnosti dělíme na:

- impersonaci
- lidskou psychologii a manipulaci
- schopnosti útočníka

Prvním a základním principem je impersonace, neboli předstírání, že útočník je někým jiným. Persona, kterou útočník představuje je vždy ovlivněna informacemi, které získal útočník předem. Dobrým příkladem nám může být inspektor, který přišel ve firmě udělat překvapivou inspekci. Tato osoba nebude ohlášena předem ale přesto má dostatečnou autoritu aby se mohla volně pohybovat a „kontrolovat“. A pokud se ji někdo pokusí zadržet a vyptávat se na otázky, má také dostatečnou autoritu aby mu znepříjemnila život ve firmě. [2]

Jiným příkladem může být nový zaměstnanec, který naopak v rámci tohoto pretextu může často žádat o pomoc bez nadměrného vzbuzení pozornosti. Výběr persony pro útočníka závisí na cíli, kterého se s ní snaží dosáhnout. Není neobvyklé, aby použil jednu pro vstup do budovy a pak další pro samotný pohyb po budově, pokud by v tomto případě měla prvotní persona moc velká omezení. Je důležité však podotknout, že pokud bude moct útočník použít pouze jednu personu, udělá to. Každá další vrstva dělá útok složitějším a tím pádem náchylnějším k neúspěchu. [2]

Dalším principem je znalost lidské psychologie a hlavně manipulace. Lze totiž očekávat, že útočník během útoku přijde do styku s dalšími osobami, které mu buďto budou stát v cestě k jeho cíli nebo mu naopak mohou pomoci k němu dosáhnout. Útočník tedy musí umět využít tyto příležitosti ve svůj prospěch, nebo alespoň odvrátit podezření od své osoby. Zde tedy plně přichází umění manipulace, jak přimět ostatní aby ho v krátké chvíli měli rádi natolik, aby mu pomohli, nebo jak přimět osobu, aby porušila nařízení a nejednala ve svém nejlepším zájmu.

Posledním principem jsou pak dodatečné schopnosti samotného útočníka, které nijak nesouvisejí se sociálním inženýrstvím. To, že útočníci preferují, aby jim někdo otevřel dveře neznamená, že sami nemusí umět otvírat zámky, nebo i jiná zabezpečení. Naopak, než riskovat zbytečné hledání potřebné osoby či klíče je často rychlejší a bezpečnější zámek otevřít šperhákem. To je pouze příklad, každý útočník disponuje jinými dovednostmi, které jim mohou útok ulehčit a tak každý útočník bude provádět přípravu i útok samotný s jistými rozdíly.

4.3 Manipulace

Manipulace je velkou součástí sociálního inženýrství, je však důležité uvědomit si, že i přes negativní podtón tohoto slova, je to naprosto běžná součást lidské komunikace. Manipulace, nebo také ovlivňování, je mezi lidmi naprosto běžný a přirozený proces, každý z nás ji zažil a sám někdy využil. Asi nejlepším příkladem si můžeme připomenout výchovu dítěte.

Manipulace o které však budeme mluvit dále nebývá použita pro dobro druhého ale ve vlastní prospěch. A bohužel často platí, že pokud si oběť neuvědomuje manipulaci, má pocit, že akce které provedla byly z její vlastní vůle nebo že byly prospěšné.

Aby jsme se proti manipulaci mohli chránit, musíme rozeznat situace, kdy se námi někdo snaží manipulovat. Proto si zde ukážeme známé a používané techniky a hlavně, jak je rozpoznat a bránit se.

4.3.1 Reciprocita

I když nám slovo reciprocita mnohdy nemusí být jasné a nemusíme znát jeho význam, setkali jsme se s ní naprosto všichni. Reciprocita je totiž sociální konstrukt týkající se dávání, přijímání a splácení darů, služeb či ústupků. Pokud nám například někdo prokáže laskavost, máme tendence mu tuto laskavost oplatit laskavostí z naší straky. A jak prokazují studie, tento koncept se vyvíjí již u dětí ve věku 3-4 let [19]. Nemůžeme se proto divit, že je to velmi silný manipulační prostředek.

S reciprocitou je svázáno hned několik problémů, jak představuje Robert B. Cialdini [5]. Prvním je skutečnost, že tento konstrukt je tak silně zakořeněn v lidské mysli, že nezáleží na tom, jestli druhou osobu máme rádi. Náš pocit nutnosti vrátit laskavost bude naprosto stejný. Tento fakt sám o sobě nemusí být až tak velký problém, dokud ho nespojíme s další skutečností. Konstrukt reciprocity je efektivní, i když je laskavost nevyžádaná, neboli, pokud jsme ji nepotřebovali a někdo jiný nám ji vnutil. Pokud by ani toto nebylo dost, tento konstrukt lze dále využít k vytvoření nerovnoměrné akce. Lze tedy použít malou počáteční laskavost k dosažení velké laskavosti.

Z těchto principů tedy vyplývá, že je možné vytvořit situaci, kdy jedna strana určí obě laskavosti, jednu větší než druhou a my jsme stejně vedeni ke splnění naší sociální obligace.

I když se zde bavíme o laskavostech, stejný princip funguje s dary nebo ústupky, a je velmi častou vyjednávací taktikou. Nejdříve vyžadujeme mnohem vyšší požadavky, než ve skutečnosti chceme a pak ustoupíme na naše potřebné. Vytvoříme tak situaci, kdy my jsme

ustoupili a je teď na druhé straně, aby nám vyhověla. Jediným klíčovým faktorem fungování této strategie je vhodná volba prvotních požadavků. Musí být dostatečně vysoké, aby byl vytvořen dostatečný ústupek, avšak nesmí přesáhnout extrémní meze, protože jinak budou brány jako nesmyslné a taktika přestane fungovat. Je také nutné podotknout, že oběť si často neuvědomuje tuto manipulaci a tak má pocit satisfakce, protože jsme jejím požadavkům ustoupili, a je tak náchylnější na další požadavky z naší strany.

Pokud snad potřebujeme další důkaz o síle tohoto principu, stačí si vyhledat informace a místě zvaném Jonestown [20].

