PŘÍRUČKA O SOCIÁLNÍM INŽENÝRSTVÍ

Pro firmy

Obsah

Proč by se malé a středně velké podniky (SMB) měly zajímat o sociální inženýrství?

Podle průzkumu provedeného v roce 2019 společností Zogby Analytics pro americkou neziskovou společnost National Cyber Security Alliance si malé a střední podniky stále více uvědomují, že jsou cílem počítačových zločinců. Téměř polovina (44 %) společností s 251 až 500 zaměstnanci uvedla, že se v posledních 12 měsících setkala s únikem dat. Průzkum zjistil, že se 88 % malých podniků domnívá, že jsou přinejmenším „do jisté míry pravděpodobným" cílem počítačových zločinců. Z toho téměř polovina (46 %) se domnívá, že jsou „velmi pravděpodobným" cílem.

Škody jsou hmatatelné a rozsáhlé, což dobře dokládá výroční zpráva Útvaru FBI pro vyšetřování internetového zločinu (IC3). Jen v roce 2020 obdržel útvar IC3 19 369 stížností na podvody realizované zneužitím firemních e-mailů (BEC) nebo zneužitím e-mailových účtů (EAC) s odhadovanými ztrátami přesahujícími 1,8 miliardy dolarů. BEC/EAC jsou sofistikované podvody zaměřené na firmy i jednotlivce, kteří provádějí převody finančních prostředků.

Jak uvádí zpráva Data Breach Investigations Report za rok 2019, zahrnovalo 33 % narušení útoky využívající techniky sociálního inženýrství, což z nich činí druhou nejpoužívanější taktiku po hackerských útocích.

Po narušení bezpečnosti

utrpělo finanční ztrátu	podalo návrh na konkurz	ukončilo svoji činnost
37 %	25 %	10 %

