HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
29. – 31. JÚLA 2022

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Máte počítač alebo mobil? Tak sa stávate cieľom útokov

Výhodou záškodníkov je, že ľudia proste odmietajú uveriť, že práve oni by sa dali „nachytať“. FOTO: SHUTTERSTOCK

TÉMA

Globálne aj na Slovensku je phishing stále najrozšírenejšou a najúspešnejšou formou kybernetického útoku. A zároveň témou, kde koluje najviac mýtov.

Vlny podvodných mailov a správ sú čoraz agresívnejšie. Najčastejšími cieľmi phishingu na Slovensku sú subjekty vo verejnej správe a v bankovníctve, respektíve klienti bánk.

Sme svetoví

Phishing bol aj minulý rok najrozšírenejšia forma kybernetického útoku. Spôsoby útočníkov sa príliš nemenia, stále používajú podobné triky, ako sú imitácie poštových a doručovateľských služieb a bánk.

„Za prvý polrok 2022 vzrástol počet phishingových útokov na Slovensku o 31 percent v medziročnom porovnaní,“ konštatuje Ján Doboš, ktorý stojí v prvej línii ochrany kybernetického priestoru štátu. Celkovo bolo evidovaných 176 396 phishingových útokov, čo zahŕňa útoky „odrezané“ bezpečnostnými prvkami, pokusy aj reálne incidenty.

Na toto zabudnite

Pred rokmi sa predpokladalo, že vlny phishingu súvisia so sezónnosťou, čiže s prázdninami, so sviatkami alebo s výpredajmi. Väčšina používateľov ešte stále naivne predpokladá, že nie sú pre útočníkov zaujímaví. Alebo ešte horšie – že sú dosť skúsení a dostatočne bystrí.

„Phishingové útoky niekedy pripomínajú kobercové nálety a ich životnosť je vtedy relatívne krátka, inokedy sú to cielené útoky na konkrétne osoby,“ hovorí Boris Mutina zo spoločnosti Excello, ktorá sa špecializuje aj na emailovú bezpečnosť. A potvrdzuje trend – phishingu bude pribúdať a zároveň sa bude zvyšovať aj jeho sofistikovanosť.

Nočné mory profesionálov

Bežní používatelia vo firmách sa stávajú čoraz atraktívnejšími cieľmi, keďže prostredníctvom nich je možné dostať sa k hodnotným informáciám. Zločinecké gangy a špionážne skupiny majú takto „na dosah“ osobné údaje, dôverné firemné informácie aj obchodné tajomstvá.

„Nápor phishingu na používateľov je enormný,“ opisuje prostredie Marian Klačo, ktorý je vo Volkswagene Slovakia zodpovedný za bezpečnosť IT a prevádzkových technológií.

Zničujúca kreativita

Tie najhoršie ransomvérové incidenty sa aj vo svete prevádzkových technológií – automobilový priemysel nevynímajúc, začali práve phishingovými útokmi. Popri emailoch, ktoré podsúvajú prílohu so škodlivým kódom alebo odkaz na web, sa objavujú aj iné formy útokov.

Pribudli smishing, čiže phishing cez správy, alebo vishing známy ako telefonáty z call centra. „Útočníci hľadajú stále nové možnosti, ako získať od používateľov citlivé informácie a podľa môjho názoru je najagresívnejšou metódou social media phishing,“ dodáva Marian Klačo.

Tí najzraniteľnejší

Bezpečnostní špecialisti identifikujú tri mimoriadne zraniteľné skupiny. Seniori sú vystavení rizikám, ktorým nerozumejú alebo nevedia na ne reagovať. Strach, pochybnosti a neistota spolu s nátlakom útočníkov sú spúšťače nesprávnych reakcií.

Ženy sú často obeťami podvodníkov, ktorí sa vydávajú za zamilovaných lekárov či vojakov zo zahraničia. Tí získavajú ich dôveru a lákajú peniaze pod zámienkou liečby chorého dieťaťa či návratu domov.