Obrana

Obrana vůči konstruktu reciprocity není jednoduchá. Na první pohled by se mohlo zdát že prostě stačí odmítnout jakékoli laskavosti, dárky či ústupky. Tím však ničíme jakoukoli šanci využití původního účelu reciprocity a budeme také často vystupovat jako sociálně hrubí. Naštěstí je i lepší cesta. Robert B. Cialdini totiž ukazuje, že pokud nebudeme úvodní akt vnímat pod tímto konceptem ale jako akt manipulace, koncept přestává platit, nebo by jeho verze mohla vypadat i jako „manipulaci oplatíme manipulací“ [5]. Je tedy velmi důležité snažit se rozpoznat, kdy nabídnutý prvotní akt je opravdový s dobrými úmysly, nebo zda se jedná o prvotní krok manipulace.

4.3.2 Závazek a konzistence

Konzistenci můžeme chápat jako předvídatelnost či důslednost člověka v jeho názorech a činech. Pokud se tedy v jedné situaci člověk nějakým způsobem zachová, bude konzistentní právě tehdy, když se zachová stejně za případu, že tato situace nastane znovu. Lidé mají až obsesivní potřebu být svými činy a hlavně vypadat konzistentně. Je možné identifikovat 2 hlavní důvody proč tomu tak je [5]. Prvním důvodem je samotný mozek. Mozek využívá

konzistentnost jako mentální zkratku pro šetření své energie, konzistentnost mu totiž dovoluje nemyslet nad každým činem či rozhodnutím a pouze reagovat stejně, jak již jednou udělal. Druhým důvodem je pak lidská společnost. Konzistentnost je brána jako pozitivní vlastnost, nekonzistentnost pak jako velmi negativní vlastnost. Z těchto důvodu tedy můžeme hovořit o automatické konzistenci chování člověka, kdy bez dalšího myšlení se bude chovat konzistentně, i kdyby to třeba nebylo v jeho nejlepším zájmu. Manipulace je pak tedy zkonstruovávána tak, aby využila právě automatické konzistence.

Závazek je poté prvotní krok manipulace. Závazek neslouží totiž pouze k tomu, aby jsme vykonali slíbenou akci ale také pozměňuje, jak na sebe vnitřně nahlížíme [5]. A právě k naší vnitřní identitě nahlíží mozek, pokud se snaží být konzistentní. Největší výhodou této metody je fakt, že pokud se manipulátorovi povede změnit vnitřní identitu cíle, nemusí vynakládat další úsilí, aby tento stav udržel, cíl se o to postará sám. Zapříčinit tuto vnitřní změnu není jednoduchá záležitost. Záleží totiž na 2 faktorech. O kolik je tato změna odlišná od již přítomného vnitřního stavu a jak rychle této změny chce manipulátor docílit. Je důležité si uvědomit, že bude jednodušší přimět někoho, kdo již aktivně protestuje proti globálnímu oteplování a vnímá sám sebe jako milovníka přírody, aby začal navíc protestovat i proti testování na zvířatech, a rozšířil tak své vnitřní vnímání na milovníka přírody a zvěře. Bude mnohem těžší přimět někoho, kdo nikdy neprotestoval a ani o tuto tématiku nemá zájem. A pokud s takovýmto postojem někdo silně nesouhlasí, je téměř nemožné ho tímto způsobem ovlivnit. Otázka času se pak projevuje v principu inkrementální změny po malých krůčcích. Tam, kde by byla velká změna přesvědčení odmítnuta je totiž možné dosáhnout požadovaného cíle, pokud k tomu máme dostatek času. Tento postupný manipulační přístup však lze za určitých podmínek provést

i v kratším časovém úseku. Dejme si za příklad 2 dobrovolné dotazníky. První se zeptá na číslo bankovního účtu hned v první otázce a jistě se najdou tací, kdo zde přestanou tento dobrovolný dotazník vyplynovat. Druhý dotazník používá principy manipulace a tak bude mít jednoduché otázky na začátku, takové na které není žádný odpor odpovědět. Otázka na bankovní účet se bude nacházet až ke konci. Ve chvíli, kdy se k otázce o bankovním účtu osoba dostane, se již vidí jako nápomocného člověka, který odpovídá na zadané otázky a tak odpoví i na tuto [2]. Odpoví zde i ti, kdo by na stejnou otázku bez změny vnitřního stavu, tedy u dotazníku jedna, neodpověděli. Této tendence je tedy možné využít k získání stále osobnějších informaci aniž by si cíl uvědomil, že nám je nechce poskytnout.

Obrana

Je nemožné eliminovat automatickou konzistenci. To by vedlo k nutnosti strávit veškerý náš čas zvažováním možností, aniž by jsme byli schopni se rozhodnout k jakémukoli činu.

Je však možné se naučit rozeznávat situace, kdy nás automatická konzistence vede k akcím, kterým by jsme se radši vyhnuli. Pak je důležité pořádně se zamyslet nejen nad tím, jak budeme v této situaci postupovat dále, ale také, jak jsme se do ní dostali [5]. Právě tato zpětná perspektiva nám může pomoci odhalit past, a i kdyby ne, už jen to že jsme se zastavili a zamysleli se, proč naše emoce neodpovídají skutečnosti nás vyvádí z automatické konzistence a máme tak šanci naši potřebu být konzistentní překonat.

4.3.3 Pozitivní pocity

Není překvapením, že pokud k někomu cítíme pozitivní pocity jako lásku, přátelství nebo prostě někoho máme rádi, preferujeme uskutečnit jejich žádosti. Také nás asi nepřekvapí, že tyto žádosti

mohou jít za hranice toho, kde by jsme všem ostatním vždy řekli ne. Překvapující však je, jak moc nás pozitivní pocity dokáží ovlivňovat. Například i pouhá zmínka o příteli pomůže manipulátorovi využít naše kladné pocity v jeho prospěch, a to i když náš přítel není přítomen [5].

A pokud manipulátor nemá připraveného našeho přítele, není nic jednoduššího než aby se on sám stal osobou, ke které máme kladné pocity. Vytváření kladného vztahu je jednou z nejzákladnějších technik, které musí zdatný sociální inženýr ovládat [2]. Schopnost vytvořit kladný vztah je totiž klíčová k ovlivnění jedince a často na této schopnosti závisí úspěch.

