KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2022.2.64-71
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

TESTOVANIE PRIPRAVENOSTI NA PHISHINGOVÝ ÚTOK V ZDRAVOTNÍCKYCH ZARIADENIACH

TESTING THE PREPAREDNESS FOR A PHISHING ATTACKS

MATÚŠ MADLEŇÁK, KATARÍNA KAMPOVÁ

ABSTRACT: *This article deals with testing the preparedness of a selected group of users for phishing attacks. It consists of a theoretical and a practical part. The theoretical part defines the basic framework of phishing attacks. It describes the basic knowledge and definitions that need to be mastered to understand the given area. The practical part consists of testing the preparedness of a specific reference group of users through phishing training and phishing tests. The data collected from the testing was further analysed and compared to determine the potential use of phishing training and phishing testing in organisations.*

KEYWORDS: *cybercrime, phishing attacks, phishing, prevention*

ÚVOD

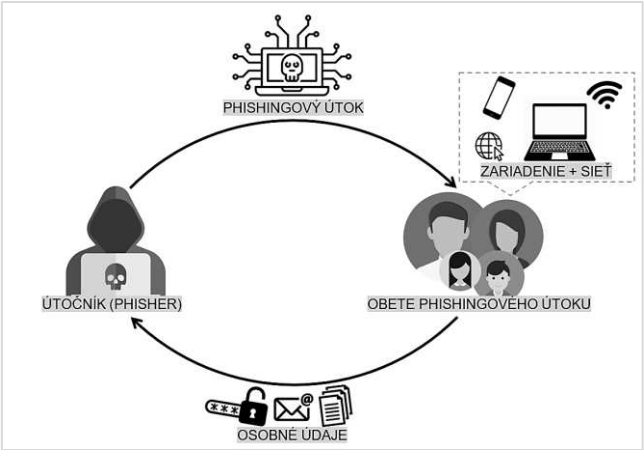
V súčasnosti takmer každá osoba používa zariadenia, ako napríklad počítač a smartfóny, ktoré sú napojené na internetovú sieť alebo telekomunikačnú sieť. V rámci týchto sieti sú častokrát spracúvavané osobné údaje, ako napríklad fotografie, údaje o polohe, číslo kreditnej karty, prihlasovacie údaje a podobne. Tieto údaje sa snažia užívatelia chrániť pred ich zneužitím. Na zabezpečenie svojich používateľských účtov a dát veľmi často využívajú rôzne technické prostriedky, ako napríklad antivírusové programy či dvojfaktorové overovanie identity. Avšak tento druh zabezpečenia nemusí byť vždy účinný pri ochrane voči phishingovým útokom. Jeden zo spôsobov ochrany voči phishingovým útokom je kritické myslenie používateľov, ktoré môže byť dosiahnuté prostredníctvom zvyšovania povedomia o phishingových útokoch. V dôsledku zvyšovania povedomia sa zvýši miera včasného odhalenia phishingového útoku priamo používateľom. Článok sa preto bude primárne zaoberať úrovňou pripravenosti na phishingový útok u vybranej skupiny uživateľov, teda ich schopnosťou identifikovať phishingový útok.

1. PHISHINGOVÝ ÚTOK

Phishing je druh kybernetického útoku, kde je cieľom útočníka (phishera) získať od obete osobné údaje, s využitím rôznych foriem, či druhov phishingových útokov. Obeť phishingového útoku nemusí predstavovať len jednotlivec, ale môže sa jednať aj o rôzne organizácie či inštitúcie. Predmetom záujmu útočníka sú hlavne osobné údaje, prihlasovacie mená a heslá, PIN kódy, informácie, kreditné karty, adresa alebo iné informácie, ktoré môže útočník zneužiť na krádež identity, či spôsobenie finančných strát. Útočník sa snaží pôsobiť dôveryhodne, čím si dopomáha využívaním cudzej identity. Môže sa napríklad vydávať za štátnu inštitúciu alebo za sprostredkovateľa služby (banka, telekomunikačný operátor,...), ktorú obeť využíva. Práve využívanie cudzej identity s cieľom získať dôveru príjmateľa je jeden zo spoločných znakov všetkých phishingových útokov (Shankar, 2019).