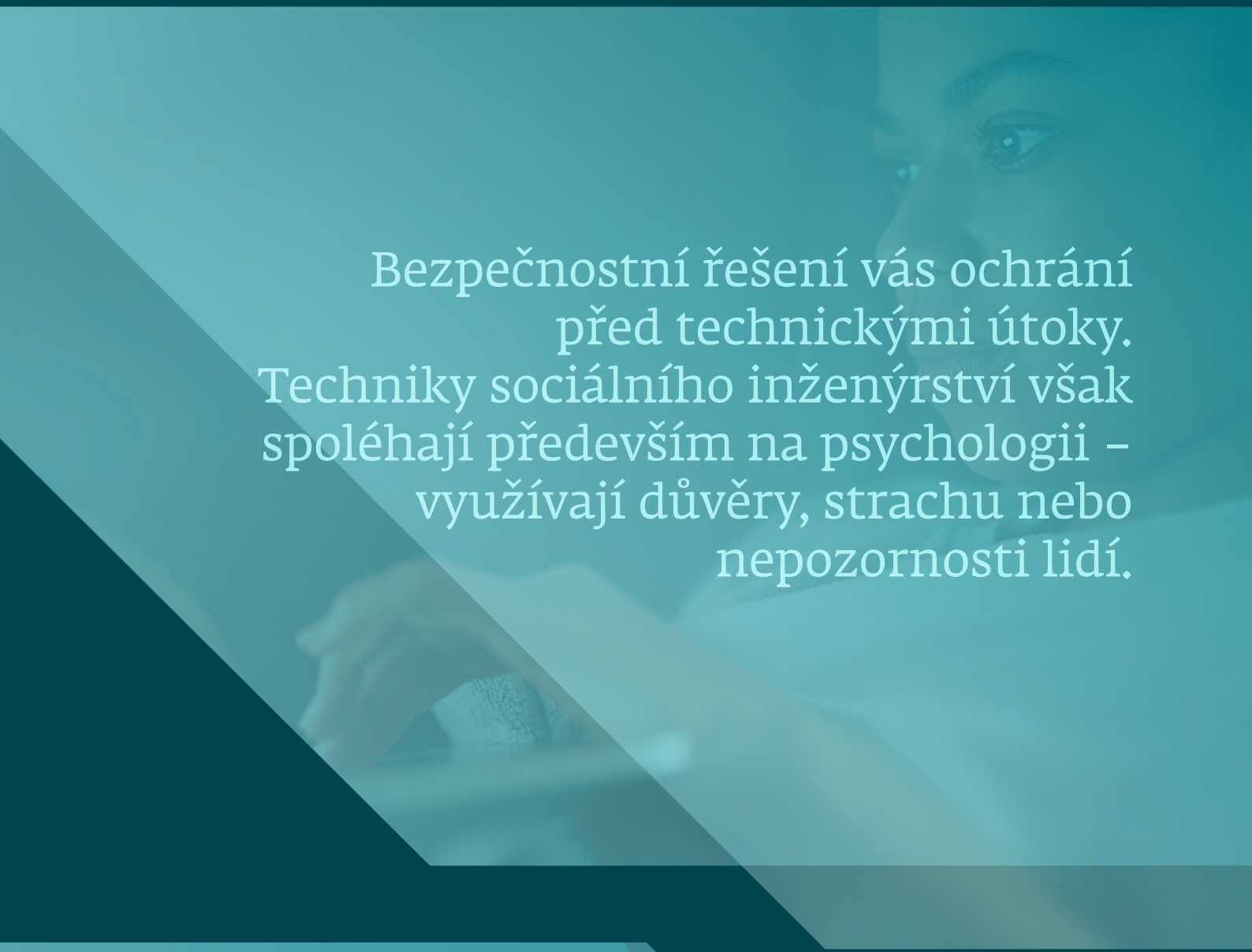
malých a středně velkých podniků

Zdroj: NCSA

Úvod

Cílem této příručky je pomoci firmě seznámit všechny zaměstnance se sociálním inženýrstvím a jeho riziky. Lidé jsou citově založené bytosti a sociální inženýrství je velmi účinný způsob, jak toho využít. Útoky tohoto typu navíc obvykle nevyžadují od útočníka odborné technické znalosti. Dosavadní zkušenosti ukazují, že přesvědčit ohromné množství uživatelů, aby prozradili citlivé informace nebo provedli škodlivé kroky, je poměrně jednoduché. Nenechte se zmást – i vy se můžete snadno stát terčem.

Na následujících stránkách najdete přehled trendů v oblasti sociálního inženýrství a příklady nejčastějších typů útoků, které můžou ovlivnit chování zaměstnanců na internetu. Najdete zde také informace, jak tyto útoky rozpoznat a chránit sebe i svou firmu.



Bezpečnostní řešení vás ochrání před technickými útoky. Techniky sociálního inženýrství však spoléhají především na psychologii – využívají důvěry, strachu nebo nepozornosti lidí.

Typy technik sociálního inženýrství

Cílený phishing
Cílená forma phishingu zaměřená na konkrétní osobu, organizaci nebo firmu. Liší se tak od typických phishingových kampaní, které se nezaměřují na jednotlivé oběti, ale míří ke stovkám tisíc příjemců.

Vishing
Tato metoda se podobná phishingu, avšak místo e-mailů využívá podvodné telefonáty. Počítačoví zločinci se přitom často vydávají za zástupce banky nebo pojišťovny.

Smishing
Pokus o sociální inženýrství prostřednictvím SMS. Cílem smishingového útoku je obvykle přesměrování obětí na webovou stránku, která má za cíl získat jejich údaje. Vyskytují se však i kampaně, při nichž jsou oběti žádány o zaslání citlivých údajů přímo v odpovědi na SMS.

(Sexuální) vydírání
Tento typ útoků využívá schéma podvodných e-mailů, které se snaží vydírat oběti pomocí nepodložených tvrzení a obvinění.

Impersonace
Technika impersonace, nazývaná také zosobnění, používá stejné postupy jako v reálném světě. Počítačoví zločinci, kteří se obvykle vydávají za generálního ředitele společnosti, kontaktují zaměstnance a snaží se je zmanipulovat, aby podnikli určité kroky, například objednali a schválili podvodné transakce.

Scareware
Software, který používá různé techniky, aby u obětí vyvolal úzkost a donutil je instalovat si do zařízení další škodlivý kód. Příkladem je falešný antivirový produkt, který podvodem přesvědčí uživatele, aby si nainstalovali určitý software k vyřešení konkrétního problému, avšak tento program je obvykle škodlivý.

Falešná technická podpora
Útočníci se snaží prodat falešné služby, odstranit neexistující problémy nebo nainstalovat řešení vzdáleného přístupu do zařízení oběti a získat neoprávněný přístup k jejím datům.

Phishing

Pravděpodobně jste již někdy v životě obdrželi e-mail, který vám zdánlivě zaslala banka nebo nějaká oblíbená online služba, s žádostí o potvrzení přihlašovacích údajů nebo čísla kreditní karty. Jedná se o běžnou phishingovou techniku. Phishingové pasti se však neustále mění a někdy je těžké je rozpoznat.

Phishing je forma útoku využívající sociální inženýrství, při kterém se útočník snaží získat přístup k přihlašovacím údajům, získat důvěrné informace nebo doručit malware. Phishingové kampaně obvykle cílí na velké množství anonymních uživatelů. Mohou však mířit i na konkrétní oběť nebo malou skupinu obětí, které spolu nějak souvisí, přičemž v takovém případě se využívají přizpůsobené podvodné zprávy (cílený phishing). Útoky zaměřené na konkrétní, většinou vysoce postavené osoby, například členy vrcholového managementu nebo majitele společností, jsou označovány jako „velrybaření" (útočníci cílí na „velké ryby").

Podvodníci přitom vědí, že poskytovatel e-mailových služeb s velkou pravděpodobností každou zprávu zkontroluje, zda neobsahuje škodlivý obsah, a přesměruje takové e-maily do složky s nevyžádanou poštou. Proto se obsah podvodných zpráv často mění.

Podle společnosti Google odeslali podvodníci uživatelům Gmailu v březnu 2020 každý den 18 milionů phishingových e-mailů týkajících se pandemie COVID-19.

Phishing

Vypuknutí pandemie COVID-19 se pro podvodníky stalo příležitostí, jak vydělávat na nejistotě, strachu a nedostatku dodávek spojených s touto krizí. Jak odhaluje zpráva Threat Report Q1/2020 společnosti ESET, došlo v březnu 2020 k záplavě spamu s tématikou COVID-19, který šířil malware, snažil se pomocí phishingu získat citlivé informace nebo nabízel falešné produkty.