Pre deti je phishing neznámy a netušia, prečo by si mali chrániť súkromie. V školách absentuje kvalitné vzdelávanie v kyberbezpečnosti poskytované štátom, čo považuje Boris Mutina za hanbu, ktorá sa nám vypomstí za pár rokov.

(Ne)osvietení používatelia

Skupiny, ktoré majú prístup k prostriedkom ochrany napríklad v práci, ako sú rôzne filtre, školenia či pravidelné testy, sú viac odolné. Tréningy sú čoraz častejšou súčasťou firemného vzdelávania. Na druhej strane tie isté osoby môžu zlyhávať pri súkromnom využívaní emailov, aplikácií alebo na sociálnych sieťach.

Boris Mutina po rokoch analýz phishingových mailov a riešení incidentov však varuje najmä malé firmy a drobných podnikateľov: „Agenda bezpečnosti je tu často okrajová alebo žiadna.“

> Hovorte so známymi o hrozbách phishingu. Vaša skúsenosť môže pomôcť zachrániť niekoho iného.
>
> **Ján Doboš,**
> Národné centrum kybernetickej bezpečnosti SK-CERT

Už ste sa nachytali?

Nie je to prekvapivé. „Za obdobie ostatných dvoch rokov vnímam výrazný nárast počtu phishingových kampaní voči klientom bánk,“ súhlasí Ján Adamovský, riaditeľ bezpečnosti v Slovenskej sporiteľni.

Podvodníci využívajú najrôznejšie komunikačné platformy, ľudí oslovujú cez online bazáre, sociálne siete či volajú z podvrhnutých telefónnych čísel banky alebo polície. Zároveň rastie aj sofistikovanosť a personalizácia týchto útokov.

Neskoro plakať

Podľa kvalifikovaného odhadu Jána Adamovského sa každý rok na Slovensku stanú obeťami phishingu tisícky ľudí. Reálne dôjde k odovzdaniu prihlasovacích údajov do internetbankingu, k odcudzeniu údajov z platobnej karty alebo až k samotnému odcudzeniu peňazí.

Vo firemnom svete sú najčastejšími cieľmi finanční riaditelia a zamestnanci zodpovední za vybavovanie faktúr, ktorých sa podvodníci snažia presvedčiť, aby realizovali podvodný platobný príkaz. Najčastejšie sa vydávajú za vyššie postaveného manažéra z danej firmy alebo dodávateľa, ktorý náhle zmenil účet v banke.

Na čo je phishing dobrý

Od marca zaznamenala zvýšený počet phishingových kampaní cielených na zamestnancov aj Všeobecná zdravotná poisťovňa. „Každý takýto útok vieme využiť na zlepšovanie a aktualizáciu našich spamových filtrov, čím sa snažíme zabezpečiť, aby každá ďalšia kampaň od útočníkov bola menej a menej úspešná,“ reaguje Martin Fischer, manažér oddelenia kybernetickej bezpečnosti.

Najväčší podiel na úspešnosti alebo neúspešnosti cielených kampaní má však samotný používateľ, preto je vzdelávanie v oblasti informačnej bezpečnosti prioritou.

Odborníci sa zhodujú

„Musíme citlivo a cielene vyskladať také formy, druhy, témy a rozsah vzdelávacích aktivít, aby reflektovali cieľové skupiny zamestnancov,“ opisuje stav Peter Dufek, manažér kybernetickej bezpečnosti v sieti Svet Zdravia a ProCare.

Podľa jeho skúseností je najväčším motivátorom, keď je téma phishingu naviazaná so súkromným životom. Kampane a podvody nie sú udalosťami iba v zamestnaní a rady, ako sa chrániť, si chce vypočuť veľa poslucháčov. Ak nadchnete pre spoluprácu ľudí, získate pre budovanie kybernetickej odolnosti maximum.