Phishing, resp. phishingové útoky využívajú techniky sociálneho inžinierstva, ktoré je založené na ovplyvňovaní a manipulácií ľudí vo svoj prospech. Pri phishingových útokoch je obeti phishingového útoku predhodená pomyselná návnada (neodolateľná ponuka, odkaz, príloha,...) prostredníctvom emailovej, SMS alebo telefonickej komunikácie. Cieľom je prinútiť obeť kliknúť, otvoriť, reagovať alebo inak interagovať s daným podnetom, čím sa stáva phishingový útok čiastočne alebo úplne úspešný (Alabdan, 2020, Sociálne inžinierstvo, 2021).

Vo všeobecnosti je možné princíp phishingového útoku popísať pomocou jednoduchej schémy, znázornenej na obrázku 1. Útočník (phisher) vykoná phishingový útok, s ktorým je konfrontovaná obeť.



Obrázok 1 Schéma phishingového útoku (Vlastné spracovanie)

Spoločným znakom obetí phishingového útoku je skutočnosť, že využívajú zariadenia, ktoré sú napojené na internetovú, telekomunikačnú, či inú sieť, prostredníctvom ktorej je realizovaný phishingový útok. V prípade, že nie je identifikovaný phishingový útok, môže dôsť k vzniku kybernetického bezpečnostného incidentu, ktorého následky môžu mať rozsah ohraničený na obeť útoku, ale aj na celú organizáciu.

1.1. Druhy phishingových útokov

Existujú rôzne druhy phishingových útokov, ktoré sa od seba líšia prevažne spôsobom realizácie, zameraním na obete a aj tým, aké médium využijú na relizáciu phishingového útoku. Phishingové útoky sú páchané hlavne prostredníctvom internetu, SMS/MMS alebo telefonátov. Phishingové útoky realizované prostredníctvom SMS alebo MMS sú označované ako Smishing a útoky prostredníctvom telefonických hovorov ako Vishing (Alabdan, 2020, Lukehart, 2022, Salahdine, 2019, Sociálne inžinierstvo 2021). Prevažne množstvo phishingových útokov sa v súčasnosti realizuje prostredníctvom internetu. Medzi najčastejšie druhy týchto útokov patria:

- E-mail phishing,
- Spear phishing,
- Whaling,
- Pharming.

Email phishing – je založený na rozposielaní phishingových emailov veľkému množstu náhodných príjemcov. Útočníci často preberajú falošnú identitu dôveryhodných organizácií. Obsahom emailovej správy sú zvyčajne odkazy a prílohy, pomocou ktorých môže byť stiahnutý škodlivý softvér do prímateľovho zariadenia alebo môžu smerovať na nebezpečné weby, kde musí prijímateľ zadať svoje osobné údaje (Alabdan, 2020, Bhavsar, 2018, Shankar, 2019).

Spear phishing – je na rozdiel od email phishingu zameraný na jednotlivca, konkrétnu skupinu osôb alebo organizáciu. Útočníci sa vydávajú za osobu, ktorú prijímateľ pozná, čím zvyšuje svoju dôveryhodnosť a dokáže ľahšie ovplyvniť cieľového príjemcu (Alabdan, 2020, Bhavsar, 2018, Chiew, 2018).

Whaling – je zameraný na konkrétnych vedúcich pracovníkov, ako napríklad manažéri, riaditeľ alebo iní vysokopostavení zamestnanci, ktorí majú prístup k citlivým údajom organizácie (Alabdan, 2020, Bhavsar, 2018, Shankar, 2019).

Pharming – predstavuje technicky náročnejší druh phishingového útoku, kedy sa útočník snaží, aby táto webová stránka (vrátane domény) vyzerala ako web stránky bánk, poisťovní, inzertných portálov, sociálnych sietí a iných stránok, kde používateľ zadáva svoje osobné údaje. Zvyčajne je cieľom útočníkov krádež identity (Shankar, 2019).