Není žádným překvapením, že se pandemie stala jedním z hlavních lákadel používaných útočníky. Každá krize přináší nové okolnosti, které počítačovým zločincům poskytují ideální prostředí k inovacím.

Devadesát čtyři procent malwaru je doručeno e-maily.

Každou minutu dochází v důsledku phishingových útoků ke ztrátám v hodnotě 17 700 dolarů.

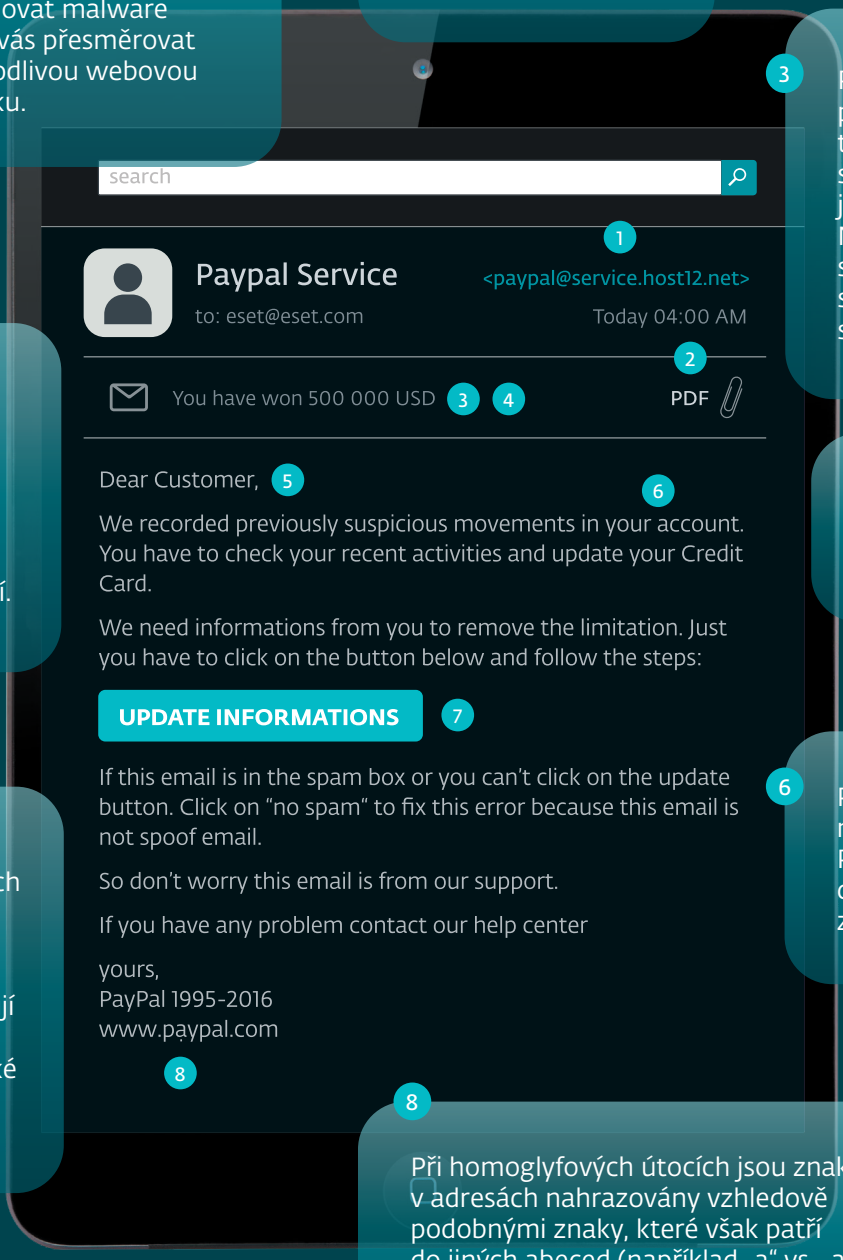
Každý den je odesláno přibližně 14,5 miliardy spamů.

Zdroje: CSO, hostingtribunal.com

Základní znaky phishingu

1 S obsahem zpráv odeslaných z neznámé e-mailové adresy zacházejte velmi obezřetně.

2 Nedůvěřujte přiloženým souborům ani neznámým odkazům. Mohou obsahovat malware nebo vás přesměrovat na škodlivou webovou stránku.



3 Příliš děsivé, nebo příliš dobré na to, aby to byla pravda? Pak se pravděpodobně jedná o podvod. Nezapomeňte, že sociální inženýrství se zaměřuje na lidské slabosti.

4 Předmět se liší od zprávy.

5 Příliš obecný pozdrav může znamenat, že zpráva nebyla adresována pouze vám, ale i řadě dalších lidí.

6 Podezřelá naléhavost? Podvodník chce, abyste zpanikařili.

7 Ve phishingových e-mailech přeložených z jiných jazyků se často vyskytují pravopisné a jiné gramatické chyby.

8 Při homoglyfových útocích jsou znaky v adresách nahrazovány vzhledově podobnými znaky, které však patří do jiných abeced (například „ạ“ vs. „a“ v adrese paypal.com).

Smishing

Smishing je typ phishingu, který využívá textové zprávy neboli SMS. I tato metoda se hojně využívala během prvních měsíců pandemie COVID-19. V této nepřehledné době například lidé dostávali SMS zprávy, které se vydávaly za oficiální zprávy od místních samospráv.