Rozlišujeme několik technik, jak se alespoň krátkodobě někomu zalíbit. Jednou z nejzákladnějších technik, které mohou manipulátoři využívat je podobnost. Máme rádi lidi kteří jsou nám v nějakém smyslu podobní, ať už to je oblékáním, vystupováním, humorem či místem původu. Stačí i pouhá zmínka, například pokud se někdo zmíní že pochází s určitého místa, řekneme že naše žena tam vyrůstala, nebo že z toho místa pochází náš otec. To vyvolá princip podobnosti a zároveň nemusíme znát odpovědi na kritické otázky o daném místě, což by bylo potřeba kdyby jsme řekli že my pocházíme z daného místa.

Další možnou taktikou, jak získat oblibu cíle jsou komplimenty. Jako lidé milujeme když nám jsou kladeny komplimenty, a to dokonce i v případě, kdy víme že nejsou zcela pravdivé. Stále však existují hranice, a je mnohem lepší použít kompliment který je pravdivý než nepravdivý. Přeci jen koncept komplimentů pro manipulaci je velmi známý a tak jsou na ně někteří lidé velmi citliví.

Předposledním trikem, který zde budeme jmenovat je pak asociace s dobrými zprávami nebo impulsy. Pokud můžeme cíli zdělit dobré zprávy, budou na nás pohlížet lépe. Naopak je potřeba vyhnou se

špatným zprávám, protože asociace funguje v obou směrech. Jako obvykle, toto není nový poznatek, je ale překvapivá jak silně asociace funguje. Výborným příkladem nám mohou být starověcí poslové, kteří bývali za dobré zprávy zahrnuti zlatem, avšak za špatné bývali popraveni, i když oni sami neměli na danou zprávu žádný vliv.

Na závěr je nutnost zmínit vzhled. I když si to nechceme připouštět, lidé jsou silně přitahování k dobře vypadajícím lidem. Navíc díky halo efektu těmto lidem přisuzujeme další kladné vlastnosti jen na základě jejich vzhledu. Pokud tedy uvidíme dobře vypadající osobu a máme možnost si z jejího chování zvolit mezi dvěma vlastnostmi, například lakomý člověk a člověk umějí zacházet s penězi, vždy zvolíme tu kladnou.

Obrana

Hlavním problémem metod využívajících pozitivní pocity je skutečnost, že fungují na podvědomé úrovni. Je tedy velmi obtížné si uvědomit, že na nás působí a i v těch výjimečných případech, kdy si působení uvědomíme, je nemožné nebýt pozitivními pocity ovlivňováni. Nabízí se nám možnost pocity potlačovat nebo dokonce převracet na negativní, pokud se domníváme že s námi někdo manipuluje. Jak však odhalit, jestli někdo má záměr manipulace nebo je to prostě přátelská osoba? Tento způsob obrany pravděpodobně způsobí více škody nežli užitku. Robert B. Cialdini nám naštěstí ukazuje jiný způsob, jak toto dilema řešit [5]. Tento trik je jednoduchý, avšak velmi efektivní. Pomůže nám zabránit vyhovění žádostí, které nejsou v našem nejlepším zájmu, i když k dané osobě máme pozitivní pocity. Stačí mentálně oddělit žádost od osoby, která tuto žádost podala. To nám dovoluje objektivně přistupovat k žádosti a zároveň nahlížet na danou osobu nadále pozitivně. Pokud se tedy před splněním žádosti zastavíme a zvážíme žádost samu o sobě, můžeme na ni reagovat aniž by jsme byli ovlivněni.

5 Praktická část

V praktické části byly kontaktovány soukromé a veřejné instituce (vyšší uzemní samosprávné celky), které musí dodržovat legislativu v oblasti kybernetické bezpečnosti a informační bezpečnost musí být velmi explicitně a detailněji řešena a dodržována, díky čemuž se lze domnívat, že právy uvedené instituce budou velmi často cíle útočníků v oblasti sociálního inženýrství. Cílem kontaktu těchto institucí bylo získat metody, které používají ke své obraně proti sociálnímu inženýrství. Bylo zřetelné, že mnoho institucí odmítlo poskytnou jakékoli informace, týkající se této ochrany. Jelikož se zde sami odkazujeme na metodu limitace informací, musíme uznat, že to je naprosto pochopitelná a validní volba, i když to nepomohlo s vypracováváním této kvalifikační práce Některé instituce však byly ochotny informace poskytnout a to i přes ztíženou situaci spojenou s COVID-19. Ta mnohdy vedla ke zvýšeným nárokům na IT specialisty se kterými jsme se snažili spojit za účelem získání potřebných informací. I když na tomto bodu selhalo několik komunikací, i tak jsme zjistili dostatek dat, aby jsme mohli sestavit tento seznam nejpoužívanějších metod. Zároveň lze také tvrdit, že seznam pokrývá v minimálním případě jádro, a v nejlepším případě většinu používaných metod. Tento fakt můžeme odvodit z opakování dat a nicotném zisku nových informací ke konci zkoumáni.

Zjištěných metody jsme rozdělili do 2 kategorií, metod zaměřených na povědomí uživatele a metod zaměřených na technologické zabránění útoku. Jednak to bylo pro zjednodušení komunikace s danými institucemi, ale také to vede k zpřehlednění celé tématiky. Můžeme tak jednodušeji pozorovat hlavní rysy obrany. Je však důležité dodat, že metody na sebe často navazují, prolínají se nebo podporují svoji funkčnost a to nejen ve své vlastní kategorii.

5.1 Metody založené na povědomí uživatelů

Jelikož útoky sociálního inženýrství z velké části závisí na uživateli, je jasné že i obrana se bude z velké části soustředit na uživatele, hlavně tedy na jeho informovanost. Tyto metody se snaží uživatele seznámit s existencí sociálního inženýrství a jak se zachovat, pokud mají podezření, že jsou nebo byli napadeni. Dalším úkolem těchto metod je také zjištění, jak úspěšně byli uživatelé s útoky seznámeni nebo jak úspěšně fungují jiné metody. Jako u všeho je totiž dobré mít zpětný výstup, aby bylo možné najít a napravit nedostatky.