Smishing – je obdobný spôsob, ako pri emailovom alebo spear phishingu, v tomto prípade však útočník využíva SMS komunikáciu. Útočník môže tiež kombinovať využívanie SMS a internetu, kedy prostredníctvom SMS odošle odkaz, pomocou ktorého sa do prijímateľovho zariadenia stiahne škodlivý softvér a útočník tak získa prístup k jeho údajom v mobilnom zariadení (Alabdan, 2020, Yeboah-Boateng, 2014).

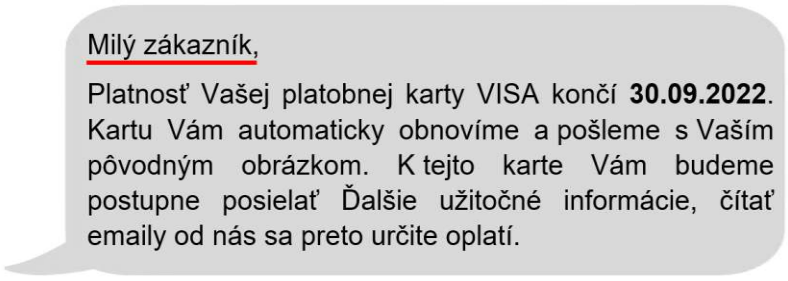
Vishing – využíva hlasovú komunikáciu na páchanie phishingových útokov, pričom vytvára na prijímateľa psychologický nátlak. Môžu byť tiež využité metódy iných druhov phishingových útokov (Yeboah-Boateng, 2014, Stavroulakis, 2010).

1.2. Signifikantné znaky phishingových útokov

Phishingové útoky sú často sofistikované a pôsobia dôveryhodne. Avšak existujú určité signifikantné znaky, na základe ktorých je možné identifikovať, že ide o phishingový útok. Poznanie týchto signifikantných znakov užívateľmi je dôležité z pohľadu odhaľovania phishingových útokov a tým zabránieniu zneužitia chránených údajov. Medzi najčastejšie vyskytujúce sa signifikantné znaky phishingových útokov patria najmä (Shankar, 2019):

- nesprávne oslovenie,
- formulácia textu,
- vyžadovanie osobných údajov,
- urgentnosť,
- neodolateľné ponuky
- podozrivé domény, odkazy alebo prílohy.

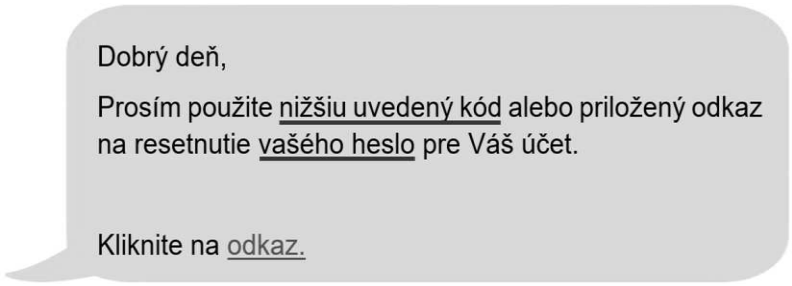
Oslovenie - organizácie často využívajú osobnejší prístup pri komunikácií so zákazníkmi a používajú oslovenia, ktoré obsahujú meno, priezvisko alebo osobné číslo zákazníka. Útočníci zvyčajne využívajú všeobecné oslovenia, bez použitia týchto údajov. Pomocou tohto znaku však nie je možné priamo identifikovať, že ide o phishingový útok, keďže niektoré organizácie nevyužívajú priame oslovenia. Na priamu identifikáciu phishingového útoku musia byť splnené aj ďalšie znaky phishingového útoku, ako napríklad: prítomnosť podozrivých domén, odkazov a príloh. Príklad nepriameho oslovenia je znázornený na obrázku 2 (Phishing, 2022, Harley, 2022, All About Phishing, 2022).