Tyto útoky mají podobný cíl jako phishing. Počítačoví zločinci se mohou **pokusit získat od vás osobní údaje nebo vás donutit kliknout na odkaz směřující na škodlivou webovou stránku**. Další technika je založená na lidském soucitu. Počítačoví zločinci zasílají textové zprávy s žádostí o příspěvek lidem v zoufalé situaci, například na fond pro oběti hurikánu nebo jiný druh charity, přičemž obvykle požadují údaje o vaší platební kartě.

Zpočátku mnoho lidí překvapilo, že hackeři mohou získat jejich telefonní čísla bez jejich vědomí. Jak ale upozorňuje mnoho odborníků na kybernetickou bezpečnost, **je snazší získat něčí telefonní číslo než e-mail, protože u telefonních čísel existuje konečný počet možností**. Uhodnout názvy e-mailových adres je obtížnější, protože obsahují více znaků.

Poznáte, co je na této SMS podezřelé?

Banka by vám pravděpodobně nikdy takto neposlala přímý odkaz. Pokud si nejste jisti, přejděte do internetového bankovnictví a zkontrolujte, zda jste i zde obdrželi stejnou zprávu. Vždy je bezpečnější přejít na oficiální webové stránky než kliknout na podezřelý odkaz.

Vishing

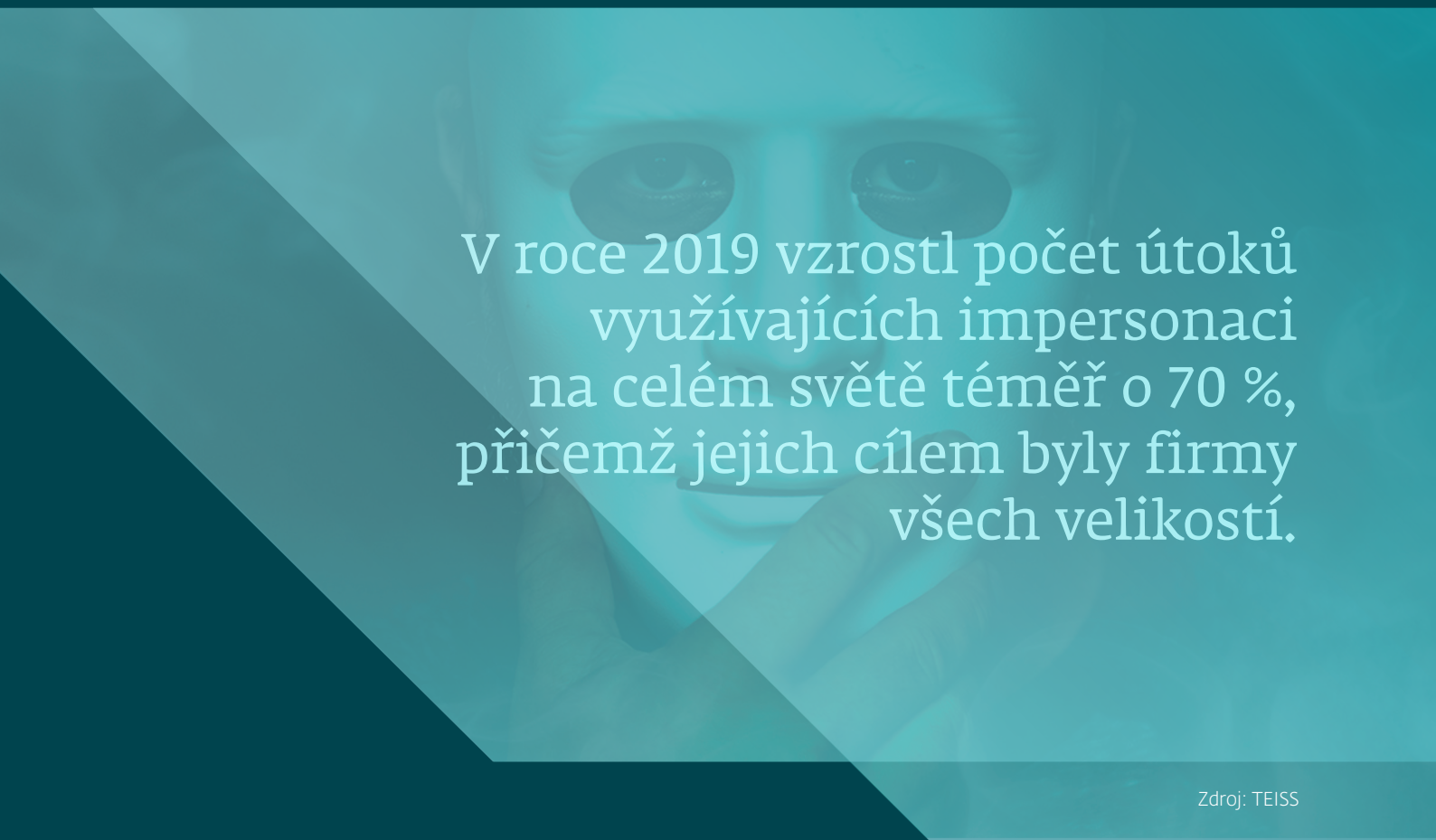
Vishing vyžaduje ještě větší herecké schopnosti než jiné typy podvodů. Obvyklý scénář je následující: Zavolá vám podvodník, který se **vydává za zástupce oficiální instituce**. Sdělí vám, že se do vašeho bankovního účtu někdo pokoušel nabourat, nebo vám nabídne nevyžádanou půjčku ve snaze získat osobní a finanční údaje. Zdá se vám jeho tvrzení příliš dobré, nebo příliš špatné na to, aby to byla pravda? Zeptejte se na další podrobnosti a **nesdělujte bez rozmyšlení žádné citlivé údaje**. Případně můžete hovor ukončit a sami se obrátit na zákaznický servis své banky, abyste si nastalou situaci ověřili.