5.1.1 Uživatelská školení

Je nemožné bránit se proti útoku, když ani nevíme, že útok existuje. Proto je školení uživatelů nejdůležitější část obrany vůči sociálnímu inženýrství a zároveň základ, na kterém pak staví většina ostatních metod ochrany.

U všech dotazovaných bylo využíváno školení jako hlavní formy obrany proti útokům z kategorie sociálního inženýrství. Je zřetelné, že přípravě a průběhu věnovaly tázané instituce značné množství času. Školení poprvé zaměstnanci podstupují hned při nástupu na novou pracovní pozici, dále se pak opakuje v jednoročním cyklu. Velmi častá byla zmínka o E-lerningu a závěrečných testech, které uživatel musí úspěšně splnit aby ukázal, že opravdu prošel školením a pochopil představovanou problematiku. Asi nejzajímavějším řešením této problematiky bylo vytvoření her pro uživatele, kde si mohli vyzkoušet problematiku sociálního inženýrství nejen jako obránci a napadení ale i jako útočníci.

Školení se většinou týkají hlavních forem sociálního inženýrství. Uživatelé se učí jak poznat typické znaky podvodných emailů, jak ověřovat odkazy, důvěryhodnost webů nebo emailů a jejich příloh. Je také reflektováno stále častější využívání Instant Messaging Aplikací

a tak se řeší i útoky nejčastěji zde používané. Důležitou složkou školení je také ukázat uživatelů, co dělat, když k útoku opravdu dojde. A to nejen v případě, že byl odhalen okamžitě. Školení se tedy také zaměřují na to, co dělat pokud uživatel má podezření na útok, pokud již klikl na podvodný odkaz, otevřel přílohu nebo, a to v nejhorším případě, co dělat když už vyplnil důvěryhodné informace.

Kritické body

Aby byly techniky a opatření na obranu uživatelů co nejefektivnější, měly by být vytvořeny s ohledem na jistá pravidla a jejich nejčastější problémy.

Techniky musí [2]:

- eliminovat nutnost přemýšlet nad správnou akcí
- vyhnout se zbytečné složitosti
- vyhnout se pravidlům bez jasného významu
- eliminovat možnost využití emocí k obcházení technik
- být realistické a proveditelné

Vytvoření optimálních technik a bezpečnostních opatření je umění. Je nutné balancovat nároky na uživatele s dosaženou bezpečností. Pokud budou nároky na uživatele nízké, uživatel je nebude mít problém vykonávat, dokonce je možné, že bude až moc horlivý v jejich výkonu. Pokud jsou však nároky na uživatele vysoké, bude se je snažit uživatel obcházet v rámci zjednodušení své práce a života. Jako příklad můžeme využít podezření na podvodný email. Standardní technikou je nahlásit toto podezření specialistům z oddělení informační techniky. Pokud bude toto nahlašování fungovat kliknutím na jedno tlačítko v emailu, tedy bude náročnost na

uživatele minimální, můžeme očekávat, že budou uživatelé nahlašovat všechny i jen trochu podezřelé emaily. Pokud však po stisku tlačítka budou uživatelé muset vyplnit formulář velikosti A4, můžeme počítat s razantním snížením nahlašování podezřelých emailů. Je tedy nutné zvážit, kde dodatečná bezpečnost bude zasahovat do běžné práce uživatele natolik, že radši vynaloží práci na nalezení způsobu, jak ji obejít nebo ignorovat.

Je tedy ideální aby technika nebyla složitá, nezabírala uživateli nadměrné množství času, byla jasná a ve svém výsledku efektivní pro danou instituci. Toto není narážka na inteligenci uživatele, naopak je to snaha zasahovat co nejméně do jeho stávající práce. Stejně jako u útoků zde využíváme lidských tendencí k posílení obrany.

Je důležité brát v potaz, že pokud bude útočník využívat city uživatele, například soucit, může se mu uživatel snažit co nejvíce pomoci a to i obcházením nastavených opatření. Pokud si však toto uvědomujeme už při vytváření těchto opatření, můžeme na tuto situaci uživatele varovat nebo je vytvořit tak, aby to nebylo možné.

V poslední řadě je potřeba dát pozor na realistickou proveditelnost opatření a technik. To co se může při testování zdát jako ideální často ve skutečném provozu narazí na nové problémy, se kterými se při testování nepředpokládalo, což činí techniku nerealistickou. Je tedy dobré upravovat techniky podle zpětné vazby uživatelů. Ve vzácných případech se také může stát že, že technika nebo opatření je nesmyslné, ať už je to nutností vytvořit nebo nepochopením problému. V takových případech by nám právě zpětná vazba měla ukázat kde je největší problém nutný co nejdříve napravit.

5.1.2 Informování o nových útocích

Důležitou obranou proti sociálnímu inženýrství je informovanost uživatelů. Z větší části se o toto stará školení uživatelů, to však

probíhá jen v určitých intervalech a jeho příprava je složitá. Občas je však potřeba upozornit uživatele rychleji, například na právě odhalené útoky na které je dobré dát si pozor. Tato upozornění poskytuje například Národní úřad pro kybernetickou a informační bezpečnost, zkráceně NÚKIB. Odborník na bezpečnost tedy sleduje tento portál a pokud objeví hrozbu která se týká jeho uživatelů, měl by je vhodným způsobem informovat. Také pokud odborník na bezpečnost zaznamená hrozbu, která ohrožuje společnost a napadá uživatele, je dobré mít připravený komunikační kanál na který jsou uživatelé zvyklí a sledují ho. U tázaných institucí tak byly zaznamenány existence interních zpravodajů, nebo specifických schránek na intranetu.

5.1.3 Cvičné útoky

Cvičné útoky jsou velmi důležitou formou obrany, avšak někdy opomíjenou. Slouží totiž jako zpětná vazba o tom, jak dobře byl uživatel zaškolen do problematiky útoků nebo dokonce jak dobře jsou nastavené metody, které ho mají s touto problematikou seznámit. Cvičné útoky také mohou prověřit všechny ostatní metody, které jsme si jako obranu proti sociálnímu inženýrství připravili.