Obrázok 2 Vzor phishingového útoku – oslovenie (Vlastné spracovanie)

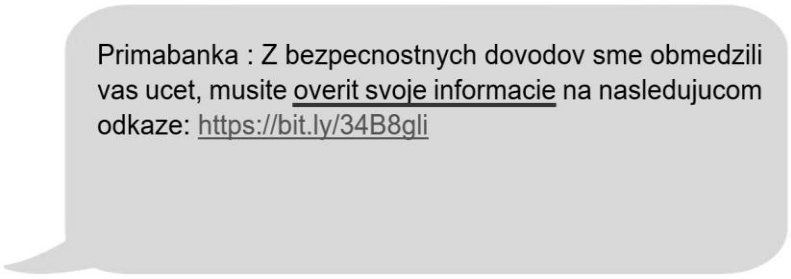
Formulácia textu – útočníci častokrát zle formulujú text alebo sa v texte nachádzajú gramatické chyby. Dôvodom môže byť často chybný preklad z iného jazyka pomocou verejne dostupných prekladačov. Práve výskyt týchto špecifík, môže prijímateľovi naznačiť, že sa jedná o phishingový útok. Avšak prijímateľ správy musí zostať obozretný, keďže aj v prípade, kedy je text formulovaný správne a bez

chýb, nie je zaručené, že sa jedná o legitímnu správu. Príklad podozrivej formulácie textu je znázornený na obrázku 3 (Phishing, 2022, All About Phishing, 2022).



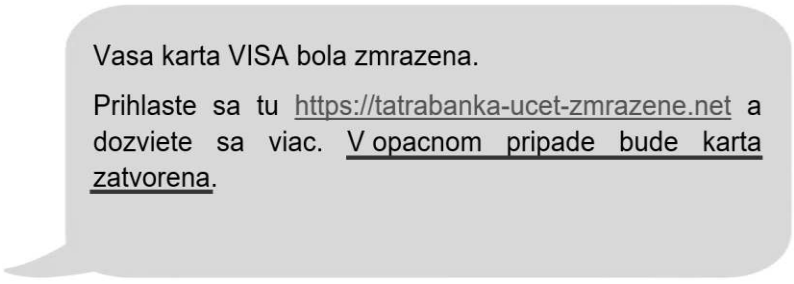
Obrázok 3 Vzor phishingového útoku – Formulácia textu (Vlastné spracovanie)

Osobné údaje – útočníci sa často vydávajú za dôveryhodné inštitúcie (banky, poisťovne, telekomunikačný operátor a podobne) a snažia sa o to, aby im prijímateľ poskytol citlivé informácie. Legitímne organizácie nikdy nežiadajú svojich zákazníkov, aby im poskytli svoje osobné údaje (číslo OP, číslo karty, prihlasovacie údaje a podobne). Príklad vyžadovania osobných údajov je znázornený na obrázku 4 (Phishing, 2022, All About Phishing, 2022).



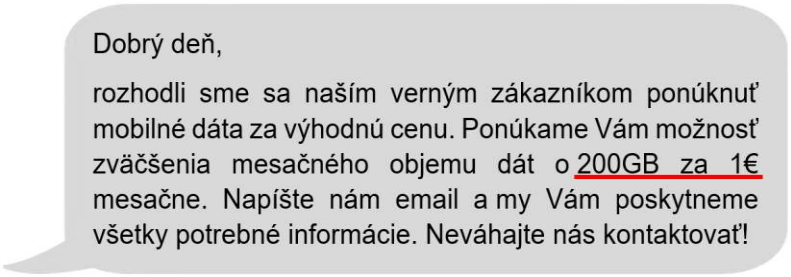
Obrázok 4 Vzor phishingového útoku – osobné údaje (Vlastné spracovanie)

Naliehanie – ďalším signifikantnými črtami pri phishingových útokoch môže byť naliehanie útočníka na prijímateľa. Útočník žiada od prijímateľa neodkladné úkony, ktoré musí prijímateľ vykonať ihneď. Útočníci často požadujú osobné údaje z dôvodu údajného narušenia bezpečnosti používateľského konta a podobne. Príklad naliehania je znázornený na obrázku 5 (Phishing, 2022, All About Phishing, 2022).