Impersonace: Když se útočník vydává za generálního ředitele

Podívejme se na další metodu útoku využívající sociální inženýrství, kdy se počítačoví zločinci vydávají za důvěryhodné osoby a snaží se manipulovat s oběťmi. Jak poznáte, že vás místo kolegy kontaktuje podvodník?

Při impersonaci se útočník vydává za někoho jiného, v tomto případě **protože chce získat informace nebo přístup k osobě, společnosti nebo počítačovému systému.** K dosažení těchto cílů používají počítačoví zločinci mimo jiné telefonní hovory, e-maily nebo aplikace pro zasílání zpráv. V mnoha případech si útočníci vybírají jména z top managementu společnosti a vytvářejí e-maily, které vypadají, jako by je skutečně napsal příslušný manažer.

Je až neuvěřitelné, kolik firemních informací o struktuře společnosti a jménech zaměstnanců je dostupných na platformách, jako je LinkedIn. Útočník se může pomocí těchto údajů pokusit kontaktovat vybrané zaměstnance firmy a **požádat je o převedení peněz, uhrazení faktur nebo zaslání důležitých údajů**. Právě proto, že tyto útoky mohou způsobit únik dat a finanční ztráty, jsou impersonace pro firmy tak nebezpečné.

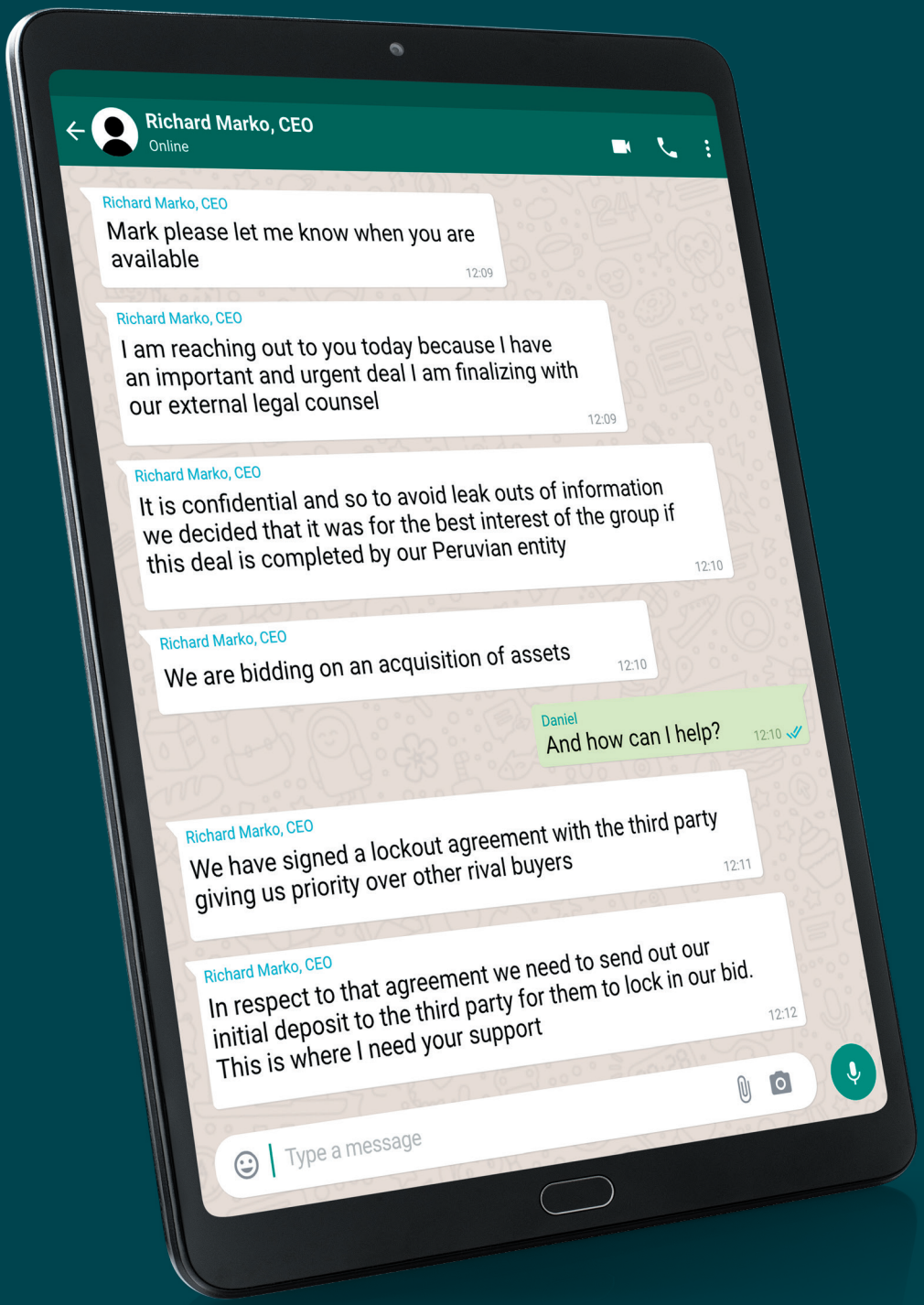


V roce 2019 vzrostl počet útoků využívajících impersonaci na celém světě téměř o 70 %, přičemž jejich cílem byly firmy všech velikostí.