Je mnoho způsobů jak tyto cvičné útoky připravit, není to však jednoduchá záležitost a tak si ukážeme alespoň některé možnosti, jak tuto situaci ulehčit. Například je možné využít pomocné programy jako Microsoft Defender Attack Simulátor, které nám pomohou se sestavením a provedením cvičného útoku.

Další možností je vyřešit celou tuto problematiku externě. Pokud zvolíme tuto možnost, najmeme externího specialistu který provede útok podle našich specifikací. Tento postup má své výhody i nevýhody. Mezi výhody patří nestrannost externího experta, který bude více kritický k výsledkům a nemá důvod je zlepšovat, spíše

naopak. Tento externí expert také může navrhnout zlepšení, která jsou pro něj zřejmá a my jsme si je nemuseli uvědomit. To je ve většině případů způsobeno tím, že my sami jsme součástí systému. Nevýhodou tohoto přístupu je nutnost volby vhodného kandidáta, náklady na jeho práci a také nutnost vynaložit v něj důvěru, protože mu dáváme za úkol na nás zatočit. Jedním zástupcem kdo tuto službu provozuje je například FLAB Cesnet.

Dalším kritériem, které musíme zvážit je zda budeme testovat veškeré uživatele, nebo budeme testovat pouze určitou skupinu či náhodně vybrané jedince. Toto je nutné brát v úvahu, protože testování všech nemusí být vždy nutné. Specifičtějším testováním naopak můžeme uvolnit zdroje, které pak lze využít jinde. Například k hlubšímu testování vybrané skupiny. Naopak testování na příliš malé skupině nám může poskytnout výsledky, které nejsou reprezentativní pro naše uživatele a mohly by tak vést k mylným závěrům.

5.2 Technické metody

Technické metody jsou metody, založené na technických řešeních problému sociálního inženýrství, místo zaměření na uživatele. I když tak často uživateli napomáhají, nebo ho omezují v rámci zvýšení bezpečnosti, jejich primární princip je čistě technický a s uživatelem jako takovým tedy souvisí ale nejsou na něm závislé.

5.2.1 Limitování volně dostupných informací

Důležité je uvědomit si, že pokud je útočník zaměřený specificky na danou osobu, je velmi těžké, možná i nemožné, mu zabránit provést útok. Můžeme však ovlivnit kvalitu útoku a to až do krajních mezí, které činí obrana triviální, nebo množství času strávené nad přípravou útoku. Pokud útok není zaměřený na jednu specifickou

osobu, můžeme útočníka od útoku odradit. V obou případech toho můžeme dosáhnou limitací volně dostupných informací. Jak však Christopher Hadnagy a Kevin Mitnick ukazují, množství informací které o sobě volně šíříme je značné [2] [17]. A často tyto informace šíříme, aniž by jsme si toho byli vědomi. Sociální sítě jako Facebook, LinkedIn a Twitter jsou pak pro útočníka zlatý důl informací, protože není mnoho uživatelů, jež si plně uvědomují jejich rizika. Extrémní případy na sociálních sítích dokumentují každý svůj krok a značně tak útočníkovi ulehčují práci. I ti opatrnější však poskytují informace aniž by chtěli. Pokud například zveřejníme fotografii, její metadata mohou prozradit nejen kde, ale i přesný čas, kdy byla pořízena. Výborným případem nám může být příběh Johna McAfeeho [17]. Ten se stal uprchlíkem kvůli spojení s vraždou jeho souseda a nakonec byl dopaden právě díky metadatům v obrázku zveřejněném na Twiteru. Obrázek totiž obsahoval přesnou polohu místa, kde byl pořízen. Mohlo by se zdát, že tato situace se nás netýká, jelikož nejsme zločinci nebo uprchlíci a tak nemáme co skrývat. Musíme si uvědomit, že přes sociální sítě lze velice snadno sledovat pohyby jedince a zjistit tak jeho zájmy, oblíbená místa nebo lidi. To vše pak lze využít k optimalizaci útoku. Toto ukazuje Ch. Hadnagy, kdy po zjištění, že jeho cíl navštěvuje určitou tělocvičnu použil tuto informaci k úspěšnému útoku, v tomto případě získání informací kreditní karty [2].

Stejně tak s postupem technologií a hlavně umělé inteligence je stále lehčí probírat se hromadami daty a je například možné ze zveřejněných profilů na facebooku nebo tweetu na twitteru sestavit komunikační profil a tím vylepšit šance úspěšnosti sociálního útoku. Tímto se zabýval například James w. Pennabaker, tvůrce Analyzeword.com [21]. Ta je sice dnes již nefunkční, ale jiné stránky zabývající se analýzou sentimentu stále existují, často pro komerční využití firem ke zjištění sentimentu vůči nim. Je asi jasné, že nelze

očekávat aby jsme všichni šli až do rámců možností, které nám ukazuje právě Kevin Mitnick [17]. Nelze očekávat že se na internetu všichni staneme neviditelní, tuto skutečnost v závěru knihy uznává i její autor. Druhým dechem však dodává, že i normální občané by se měli zamyslet, kolik informací dávají na internet, zda je opravdu nutné toho tolik sdílet a jestli není dobré se zamyslet, co o nás naše sdílená data vypovídají.

Stejným přístupem se musí řídit i tázané instituce. Bylo mnoho tázaných institucí, jejichž interní politika je neodpovídat na jakékoli dodatečné otázky týkající se bezpečnosti. Proto můžeme být rádi, že byli i jiní, ochotni poskytnou data pro tento výzkum a to s plným vědomím bezpečnostních rizik, která jsme se pro ně snažili co nejvíce minimalizovat. Limitování informací totiž není ochrana, na kterou je možné se plně spoléhat a proto je potřeba mít připravené metody na které je větší spolehnutí.