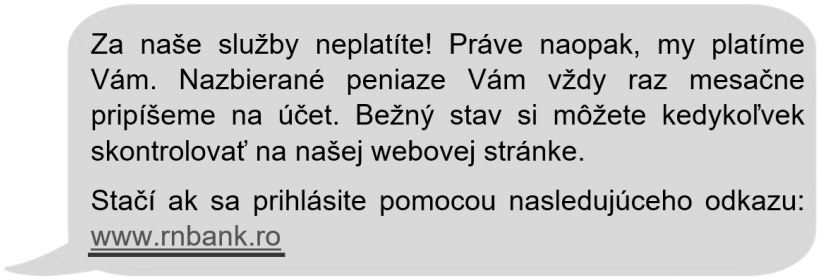
Obrázok 5 Vzor phishingového útoku – naliehanie (Vlastné spracovanie)

Príliš výhodné ponuky – útočníci často lákajú svoje obete na ponuky, ktoré znejú neodolateľne a príliš výhodne. Môže sa jednať napríklad o tvrdenie, že prijímateľ vyhral finančné prostriedky, získava výhody od operátora alebo iné podozrivo výhodné ponuky, ktoré sú však nepravdivé. Príklad podozrivej ponuky je znázornený na obrázku 6 (Phishing, 2022, All About Phishing, 2022).



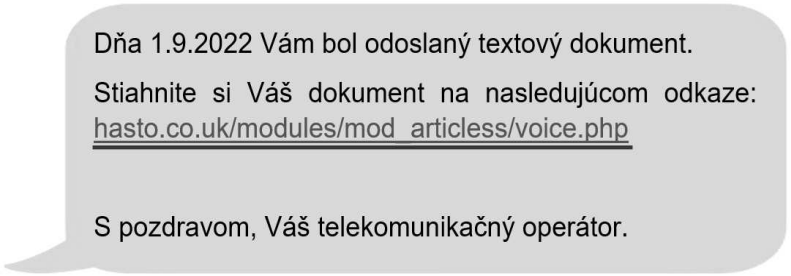
Obrázok 6 Vzor phishingového útoku – príliš výhodné ponuky (Vlastné spracovanie)

Doména – nakoľko sa páchateľ snaží vystupovať dôveryhodne, často využíva doménu, ktorá je podobná organizácii, za ktorú sa vydávajú. Častým príkladom môže byť zamenenie symbolov alebo písmen v doméne. Niekedy sú však páchatelia menej opatrní a využívajú úplne rozdielne domény, bez snahy o napodobenie originálnej domény alebo využívajú zahraničné domény. Útočník môže napríklad použiť rumunskú doménu (.ro), prípadne inú zahraničnú doménu, čo vzbudzuje pozornosť, pokiaľ sa vydáva za organizáciu, ktorá sídli v Slovenskej republike. Príklad podozrivej domény je znázornený na obrázku 7 (Phishing, 2022, Simister, 2021).



Obrázok 7 Vzor phishingového útoku – doména (Vlastné spracovanie)

Odkazy a prílohy – útočníci sa často snažia presmerovať svoje obete na škodlivé web stránky, kde musí používateľ uviezť svoje osobné údaje alebo kde bude do jeho zariadenia stiahnutý škodlivý softvér. Na to využívajú útočníci rôzne formy odkazov na web stránky, hypertextové odkazy alebo prílohy v emailovej komunikácií. Príklad podozrivej formulácie textu je znázornený na obrázku 8 (Phishing, 2022, Simister, 2021).



Obrázok 8 Vzor phishingového útoku – odkazy a prílohy (Vlastné spracovanie)

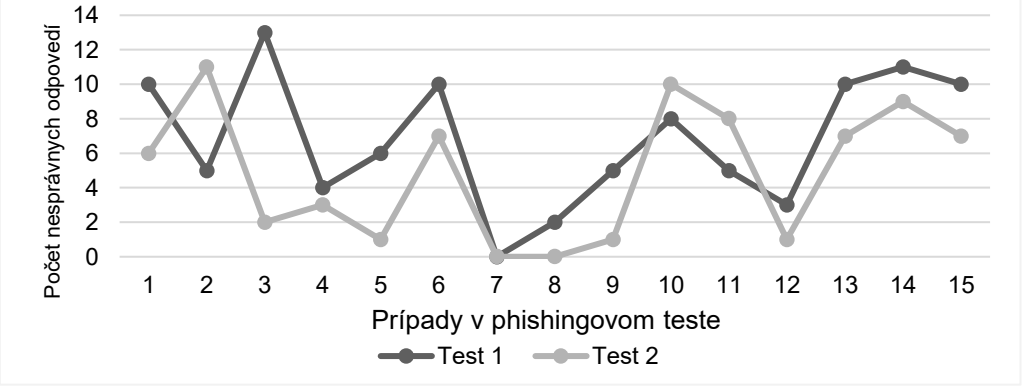
Poznanie signifikantných znakov phishingových útokov je základným predpokladom na ich zastavenie a minimalizovanie možných dopadov. Jedným so spôsobov, ako zvýšiť povedomie o týchto znakoch je vzdelávanie užívateľov. V rámci vzdelávania je potrebné sa zameriavať na: hrozby phishingových útokov, spôsoby, ako odhaliť rôzne druhy phishingu pomocou ich signifikantných znakov a taktiež na overovanie vedomostí, napríklad prostredníctvom phishingového testovania.