Zdroj: TEISS

Skutečný příběh: Útok impersonací na společnost ESET

Cílem kybernetického útoku se může stát každá organizace. V roce 2020 čelila společnost ESET útokům, kdy se podvodník vydával za generálního ředitele prostřednictvím zpráv v aplikaci WhatsApp. Cílem těchto pokusů bylo předstírat existenci významné nabídky, která vyžadovala finanční zálohu.



Jak odvrátit útoky využívající impersonaci

Klíčem k úspěchu je všímavost. Čím více toho o útocích založených na předstírání identity víme, tím lépe se jim můžeme vyhnout. Podívejme se, jak fungují e-maily používané při impersonaci. Mnohé z nich se snaží v obětech vyvolat pocit naléhavosti a obav, který je má přinutit k provedení požadovaného úkolu. Může jít o něco, co by vám připadalo neobvyklé a podezřelé, jako jsou nákupy, které nesouvisejí s podnikáním společnosti, u klientů, které neznáte. Útočníci také obvykle pro splnění požadovaných úkolů stanoví krátkou lhůtu.

Podvodné zprávy často obsahují gramatické chyby nebo je v nich nesprávně použit firemní branding. Toto jsou však jen ty snáze rozpoznatelné e-maily. Útočníci zběhlí ve vydávání se za jinou osobu mohou vytvořit e-mailovou zprávu, která vypadá velmi reálně, včetně oficiální fotografie zaměstnance nebo podpisu na konci e-mailu. I když se tedy šablona zdá být v pořádku, buďte obezřetní, pokud se vám požadavek ve zprávě zdá zvláštní.

ZAMYSLETE SE NAD SOUVISLOSTMI

Někdy jsme příliš zaneprázdněni a rozhodujeme se bez velkého přemýšlení. Možná vám to zabere pár vteřin navíc, ale vždy zvažte, zda e-mail dává smysl. Proč přesně se tento kolega ptá právě na tento nákup nebo žádá tyto citlivé osobní informace? **Cokoli, co je neobvyklé a odchyluje se od tradičních postupů, by mělo být varovným signálem**. I když e-mail podle všeho pochází od důvěryhodné osoby, například od generálního ředitele, může se jednat o podvod. Buďte ostražití a ověřte si všechny požadavky u svých kolegů.

MIMO KANCELÁŘ?

Někdy mohou počítačoví zločinci vědět, že je někdo mimo kancelář, a jednat, jako by ho zastupovali. V takovém případě si příslušné informace ověřte u nadřízeného nebo spolupracovníků osoby, kterou útočník zdánlivě zastupuje. Jak se říká, dvakrát měř, jednou řež.

Jak odvrátit útoky využívající impersonaci

KONTROLUJTE E-MAILOVOU ADRESU

Přišel vám firemní e-mail z osobního účtu? E-mailová adresa může zdánlivě patřit někomu, koho znáte. Vždy je však lepší odpovědět dané osobě na její oficiální e-mailovou adresu. Někdy také mohou hackeři použít e-mail, který vypadá téměř jako oficiální firemní adresa, jen s malou odchylkou, například „m“ je nahrazeno písmeny „rn“.

Implementujte štítek „EXTERNÍ“

V rámci nedávné změny interního zabezpečení ve společnosti ESET jsou e-maily přicházející mimo firemní doménu vždy označeny jako EXTERNÍ. Toto opatření by sice nepomohlo, pokud by podvodník předstíral odeslání e-mailové zprávy ze soukromého e-mailu generálního ředitele, ale může pomoci identifikovat e-maily, které se snaží falšovat doménu (viz výše uvedenou záměnu „m“ a „rn“).

OVĚŘTE IDENTITU OSOBY PROSTŘEDNICTVÍM JINÉHO KOMUNIKAČNÍHO KANÁLU

Pokud jste obdrželi podezřelou zprávu na WhatsAppu, měli byste dané osobě napsat prostřednictvím firemního e-mailu nebo jí zavolat zpět. Nebo se jí jednoduše **zeptejte osobně**. Nebojte se, že budete obtěžovat, i když třeba zrovna daná osoba nemá čas. Možná byste si netroufli vyrušovat svého generálního ředitele. Není se čemu divit, protože čím vyšší pozici kolega má, tím více váháme, zda ho oslovit, zvlášť když je mimo kancelář. V takovém případě **zvažte konzultaci s kolegou nebo nadřízeným**. Například o naléhavé platbě velké faktury po splatnosti by jistě věděl (nebo měl vědět) finanční nebo provozní ředitel, takže se s nimi poraďte. Pamatujte, ostražitost se vyplácí.