Hovorte, nehanbite sa

Sociálne inžinierstvo v phishingových kampaniach čoraz viac využíva otvorené zdroje. Útočníci si o svojom cieli zistia čo najviac a správy prispôsobia, aby boli dôveryhodnejšie, a teda úspešné.

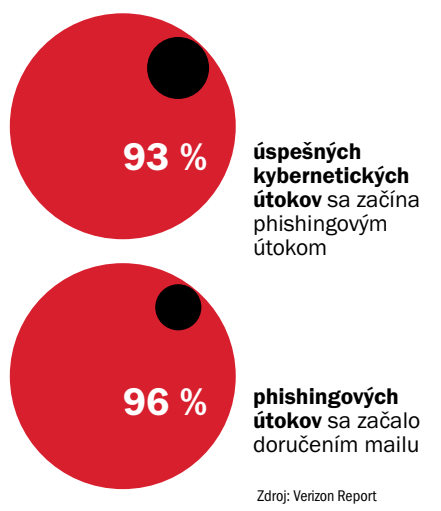
Phishing sa týka každého. Aj tých, čo si myslia že sú proti nemu imúnni. Hoci dokonalé riešenie neexistuje, pomáha neustála ostražitosť a povedomie o téme.

„Hovorte so známymi o hrozbách phishingu a otvorene aj o tom, ak ste na phishing naleteli. Nie je to hanba, vaša skúsenosť a svedectvo môžu pomôcť zachrániť niekoho iného,“ jednoducho uzatvára ťažkú tému Ján Doboš z Národného centra kybernetickej bezpečnosti SK-CERT. Platí to pre používateľov aj pre firmy.

Podnetom na spracovanie témy phishingu sa stal nárast phishingových kampaní a hrozieb, ktoré sa s nimi spájajú. Vzhľadom na mimoriadny záujem o tému sa praktickým radám a ukážkam budeme venovať aj v augustovej prílohe Hospodárskych novín Kybernetická bezpečnosť.

Prečítajte si aj anketu profesionálov

Ktoré používateľské zvyklosti a aplikácie najviac ohrozujú osobnú a firemnú bezpečnosť?



Zdroj: Verizon Report

1 122 579

unikátnych phishingových kampaní **od 1. mája 2021** do **30. apríla 2022**

medziročný nárast **61 percent**

Zdroj: Phishing Landscape 2022

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · eset · Progress · MICRO FOCUS · Qubit · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 29. – 31. JÚLA 2022

Toto je zoznam najhorších zvyklostí

ANKETA

Bezpečnostní profesionáli často opakovanie riešia tie isté pochybenia. Ráno, na obed, večer, v noci. Stále a dokola. Tak sa pýtame, ktoré používateľské zvyklosti najviac ohrozujú osobnú a firemnú bezpečnosť?

Ivan Makatura, generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

V prostredí väčších organizácií je bezpečnosť ohrozená rutinou a vedomým obchádzaním bezpečnostných politík. V súkromí nás ohrozuje ľahkovážnosť, najmä čo sa týka aktualizácií softvéru a klikania na každú sprostosť, čo človeku príde pod ruku.

Henrich Šnajder, manažér IT bezpečnosti
Orange Slovensko

Na dark webe je v ponuke 18 miliárd uniknutých a zverejnených prihlasovacích údajov. Z tohto počtu môžu byť práve tie vaše kľúčom do firemného prostredia. Používanie rovnakých alebo podobných hesiel vo firemnom a súkromnom prostredí je cesta do kyberbezpečnostného pekla.

Ivan Kopáčik, bezpečnostný expert
Gordias

Pohodlnosť a nevzdelanosť. Prehnane pohodlní ľudia majú tendenciu obchádzať bezpečnostné opatrenia. Nevzdelaní ich zase používať nevedia. Zabudnuté „zombie“ aplikácie sú ohrozením bez ohľadu na to, o akú aplikáciu ide. Sú bezpečnostne neudržiavané a môžu byť ľahko zneužité.