2. METODICKÝ POSTUP

Prvým krokom prípravy vzdelávania užívateľov bola príprava školiacich materiálov, ktorých obsah má slúžiť na oboznamovanie sa vybranej skupiny užívateľov o phishingových útokoch. Informácie obsiahnuté v školiacich materiáloch sa zameriavajú hlavne na signifikantné znaky phishingových útokoch. Vybraný spôsob školenia bol formou prezentácie, ktorej cieľom bolo poukázať na tieto znaky, a možné spôsoby ako ich odhaliť v praxi. Ďalším krokom bolo overenie prínosu školenia, a teda schopnosti identifikovať phishingový email alebo SMS daným užívateľom. Na toto overenie bol primárne spracovaný phishingový test, ktorý pozostáva z titulnej strany a pätnástich príkladov emailov alebo SMS. V phishingovom teste sa nachádzalo 5 legitímnych a 10 podvodných emailov alebo SMS. Respondenti, resp. užívatelia svoje odpovede značili do odpoveďového hárku. Samotné školenie a overenie získaných vedomosti bolo realizované vo vybranej organizácie a po konzultácií s vedením spoločnosti prebehlo preferovanou fyzickou účasťou školiteľa v priestoroch organizácie. Pred vykonaním školenia respondenti spracovali prvý phishingový test, v rámci ktorého bolo potrebné identifikovať phishingové a legitímne emaily a následne označiť odpovede do odpoveďového hárku. Po vypracovaní phishingového testu bolo realizované školenie, v rámci ktorého boli respondenti oboznámení s phishingom ako aj so signifikantnými znakmi, ktoré sú charakteristické pre phishingové emaily alebo SMS. Cieľom tohto školenia bolo primárne rozšíriť vedomosti užívateľov, resp. respondentov o možnostiach ako odhaliť phishingové útoky v praxi. Po vykonaní školenia, boli respondenti požiadaní o vyplnenie druhého phishingového testu, ktorý bol identický s prvým, avšak respondenti svoje odpovede zaznačovali do druhého odpoveďového hárku. Vykonanie phishingového testu pred a po školení poskytuje informácie, ktoré hovoria o pripravenosti respondentov na phishingové útok a o ich schopnostiach odhaľovať ich. Samozrejme, plán vzdelávania musí byť rozšírený o cykly školení tak, aby informácie získané z prvotného školenia boli v užívateľoch upevňované a rozširované.

3. TESTOVANIE PRIPRAVENOSTI NA PHISHINGOVÝ ÚTOK

Testovanie pripravenosti na phishingový útok bolo realizované v skupine 15 respondentov vo vybranom zdravotníckom zariadení. Respondenti dosiahli v prvom phishingovom teste úspešnosť 55 %. V druhom phishingovom teste, ktorý bol realizovaný až po aktívnom preškolení, dosiahli respondenti úspešnosť 68 %, čo predstavuje zlepšenie o 13 % v porovnaní s prvým phishingovým testom. Z celkového počtu 15 respondentov bolo pri 13 respondentov zaznamenané zlepšenie výsledkov v porovnaní s výsledkami nadobudnutými z prvého phishingového testu. Jeden respondent dosiahol totožné výsledky v oboch phishingových testoch a jeden respondent preukázal zhoršenie v rámci druhého phishingového testu. Vyhodnotenie testov bolo zamerané i na komparáciu nesprávnych odpovedí v jednotlivých phishingových testoch, podľa čoho je možné zistiť, v ktorých otázkach vzniklo najviac nesprávnych odpovedí, a teda v ktorých oblastiach musia byť respondenti ešte preškolení. V druhom phishingovom teste v porovnaní s prvým klesol počet nesprávnych odpovedí takmer vo všetkých prípadoch, okrem prípadov 2, 10 a 11. Porovnanie nesprávnych odpovedí je znázornené na obrázku 9.