(Sexuální) vydírání

„Ahoj, příteli. Ty mě neznáš, ale já tě znám velmi dobře. Lépe, než bys čekal. Tohle je tvoje heslo, že?“

E-mail, jako je tento, se může objevit i ve vaší poštovní schránce. Záhadný vyděrač obvykle tvrdí, že příjemce e-mailu sledoval přes webovou kameru, když se díval na obsah pro dospělé, a nutí jej, aby zaplatil, jinak to řekne rodině a spolupracovníkům. Aby dokázal, že se do počítače skutečně naboural, uvede nějaké heslo, které oběť používá. Takovéto vydírání je však obvykle podvod.

ŽIJEME VE ZLATÉM VĚKU VYDĚRAČSKÝCH PODVODŮ

Zářným příkladem toho, jak hackeři zneužívají technologie a krizi k šíření podvodů, je pandemie COVID-19. S přechodem mnoha společností na vzdálenou práci a domácí kanceláře, kde zaměstnance nechrání firemní síť, počet webových hrozeb výrazně vzrostl. Počítačoví zločinci například vyhrožovali oběti, že pokud nesplní jejich podmínky, nakazí ji a její rodinu koronavirem.

Když zaplatíte požadovanou částku, přijdete o peníze, podpoříte podnikání zločinců a pomůžete jim páchat další podvody.

POCHOPTE, CO ÚTOČNÍK CHCE

Měli byste vědět, že hlavním účelem vyděračských e-mailů je donutit vás zaplatit – nejlépe v bitcoinech, což hackerům umožňuje anonymní výběr peněz. Podvody jsou skvělý byznys: Podle Útvaru FBI pro vyšetřování internetového zločinu způsobilo v roce 2020 vydírání e-mailem ztráty ve výši přibližně 70,9 milionu dolarů.

JAK REAGOVAT NA VYDĚRAČSKÉ PODVODY

Neposílejte žádné peníze, neodpovídejte na e-maily ani neklikejte na žádné odkazy či přílohy. Stanete-li se obětí vyděračského podvodu, vždy informujte IT oddělení společnosti nebo interní bezpečnostní oddělení.

Nejlepší prevencí je používání silných hesel. Obchod s hesly je také důvod, proč si každý musí čas od času změnit heslo nebo proč je nutné používat další prvky ochrany (vícefaktorové ověřování).

POKUD JE V E-MAILU ZMÍNĚNÉ SPRÁVNÉ HESLO, NEPANIKAŘTE

Uvedení skutečného hesla je jen další technika, jak příjemce znejistit. Útočníci mohou znát vaše heslo, ale nic dalšího nejspíš nemají. Heslo pravděpodobně zakoupili na dark webu nebo mohlo být zcizeno při úniku dat.

NEPODCEŇUJTE ZABEZPEČENÍ PŘI PRÁCI NA DÁLKU

Flexibilní pracoviště a kanceláře jsou skvělé, ale jen pokud jsou dobře zabezpečené a víte, jak s nimi zacházet. Sítě Wi-Fi jsou oblíbeným cílem útoků, takže chcete-li mít jistotu, že připojení a firemní data jsou v bezpečí, měli byste raději používat virtuální privátní síť (VPN), která umožňuje vytvořit bezpečné připojení k firemní síti.

Jak hackeři získají přístup k vašemu počítači a webové kameře?

Když se budete chovat opatrně, nezpůsobí vám vyděračské podvody žádnou škodu. Přesto byste měli vědět, že existuje způsob, jak hackeři mohou získat přístup k vaší webové kameře. K infikování vašeho zařízení softwarem pro vzdálenou plochu často používají malware, jako je například trojský kůň, ale k tomu potřebují vaši pomoc. Někdy stačí, abyste si stáhli neznámý software. I když si myslíte, že jste právě získali požadovaný program, může se v souboru skrývat škodlivý kód. Nevědomky jste právě pomohli hackerům infikovat své zařízení. A nečekejte, že se kontrolka webové kamery rozsvítí, když vás začnou sledovat. To by pak nebyli inkognito, že?

V případě, že máte infikovaný počítač, může hacker nejen pozorovat intimní okamžiky vašeho života, ale také zachytit důvěrná data a dokumenty, a pokud hacknul i mikrofon, nahrávat také vaše rozhovory.

Jak reagovat na vyděračské zprávy

1. Jednejte pomalu a s rozmyslem, vyvarujte se unáhlených akcí.
Počítačoví vyděrači se zaměřují na lidské slabosti a snaží se vámi manipulovat, abyste provedli škodlivou akci. Pokud tedy obdržíte zprávu, která ve vás vyvolá obavy, nespěchejte a zvažte možnost, že informace v e-mailu nejsou pravdivé. V případě pochybností se vždy obraťte na IT oddělení nebo technickou podporu poskytovatele zabezpečení.

2. Vyděračům nic neplaťte.
Vyděračské e-maily jsou obvykle jen podvod. To znamená, že tvrzení pachatelů nemají reálný základ: téměř jistě nemají žádné video s vámi ani s tím, co jste sledovali, nepůsobí u orgánů činných v trestním řízení a ani si neobjednali vaši vraždu.