Martin Fábry, konzultant pre kyberbezpečnosť kritickej infraštruktúry
Accura

Firemnú bezpečnosti najviac ohrozuje laxný prístup vrcholového manažmentu v otázke kybernetickej ochrany. Častým javom je kontinuálne bombardovanie manažmentu rizikami, či už to robí IT tím, alebo bezpečnostné oddelenie, bohužiaľ, bez akejkoľvek reakcie. V mnohých firmách prevláda syndróm kybernetickej naivity – „my všetko vieme a útočníci si nás nevšímajú“, na čo nedávno doplatili aj mnohé slovenské firmy ransomvérovými útokmi.

Andrej Žucha, generálny riaditeľ
ALISON Slovakia

V kybernetickom priestore nás ohrozujú všetky faktory ako v reálnom svete. Slepá dôvera k správam, v tomto prípade najčastejšie mailovým, slepá dôvera k webovým stránkam, dôveryhodnému hlasu, nástojčivým argumentom a dojemným vyznaniam lásky, ale aj prehnaná dôvera k technologickým značkám a ich komunikácii.

Martin Lohnert, riaditeľ centra kybernetickej bezpečnosti Void SOC
Soitron

Náš tím kybernetických obrancov najviac trápia používatelia, ktorí k bezpečnosti pristupujú ľahkovážne. Tí, ktorí z nedbalosti či pohodlnosti používajú rovnaké heslá v práci aj pri registrovaní sa na pofidérnych webových stránkach, otvárajú podozrivé prílohy a odkazy, nevšímajú si bezpečnostné upozornenia či aktualizácie. Nájdu sa v každej firme. A keďže našou úlohou je pomôcť ich chrániť ešte skôr, ako sa použijú na vlastných chybách, zostáva nám len bojovať ďalej – hrozby včas odhaľovať a správne na ne reagovať.

Tomáš Zaťko CEO, etický hacker
Citadelo

Používateľská zraniteľnosť na manipuláciu podvodníkmi – na phishing a iné formy sociálneho inžinierstva.

Rastislav Janota, riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Ľahostajnosť, prípadne jej kombinácia s lenivosťou. Vlastné peniaze, či už v peňaženke, alebo prístupné internetbankingom, chránime dôsledne. Ale z mne neznámej príčiny nepristupujeme rovnako dôsledne aj k ochrane našich ďalších cenných aktív, počítačov, účtov do programov či rôznych služieb na internete. A neuvedomujeme si, že tak riskujeme oveľa viac ako jednoduchý obsah peňaženky.

Ján Grujbár, generálny riaditeľ
Aliter Technologies

To, čo najviac ohrozuje bezpečnosť, je neznalosť a ľahkovážnosť. Tak ako si chránime seba a svoj reálny majetok, je potrebné si chrániť aj svoju digitálnu identitu a údaje. Zakázal by som otvárať neznáme maily, klikať na podozrivé linky v správach, zapisovať si heslá na papieriky. Naopak, prikázal by som používať multifaktorovú autentifikáciu, mobil a počítač pravidelne aktualizovať a dáta zálohovať.

Martin Oczvirk, riaditeľ odboru informačnej bezpečnosti a certifikácie
Úrad na ochranu osobných údajov

Ohrozuje nás používateľská lenivosť a inštalovanie si aplikácií, ktoré naozaj nepotrebujeme – presne povedané, potreba skúšať nové apky a potom zabudnúť, že sme si ich niekedy nainštalovali. Čo by som zakázal plošne, je vydanie aplikácie bez poriadneho otestovania funkčnosti a bezpečnosti. Nie je nič horšie, ako keď sa robí v zhone, lebo niečo treba rýchlo podsunúť na trh. Pre aplikácie to platí dvojnásobne.