Obrázok 9 Porovnanie nesprávnych odpovedí vo phishingových testoch (Vlastné spracovanie)

Prípad 2 reprezentuje legitímny reklamný email, v rámci ktorého bola prijímateľovi zaslaná zľava vo výške 10 %. V danom prípade boli respondenti v druhom phishingovom teste viac skeptický, nakoľko sa v danom prípade nachádzala ponuka zľavy na nákup, odkaz na zahraničnú doménu a tiež kontaktné údaje so zahraničnou doménou. Emailová správa je však legitímna, keďže výška 10% nepredstavuje neodolateľnú ponuku a obdobná zľava je bežne poskytovaná stálym zákazníkom. Spoločnosť tiež využíva zahraničnú doménu, keďže sa jedná o medzinárodnú spoločnosť.

V prípade 10 bola respondentom predložená legitímna emailová správa od banky, so žiadosťou o overenie údajov. Respondenti ho však považovali za podvodný pravdepodobne kvôli nepriamemu osloveniu a nutnosti prihlásenia pomocou odkazu uvedeného v texte. Prípad 10 je však legitímny, keďže na oslovenie bolo použité osobné číslo klienta a uvedený odkaz smeruje na legitímnu webovú adresu.

V ďalšom prípade, označenom pod číslom 11 bola respondentom predložená legitímna emailová správa od spoločnosti Microsoft so žiadosťou o overenie emailovej adresy. Zvýšený počet nesprávnych odpovedí v druhom phishingovom teste mohol byť spôsobený hlavne kvôli kontaktným údajom odosielateľa, keďže pôsobia nezvyčajne a respondenti ich mohli vyhodnotiť ako podvodné. Avšak v prípade, že tieto kontaktné údaje dohľadáme prostredníctvom online vyhľadávača, tak zistíme, že údaje sú legitímne a daná spoločnosť ich bežne využíva na kontaktovanie svojich zákazníkov.

Na základe takto realizovaných školení je možné zvyšovať povedomie užívateľov o phishingových útokoch, ktoré v súčasnosti tvoria až 53,4 % všetkých zaznamenaných útokov (Štatistika, 2022) a taktiež môže byť súčasťou dlhodobého plánu rozvoja v rámci organizácie, ktorý je pre niektoré organizácie vyžadovaný zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

4. DISKUSIA

Hlavným cieľom prieskumu bolo zistiť pripravenosť na phishingové útoky u vybranej skupiny užívateľov, rozšíriť ich povedomie o phishingových útokoch a v neposlednom rade overiť účinnosť takýchto školení vo vzťahu k phishingovým útokom. Referenčnú skupinu v našom prípade predstavovalo 15 zamestnancov zdravotníckeho zariadenia, ktorí mali rovnaké pracovné zaradenie. Daná skupina respondentov bola zvolená hlavne z dôvodu, že v rámci svojej profesie aktívne využívajú internetové, SMS a telefonické komunikačné kanály, čo zvyšuje riziko hrozby phishingových útokov a následného potenciálneho dopadu, ktorý v zdravotníckych zariadeniach môže byť veľmi veľký.