3. Na e-mail nijak nereagujte.
Na podvodné zprávy neodpovídejte, nestahujte jejich přílohy a neklikejte na vložené odkazy ani na žádný jiný obsah, protože tyto prvky mohou vést k malwaru nebo jiným hrozbám.

4. Zkontrolujte a případně změňte své heslo.
V některých případech zločinci testují uniklé přihlašovací údaje a v případě úspěchu používají hacknutý účet alespoň k šíření svých zpráv. Jestliže tedy útočník uvede některé z vašich aktuálních hesel, okamžitě je změňte a aktivujte vícefaktorové ověřování, abyste zvýšili ochranu.

5. Odešlete e-mail svému IT oddělení.
Pokud vaše společnost žádné IT oddělení nemá, můžete alespoň zkontrolovat počítač a síť pomocí spolehlivého bezpečnostního řešení a ujistit se, že nedošlo k úniku nebo prozrazení žádného z vašich hesel.

6. Zabezpečte webovou kameru.
Abyste předešli možnému zneužití integrované webové kamery, používejte bezpečnostní software nebo alespoň přelepte kameru páskou. Budete tak mít jistotu, že zločinci nemají možnost nahrát video, na kterém sedíte před zařízením.

7. Používejte antispamové řešení.
Spolehlivé bezpečnostní řešení s funkcí proti nevyžádané poště vám pomůže zabránit tomu, aby se ve vaší doručené poště v budoucnu objevovaly vyděračské e-maily.

Další techniky sociálního inženýrství, o kterých byste měli vědět

Scareware je typ malwaru, který se snaží oběti přimět k nákupu a stažení potenciálně nebezpečného softwaru. Je to metoda, která velmi rychle upoutá pozornost lidí a vystraší je. Reklamní okna, která se obtížně zavírají, softwarové společnosti s názvy, o kterých jste nikdy neslyšeli, a neoprávněné skenování počítače na přítomnost virů – to vše jsou typické znaky scarewaru.

Problémem je, že tyto programy obvykle zobrazují seznam desítek nebo stovek falešných virů. Scareware však váš počítač nekontroluje a tyto údajně nalezené výsledky se nezakládají na pravdě. Varování před infekcí vás má pouze zmanipulovat k tomu, abyste si některý z těchto programů skutečně stáhli. Tyto podvody často využívají falešný bezpečnostní software, jako je Advanced Cleaner, SpyWiper nebo System Defender.

Zůstaňte u známých, prověřených a aktuálních softwarových produktů

Budete tak vědět, že nabídka ke stažení bezplatného softwaru může být podvod. Velmi vhodné je také používat blokátory vyskakovacích oken na pracovních zařízeních a filtry adres URL. Používejte nástroje pro zabezpečení webu a bránu firewall a zabraňte tak útočníkům v jejich jednání.

Podvody s technickou podporou úzce souvisejí se scarewarem. Na rozdíl od něj však útočníci předstírají, že jsou součástí zavedené společnosti, jako je Microsoft. Tito podvodníci nespustí automatické skenování počítače. Místo toho vás mohou požádat, abyste otevřeli některé soubory, a pak vám sdělí, že tyto soubory mají problém... který však neexistuje. Podle americké Federální obchodní komise (FTC) nejsou podvody s technickou podporou ničím neobvyklým. V roce 2019 obdržela FTC více než 100 000 hlášení o takových podvodech.

Kontrolní seznam pro správce IT:

5 způsobů jak chránit organizaci před útoky využívajícími sociální inženýrství

1. Pořádejte pravidelná školení o kybernetické bezpečnosti pro všechny zaměstnance, včetně vrcholového managementu a pracovníků IT. Tato školení by měla prezentovat nebo simulovat reálné scénáře. Probírané body musí být použitelné a hlavně aktivně testované mimo školicí místnost.

2. Hledejte slabá hesla, která by mohla útočníkům otevřít dveře do sítě vaší organizace. Chraňte hesla další vrstvou zabezpečení a implementujte vícefaktorové ověřování.

3. Implementujte technická řešení pro boj s podvodnou komunikací, která detekují spamové a phishingové zprávy, umístí je do karantény, neutralizují a odstraní. Některé nebo všechny tyto funkce nabízí bezpečnostní software, včetně řady produktů od společnosti ESET.

4. Vytvořte pro zaměstnance srozumitelné bezpečnostní politiky, které jim pomohou určit, jaké kroky mají podniknout, když se setkají se sociálním inženýrstvím.

5. Chraňte koncová zařízení a sítě vaší organizace pomocí bezpečnostních řešení a nástrojů pro správu, jako je konzole ESET PROTECT, díky nimž získají správci dokonalý přehled a budou moci detekovat a omezovat potenciální hrozby v síti.

Společnost ESET® již více než 30 let vyvíjí špičkový bezpečnostní software pro firemní i domácí uživatele. Vysoce výkonná a snadno použitelná bezpečnostní řešení společnosti ESET, od ochrany koncových a mobilních zařízení přes šifrování až po dvoufaktorovou autentifikaci, umožňují uživatelům a podnikům bez obav naplno využívat potenciál moderních technologií. ESET sleduje a chrání nenápadně a nepřetržitě. Díky aktualizaci ochrany v reálném čase jsou uživatelé v bezpečí a podniky se nemusí obávat výpadků. Další informace najdete na adrese www.eset.cz.