Diana Legdanová, vedúca úseku bezpečnosti
Východoslovenská energetika Holding

Jednou z najhorších zvyklostí, v prípade kritických osôb alebo systémov, až extrémne ohrozujúcou, je písanie hesiel na papieriky. Žiaľ, je to aj dnes stále pretrvávajúci zlozvyk. Za nebezpečné považujem aj mítingové aplikácie, aj napriek tomu, že nám v ostatných rokoch veľmi pomohli. Najmä ich funkcionalitu nahrávania využívanú z pohodlnosti alebo dokonca alibizmu.

Marián Illovský, audítor kybernetickej bezpečnosti
Auditori.it

Najhorší prístup, ako bojovať so zvyklosťami, ktoré ohrozujú bezpečnosť, je niečo zakázať. Lepšia, aj keď náročnejšia cesta je vzdelávanie používateľov a jasná identifikácia rizík spojených s aplikáciami či technológiami. Zákaz by som využil iba v prípade, keď sú aplikácia, alebo technológia považované za nebezpečné relevantnými zdrojmi, vtedy iná možnosť neexistuje.

Július Selecký, senior technický špecialista
ESET

V mojej „bubline“ je používateľské správanie na celkom slušnej úrovni. U zákazníkov sa však stretávam s rôznymi zlými bezpečnostnými návykmi. Často majú neaktualizované programy či OS, využívajú verejné WiFi bez VPN a nevyužívajú dvojfaktorovú autentifikáciu. Občas niektorí nevyužívajú ani kvalitné zabezpečenie na zariadeniach, keďže žijú v domnienke, že napríklad ich MacBook nemôže dostať vírus.

Tomáš Hettych, viceprezident
ISACA

Osobnú bezpečnosť ohrozuje najmä používanie slabých hesiel, zdieľanie osobných údajov na sociálnych sieťach a slabé povedomie o bezpečnosti. Firemná bezpečnosť má najväčší problém s privilegovanými používateľmi, predovšetkým z radov stredného a vyššieho manažmentu. Tento typ používateľa spravidla deklaruje, že nemá čas na vzdelávanie, ale na druhej strane disponuje citlivými a ľahko zneužiteľnými informáciami.

Miloslava Gábrišová, technická riaditeľka
Energotel

Medzi najviac exponované ohrozujúce používateľské zvyklosti radíme náchylnosť na phishingové či vishingové kampane, ktoré sú často okrem kompromitácie osobných či bankových údajov prekurzorom k úspešnému ransomvérovému útoku. V kombinácii s nedostatočným zálohovaním môže byť takýto ransomvérový útok pre organizáciu devastačný s časom obnovy v dňoch až týždňoch.

Michal Gross, manažér IT bezpečnosti
365.bank

Zvyklosti, ale aj nevedomosť. Sú bránou pre manipuláciu používateľov aj únik dát prostredníctvom technológií. Rutinné klikanie pri inštalácii, používanie predvolených hesiel na zariadeniach a nedostatočné nastavenie práv služieb môže viesť k nechcenému publikovaniu osobných informácií na sociálnych sieťach alebo úniku cez nezabezpečené smart zariadenia. Pre firmy sú zdrojom hrozieb neautorizované aplikácie a cloud služby.

Roman Čupka, hlavný konzultant
Progress | Flowmon a CEO Synapsa Networks

Bežným používateľom chýba určitá dávka digitálnej paranoje. Základné pravidlo je – čo by som neurobil vo fyzickom priestore, neurobím ani v tom digitálnom – a opačne. Pokiaľ by sme chceli byť 100-percentne chránení, nepoužívali by sme maily, sociálne siete ani internet. To je však takmer nemožné, preto treba byť zdravo podozrievavý a premýšľať nad tým, aké riziká vyplývajú z nášho konania v digitálnom priestore.