Výsledky, ktoré boli získané od danej referenčnej skupiny poukazujú na to, že phishingové školenia boli efektívne, nakoľko sa podarilo zvýšiť úspešnosť správnych odpovedí v druhom phishingovom teste, ktorý bol realizovaný až po phishingovom školení. Taktiež sa podarilo odhaliť oblasti, ktorým je nevyhnutné sa venovať v ďalších cykloch školení. Tieto oblasti vyplynuli z odpovedí respondentov, ktoré nevykazovali progres zlepšenia. Prezentované mechanizmy je možné uplatniť v akejkoľvek referenčnej skupine s cieľom zníženia úrovne úspešností phishingových útokov

ZÁVER

Téma kybernetickej bezpečnosti je v súčasnosti na vzostupe. Výrazný vplyv na jej vzostup mal práve COVID – 19, keďže sa veľa pracovných činnosti presunulo do kybernetického prostredia. Organizácie si uvedomujú význam kybernetickej bezpečnosti a snažia sa ju zaistiť rôznymi technickými prostriedkami. Avšak najväčší podiel útokov je realizovaných prostredníctvom sociálneho inžinierstva, ktorého názov vychádza z psychologického pôsobenia na ľudí, za účelom ich oklamania a okradnutia. Používané sú rôzne typy sociálneho inžinierstva, avšak v článku sme sa zamerali na phishing, ktorý tvorí najvýraznejší podiel a na postup školení a testovaní, ktoré vplývajú na úroveň povedomia zamestnancov, resp. užívateľov.

Školiace materiály a metodické postupy boli aplikované v rámci prieskumu u zamestnancov vybraného zdravotníckeho zariadenia. Komparácia a analýza jednotlivých výsledkov poukázala na efektívnosť týchto mechanizmov, a preto je možné ich použiť ako formu prevencie pred phishingovými útokmi v rôznych organizáciách.

POĎAKOVANIE

Tento článok bol pripravený v rámci podpory projektu APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach.

LITERATÚRA

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future internet*. 12(10), 169. ISSN 1999-5903

All About Phishing Scams & Prevention: What You Need to Know (2022). AO Kaspersky Lab. Retrieved September 13, 2022, from https://www.kaspersky.com/resource-center/preemptive-safety/phishingprevention-tips

Bhavsar, V., Kadlak, A., & Sharma S. (2018). Study on Phishing Attacks. *International Journal of Computer Applications.* 182(33), 27-29. ISSN 0975-8887

Harley, D. & Lee, A. (2007). PHISH PHODDER: IS USER EDUCATION HELPING OR HINDERING?. ESET, spol. s.r.o.. Retrieved September 13, 2022, from https://www.welivesecurity.com/wpcontent/uploads/2012/11/PhishPhodder.pdf

Chiew, K., Yong, K., & Tan, Ch. (2018). A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches. *Expert Systems With Applications.* 106(1), 1-20. ISSN: 0957-4174

Lukehart, A. (2022). 2022 Cyber Attack Statistics, Data, and Trends. Parachute Technology. Retrieved September 13, 2022, from https://parachutetechs.com/2022-cyber-attack-statistics-data-and-trends/

Phishing, (2022) ESET, spol. s r.o.. Retrieved September 13, 2022, from https://www.eset.com/sk/phishing/

Salahdine, F. & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future internet*. 11(4), 89. ISSN 1999-5903

Shankar, A., Shetty, R., & Nath K, B. (2019). A Review on Phishing Attacks. *International Journal of Applied Engineering Research*. 14(9), 2171-2175. ISSN 0973-4562

Simister, A. (2021). 10 Ways to Prevent Phishing Attacks. Lepide Retrieved September 13, 2022, from https://www.lepide.com/blog/10-ways-toprevent-phishing-attacks/

Sociálne inžinierstvo (2021). Ministerstvo investícií, regionálneho rozvoja a informatizácie SR. Retrieved September 13, 2022, from https://www.csirt.gov.sk/socialne-inzinierstvo.html

Stavroulakis, P., & Stamp, M. (2010). Handbook of Information and Comminication Security. Springer.

Štatistika incidentov 2021 (2022). Ministerstvo investícií, regionálneho rozvoja a informatizácie SR. Retrieved September 13, 2022, from: https://www.csirt.gov.sk/

Yeboah-boateng, E., & Amanor, P. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*. 5(4), 297-307. ISSN 2079-8407

Matúš Madleňák, Ing.

Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, 010 26 Žilina

e-mail: madlenak3@uniza.sk

Katarína Kampová, doc., Ing., PhD.

Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, 010 26 Žilina

e-mail: katarina.kampova@uniza.sk