5.2.2 Spam Filter

Spam filtry jsou prvotní ochrana proti phishingu. Mnoho známých phishingových emailů totiž vykazuje stejné rysy, takže je možné je přes spam filtry identifikovat. Samotný Google potvrzuje, že blokuje více jak 100 milionů phishing emailů za den [22]. To znamená že spam filtry zachycují velké množství phishingových útoků, je však jasné, že se nelze spoléhat výhradně na jejich funkčnost. Každá spam filter totiž malé procento příchozích zpráv identifikuje špatně, ať už v lepším případě spam jako normální zprávu, nebo v horším případě normální zprávu jako spam. Také u tázaných institucí byly spam filtry samozřejmostí, avšak přístup k nim byl často naprosto rozdílný, v závislosti na interním fungování emailů. Někteří se plně spoléhali na externě fungující služby, jako například Office 365, včetně cloudových služeb Microsoftu pro správu elektronické pošty s ním spojených. Většina však využívá kombinaci externím a interních

spam filtrů, což se zdá být nejlepší volbou. Využívají tak kvalitně vytvořené externí filtry na hrubé filtrování a mají pak dodatečné interně psané filtry na již nalezené hrozby nebo jiné specifické případy.

5.2.3 Proxy a Blokování obsahu

Pokud víme, že je něco škodlivé, není nic jednoduššího než k tomu zablokovat přístup. Na tomto jednoduchém principu funguje blokování obsahu. Pomocí kategorizační uživatelské webové proxy můžeme vytvořit blokace vstupu na nepovolené kategorie a také upozornění při vstupu na neznámou kategorii. Stejný princip, který zabraňuje uživatelům volný pohyb po internetu za účelem zvýšení efektivnosti lze tak využít ke zvýšení bezpečnosti. Často bývá také dobré zahrnou do blokovaných stránek stránky na sdílení souboru jako ulož.to, aby se uživatelům zamezilo stahování souborů. Princip blokování tak slouží eliminaci náhodného přístupu na nežádoucí stránky, například pomocí podvodného odkazu. Další výhodou je varování uživatele, pokud přistupuje na podezřelé nebo neznámé stránky.

5.2.4 Upozornění, notifikace

V závislosti na spam filtrech pak fungují upozornění. V závislosti na nastavení spam filtrů totiž nemusí být email odhozen nebo převeden do speciální složky. Další možností je označení pro uživatele, aby ho upozornil na podezření, avšak nechal finální volbu jak bude s emailem zacházeno na něm. Toto lze vnímat více směry. Na jednu stranu lze upozornění brát jako dobrou indikaci pro uživatele, že si musí dávat větší pozor. Na druhou stranu by to mohlo vést k mylné důvěře uživatele v upozornění. Uživatel by se mohl mylně domnívat, že neoznačené emaily jsou vždy bezpečné, což by vedlo k jeho menší

opatrnosti. Je nutné dodat že mnoho dotázaných institucí upozornění nepoužívalo, i když někteří ho plánovali zařadit do budoucí obrany.

5.2.5 Minimalizace následků úspěšného útoku

Často opomíjená ale velmi důležitá je minimalizace následků úspěšného útoku. Je totiž lepší předpokládat a být připraven na situaci, že obrana bude prolomena, než naivně věřit tomu, že tato situace nemůže nastat. Proto je potřeba brát tuto situaci v potaz a připravit se na ni. Jelikož toto blízce souvisí s celkovým nastavením systému, práv a přístupů, které se řeší mnoha způsoby, nelze zde doporučit jednotné rady, které by byly aplikovatelné naprosto pro všechny. Můžeme však říci některé nejčastější pochybení nebo připomínky, kde lze systémy vylepšit a při tom minimalizovat možné následky úspěšného útoku.

Je nutné zvážit, k čemu všemu má každý uživatel mít přístup, či identifikovat jedince, kteří jsou nejvíce v ohrožení napadení. Asi nejdůležitější je však poučit se z již provedených, i když třeba neúspěšných útoků. Analýzou útoku totiž zjistíme nejen napadenou část, ale i škody kdyby útok uspěl a můžeme tak navrhnout řešení, která tyto škody minimalizují. V neposlední řadě si pak musíme dát pozor na chybná nastavení, můžeme mít vše sebelépe navržené ale pokud opravdu neotestujeme kritické body přístupů, můžeme nechtěně opominout nějakou chybu, kterou pak může útočník využít.

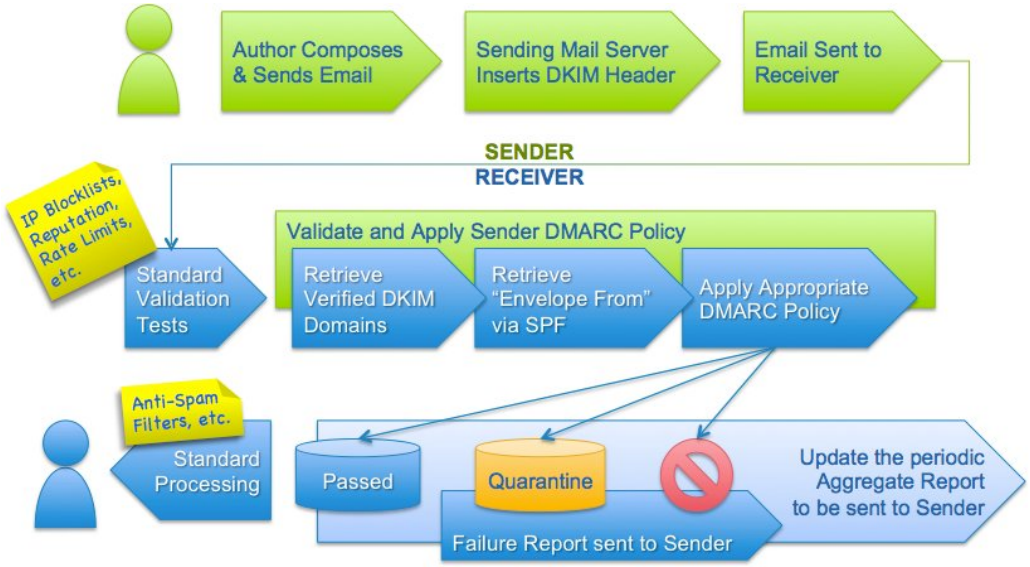
5.2.6 SPF, DKIM, a DMARC

Metody ochrany zmiňované zřídka a hlavně v kontextu nového zavádění jsou implementace SPF, DKIM a DMARC. Tyto metody jsou na sebe blízko vázané a slouží k odhalování a odstraňování podvodných emailů.