Branislav Magula, vedúci odboru IT OT bezpečnosti
Slovenská elektrizačná prenosová sústava

Medzi zvyklosti výrazne ohrozujúce bezpečnosť by som zaradil zdieľanie informácií dôverného charakteru prostredníctvom sociálnych sietí, neuvážené klikanie na odkazy v mailoch a aplikáciách, používanie slabých hesiel, zanedbávanie pravidelnej aktualizácie operačných systémov a aplikácií a pripájanie sa k verejným WiFi sieťam. A vo všeobecnej rovine – podceňovanie problematiky bezpečnosti všeobecne.

Igor Práznovský, riaditeľ odboru bezpečnosti informačných systémov
Sociálna poisťovňa

Chýbajúce bezpečnostné povedomie. Bežný používateľ chce pohodlne používať svoje tri heslá, pre dvanásť rôznych online obchodov a nemieni heslo Rexo1993 meniť. Nie vždy je obozretný a rozumie, že Apple.com a Ápple.com nie je to isté. Je našou úlohou ho upozorniť, že jeho heslo nie je bezpečné a je potrebné ho zmeniť a zároveň posilňovať povedomie v oblasti kybernetickej bezpečnosti. Rexa môžeme mať doma, ale v online priestore si zapnime dvojfaktor.

Matej Síleš, manažér IT bezpečnosti
UPC BROADBAND SLOVAKIA

Najväčším zlozvykom je používanie ľahko uhádnuteľných hesiel, prípadne ich zapisovanie na viditeľné miesta. Zakázať môžeme všetko, ale tým bude klesať efektivita práce. Bezpečnosť nie je iba o reštrikciách, ale hlavne o bezpečnostnom povedomí užívateľov a uvedomovaní si rizík spojených s prácou s informáciami a informačnými systémami.

Miroslav Chlipala, partner
Advokátska kancelária Bukovinský & Chlipala

Pekná otázka. Áno, súhlasím. Sú to práve stereotypné používateľské zvyklosti, ktoré ohrozujú bezpečnosť. Takí sme! Zvyk je železná košeľa! Máme iba jednu možnosť, ako na to. Naučme sa pýtať sami seba, prečo to tak robím? Naučme sa, že jedinou prípustnou používateľskou zvyklosťou je nemať žiadnu stereotypnú a nekriticky používanú používateľskú zvyklosť.

Miroslav Ilavský, riaditeľ
i-Secure

Zlé bezpečnostné návyky zamestnancov. Upozorňujeme na to roky, stále sa nájdu zamestnanci, ktorí používajú jedno heslo všade, sila hesla je nízka alebo ho majú napísané na papieriku prilepenom na monitore. Nízka odolnosť zamestnancov voči rôznym druhom šíreného malvéru a phishingu. Zakázal by som neautorizované USB zariadenia, sociálne siete a škodlivé weby na pracovisku a použitie súkromných zariadení na prácu.

Ján Golais, poradca bezpečnosti
Slovak Telekom

Narušenie osobnej aj firemnej bezpečnosti má rovnaké základy. Ak to nie je zabezpečené formou vynútenia, tak je to určite pohodlnosť užívateľa. Využívanie jednoduchých hesiel či nedôslednosť, ktorá vedie k zdieľaniu hesiel, podcenenie, ktoré vedie k prihlasovaniu do systémov z cudzích zariadení. Na vrchole pyramídy je tvrdohlavosť tých, čo rozhodujú, ktorá vedie často k zjednodušovaniu procesov.

Vladimír Jančok, vedúci oddelenia informačná bezpečnosť
VÚB

Spoločnou hrozbou pre firemnú aj osobnú bezpečnosť je ešte stále podceňovanie, až nedbanlivosť pri práci s heslami a prihlasovacími údajmi. S tým súvisí aj obozretnosť pri zadávaní prihlasovacích údajov na webové stránky, ktoré si používateľ otvorí cez link v maili alebo esemeske v mobile. Situáciu môže skomplikovať aj zastaraný internetový prehliadač.

Vzhľadom na mimoriadny záujem sa budeme venovať radám a príkladom aj v auguste