SPF (Sender Policy Framework) je metoda snažící se zabránit falšování adresy odesilatele u emailu. SPF totiž umožňuje vlastníkovi domény specifikovat, které emailové servery používají k posílání emailů. Pokud tedy přijde zpráva, která tvrdí že pochází z dané domény a i my máme nastavené SPF, můžeme si ověřit, jestli tato zpráva opravdu splňuje požadavky ověření. Ověřujeme tedy, že dané zpráva pochází ze serverů specifikovaných vlastníkem domény. Pokud tomu tak není, můžeme považovat tuto zprávu za podvodnou. [23]

DKIM (DomainKeys Identified Mail) je metoda zabraňující falšování obsahu zprávy. V kombinaci s SPF tedy zkontrolujeme nejen jestli je email opravdu z dané domény ale také jestli jeho obsah nebyl nijak modifikován. Pokud doména využívány DKIM, její vlastníci na ní publikovali veřejný klíč. Pokud se z této domény posílá zpráva, podepíše se privátním klíčem. Po příchodu takovéto zprávy můžeme pomocí veřejného klíče zkontrolovat, že tato zpráva opravdu nebyla změněna od podepsání privátním klíčem a tím zaručíme její důvěryhodnost. [24]

DMARC (Domain-based Message Authentication, Reporting and Conformance) je přirozené spojení ale hlavně rozšíření SPF a DKIM. DMARC umožňuje vlastníkovy doménu specifikovat zásady, jak jednat se zprávami, které z jeho domény přicházejí. Tyto zásady ujasňují nejen, jaké protokoly doména využívá, SPF či DKIM ale i jak jsou využívány. DMARC také přidává adresu pro zasílání zpětné vazby, tedy statistiky o dané doméně vygenerované příjemcem zpráv. Co se týče SPF a DKIM, DMARK určuje 2 typy zacházení(nijak nesouvisející s vnitřním fungováním metod), striktní a relaxované. Striktní znamená, že protokol vyžaduje exaktní schodu a nepřipouští podřízené identifikátory. [25]



Obr. 4: DMARC grafický postup

Zdroj: [27]

5.2.7 Registrace podobných domén

Jako poslední je metoda která nechrání nás ale ostatní. Mezi dotazovanými institucemi byla zmiňována velmi zřídka, to však bude zapříčiněno spíše tím, že je to spíše metoda ochrany ostatních a ne dané instituce. Tato metoda je však běžná pro instituce, které se zajímají nejen o svoji ochranu ale i o ochranu ostatních, i kdyby jen z důvodu zachování dobré pověsti nebo zamezení poškozování jejich značky či dobrého jména. Tato metoda tedy spočívá v registraci domén, které se značně podobají té naší. Snadným příkladem si můžeme opět dát Google, který má zaregistrované nejen google.com, google.cz a podobné regionální domény ale také má zaregistrované domény jako google.org nebo google.net [26]. Google dokonce registruje i velmi podobné domény jako goooogle.com (tři o), gogle.com (jen jedno o), googel.com (přehození písmen) nebo gogole (opět přehození písmen) [26]. Registrace těchto podobných domén totiž zabraňuje jejich využití k podvodným účelům a pomáhá tak chránit nejen ostatní ale i dobré jméno organizace.

6 Závěr

Cílem této práce bylo analyzovat a ověřit přehled nejvyužívanějších metod v sociálním inženýrství a ochrany proti možných útokům v sociálním inženýrství. Při psaní této kvalifikační práce vyplynulo, že toto téma má stále větší důležitost právě kvůli navýšení útoků, které zaznamenáváme každý rok.

Práce v první teoretické části charakterizuje samotnou podstatu sociálního inženýrství, předpis obecného útoku za pomoci pyramidy SI. Další část byla zaměřena na rešerši nejčastějších typů sociálního inženýrství a jejich útokům a předcházení hrozbám. V rámci lepšího pochopení celé náročné tématiky byli představeny některé techniky manipulace, které nejsou limitované pouze na útoky sociálního inženýrství, jsou však často využívány pro zlepšení jejich úspěšnosti.

V praktické části práce bylo provedeno dotazování soukromých a veřejných institucí s následným vyhodnocením. I přes předchozí očekávání bylo překvapující, jak často byla spolupráce za zjištěním metod odmítnuta ze stran dotázaných institucí. Hlavní uvedenou příčinou byla právě citlivost informací. Dalším ztížením byla také korona-virová situace, která způsobila nadměrný nárůst práce IT techniků, které bylo nutné kontaktovat pro přesné zjištění informací. I přes tyto problémy byl kontaktován dostatek institucí, aby byl sestaven seznam nejpoužívanějších metod, spolu s jejich vysvětlením a případnými zajímavými poznatky, které ze získaných dat vznikly. K tomuto závěru můžeme dospět z důvodu opakování dat a žádnému zisku nových informací ke konci dotazování. V rámci zpřehlednění a roztřídění byly metody rozděleny na metody zaměřené na povědomí uživatelů a metody technické. Očekávali jsem, že metody zaměřené na povědomí uživatelů se budou s metodami technickými doplňovat, dalo by se i říci, že metody technické v mnoha případech složí podpůrné roli. Tato očekávání se potvrdila. Metody technické

opravdu slouží většinou jako podpora nebo také záchranná sít pro uživatele.

Téma sociálního inženýrství bude i do budoucna relevantní, jelikož je nemožné eliminovat slabiny související s lidmi ze systému. Proto se také nabízí několik další směrů, kterými by mohlo zkoumání v budoucnosti pokračovat. Jistě by bylo zajímavé zkoumat hlavně metody založené na povědomí uživatele. Jsou totiž kritické k vybudování efektivní obrany, avšak jejich vytvoření závisí na mnoha faktorech a specificky vypadající metoda může být velmi efektivní nebo naprosto neefektivní v závislosti na jakých uživatelích bude použita. Také technické metody postupují stále dopředu a jistě vznikají nové efektivnější, které se zatím běžně nepoužívají. Posledním zajímavým zkoumáním by bylo porovnání připravenosti českých institucí v porovnání s Evropu nebo zbytkem světa, nebo také zkoumání nejčastějších útoků v České republice v porovnání se světem.

7 Seznam použité literatury

[1] MITNICK, Kevin D a William L SIMON. *The art of intrusion: the real stories behind the exploits of hackers, intrudes and deceivers*. Indianapolis, Ind.: Wiley Publishing, Inc, 2006. ISBN 978-0-471-78266-7.

[2] HADNAGY, Christopher a Steve WOZNIAK. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley, 2018. ISBN 978-1-119-43338-5.

[3] VONDRUŠKA, Petr. *Metody a nástroje OSINT* [online]. Duben 2013. Dostupné z: https://is.ambis.cz/th/wqwko/DP_Vondruska.pdf

[4] KAHNEMAN, Daniel. *Thinking, fast and slow*. 1st ed. New York: Farrar, Straus and Giroux, 2011. ISBN 978-0-374-27563-1.

[5] CIALDINI, Robert B. *Influence: the psychology of persuasion*. Rev. ed., [Nachdr.]. New York, NY: Collins, 20. ISBN 978-0-06-124189-5.

[6] COHEN, Lawrence E. a Marcus FELSON. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* [online]. 1979, **44**(4), 588. ISSN 00031224. Dostupné z: doi:10.2307/2094589

[7] ROMMEL, Erwin. *Infantry attacks*. London: Greenhill, 2009. ISBN 978-1-85367-707-6.

[8] CENTER FOR INTERNET SECURITY. *Cybersecurity Spotlight – Common Cyber Hoax Scams* [online]. 14. únor 2020. Dostupné z: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-common-cyber-hoax-scams/

[9] CHIVERS, Kyle. *What is a man-in-the-middle attack?* [online]. 26. březen 2020. Dostupné z: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

[10] *Phishing Activity Trends Report, 4th Quarter 2020* [online]. B.m.: APWG. 2021. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

[11] BHARDWAJ, Akashdeep, Varun SAPRA, Aman KUMAR, Naman KUMAR a S ARTHI. Why is phishing still successful? *Computer*

Fraud & Security [online]. 2020, **2020**(9), 15–19. ISSN 1361-3723. Dostupné z: doi:10.1016/S1361-3723(20)30098-1

[12] SARGINSON, Nic. Securing your remote workforce against new phishing attacks. *Computer Fraud & Security* [online]. 2020, **2020**(9), 9–12. ISSN 1361-3723. Dostupné z: doi:10.1016/S1361-3723(20)30096-8

[13] *Top 200 most common passwords of the year 2020* [online]. Dostupné z: https://nordpass.com/most-common-passwords-list/

[14] VERIZON. *Verizon Data Breach Investigations Report 2019* [online]. 29. květen 2019. Dostupné z: https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/

[15] VERIZON. *Verizon Data Breach Investigations Report 2020* [online]. 18. květen 2020. Dostupné z: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

[16] CRANE, Casey. *Phishing Statistics: The 29 Latest Phishing Stats to Know in 2020* [online]. 22. duben 2020. Dostupné z: https://securityboulevard.com/2020/04/phishing-statistics-the-29-latest-phishing-stats-to-know-in-2020/

[17] MITNICK, Kevin D. a Robert VAMOSI. *The art of invisibility: the world's most famous hacker teaches you how to be safe in the age of Big Brother and big data*. First edition. New York: Little, Brown and Company, 2017. ISBN 978-0-316-38050-8.

[18] *Nový Občanský zákoník (úplné znění) Předpis č. 89/2012 Sb.* [online]. Dostupné z: https://www.podnikatel.cz/zakony/novy-obcansky-zakonik/uplne/#aktualni-zneni

[19] BEELER-DUDEN, Stefen a Amrisha VAISH. Paying it forward: The development and underlying mechanisms of upstream reciprocity. *Journal of Experimental Child Psychology* [online]. 2020, **192**, 104785. ISSN 0022-0965. Dostupné z: doi:10.1016/j.jecp.2019.104785

[20] GUINN, Jeff. *The road to Jonestown: Jim Jones and Peoples Temple*. New York: Simon & Schuster, 2017. ISBN 978-1-4767-6382-8.

[21] *Social Psychology Network page of James W. Pennebaker* [online]. Dostupné z: https://pennebaker.socialpsychology.org/

[22] KUMARAN, Neil a Sam LUGANI. *Protecting businesses against cyber threats during COVID-19 and beyond* [online]. 16. duben 2020. Dostupné z: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

[23] MEHNLE, Julian. *Sender Policy Framework* [online]. 17. duben 2010. Dostupné z: http://www.open-spf.org/Introduction/

[24] CROCKER, D., T. HANSEN a M. KUCHERAWY. *DomainKeys Identified Mail (DKIM) Signatures* [online]. RFC6376. B.m.: RFC Editor. 2011 [vid. 2021-04-25]. Dostupné z: doi:10.17487/rfc6376

[25] KUCHERAWY, Murray a Elizabeth ZWICKY. *Domain-based Message Authentication, Reporting, and Conformance (DMARC)* [online]. B.m.: RFC Editor, 2015. Request for Comments, 7489. Dostupné z: doi:10.17487/RFC7489

[26] *List of Google domains* [online]. Dostupné z: https://infogalactic.com/info/List_of_Google_domains

[27] *DMARC overview* [online]. Dostupné z: https://dmarc.org/overview/

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Jiří Bönsch**
Studium:	I1800158
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Sociální inženýrství**
Název bakalářské práce AJ:	Social engineering

Cíl, metody, literatura, předpoklady:

Zkoumání zranitelnosti firem vůči sociálnímu inženýrství a způsoby, kterými se firmy chrání.

Téma bude zpracováno dle metodických pokynů UHK FIM.

Literatura bude doporučena zadavatelkou BP

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Hana Švecová
Datum zadání závěrečné práce:	21.10.2019