Dokonalá ochrana proti phishingu?

RIEŠENIA

Nepoužívajte email, telefón ani sociálne siete. Ostatní môžu phishing eliminovať vhodným návykmi aj technológiami.

Phishingové kampane často využívajú, že na ich šírení sa podieľajú obete. FOTO: SHUTTERSTOCK

Keď vlani viac ako stovka odborníkov na IT bezpečnosť dostala otázku, čo považujú za najaktuálnejšiu hrozbu v kybernetickom priestore, vyše polovica z nich uviedla phishing. Rok predtým pritom phishing označila len necelá tretina respondentov.

Phishing je pre organizácie veľký postrach najmä preto, lebo zvykne stáť na začiatku závažných kybernetických útokov, zameraných napríklad na vydieranie s využitím ransomvéru, alebo na krádeže citlivých dát.

Preto prinášame najčastejšie príklady phishingu a zároveň tipy, ako ich eliminovať.

1. Kobercový nálet e-mailmi

E-mailový phishing je najznámejšia a najrozšírenejšia forma phishingu. Typickým príkladom je rozposielanie hromadných e-mailov, ktoré budia dojem, že pochádzajú od známej, dôveryhodnej značky.

Príjemcu vyzývajú k nejakému úkonu, zvyčajne podmienenému kliknutím na odkaz alebo otvorením priloženého súboru. Cieľom je však dostať do počítača adresáta škodlivý kód.

Na čo dávať pozor a ako sa brániť? Niekedy stačí venovať pozornosť gramatickým chybám a pred reakciou porozmýšľať o relevantnosti e-mailu. Rozkliknutím adresy odosielateľa môžete „preskúmať“ doménu, z ktorej e-mail prišiel.

Zvýšiť ostražitosť treba napríklad aj pri odkazoch v skrátenej podobe, tie sa totiž používajú na oklamanie bezpečnostných e-mailových brán (Secure Email Gateways). Pre vyššiu bezpečnosť je možné aplikovať systém na identifikáciu podvodných domén v kombinácii s okamžitým zablokovaním prístupov na takéto domény.

2. Telefonický phishing

Pri phishingu v angličtine označovanom ako vishing (telefonát) a smishing (SMS) zostávajú ciele útočníkov rovnaké, ale namiesto e-mailu využívajú na oklamanie obetí telefón.

Typickým príkladom je, keď sa podvodníci vydávajú za predstaviteľov dodávateľskej firmy, e-shopu, servisného strediska alebo finančnej inštitúcie a snažia sa vylákať od obete napríklad prihlasovacie údaje alebo detaily platobnej karty.

V tomto prípade si všímajte, či telefonát neprichádza z nezvyčajnej lokality, ale podozrivé by malo byť aj to, ak volajúci príliš naliehavo na okamžité poskytnutie údajov a snaží sa vyvolať dojem časovej tiesne.

Väčšina organizácií navyše využíva niekoľkostupňové overovanie používateľa a nikdy nežiada o poskytnutie kompletných osobných údajov. Pravidlom by malo byť nereagovať na neznáme alebo „skryté“ telefónne čísla a na esemesky nereagovať vôbec.

3. Phishing na sociálnych sieťach

Neprekvapuje, že sociálne médiá sa stali obľúbeným miestom pre phishingové útoky. Podvodníci využívajú na zlákanie obetí cielené reklamy alebo posielajú správy priamo cez chatovacie aplikácie sociálnych médií.

Cieľom nebýva vždy iba snaha nakaziť počítač obete škodlivým kódom, ale aj nalákať ľudí na rôzne rizikové investičné schémy a podobne.

Tu treba zvýšiť ostražitosť napríklad pri notifikáciách s odkazmi, ale aj v prípade neštandardných a podozrivých priamych správ. Najmä ak sa nás odosielateľ snaží presvedčiť, aby sme zdieľali svoju obrazovku, poskytli mu vzdialený prístup do zariadenia či osobné údaje.

Každá sociálna sieť navyše umožňuje bezpečnostné nastavenia profilu a v tomto prípade platí, že „menej znamená viac“.

Základom je v čo najväčšej miere obmedziť svoj profil ako verejný a na komunikáciu využívať iné, šifrované a zabezpečené aplikácie, nie tie na sociálnych sieťach.

4. Cielený phishing

Spear phishing predstavuje sofistikovanejšie sociálne inžinierstvo, keď si útočníci z voľne dostupných zdrojov na internete, výročných správ alebo médií vytypujú a oslovujú vybrané osoby alebo skupiny osôb v organizácii. Oslovia ich, vydávajúc sa za internú osobu alebo napríklad za partnerskú firmu, s konkrétnou požiadavkou.

Príkladom je uskutočnenie finančných transakcií, odcudzenie citlivých a dôverných údajov či infiltrácia s cieľom kompromitácie samotnej organizácie. Vytypovanou obeťou cieleného phishingu môže byť napríklad účtovníčka, administrátor IT, ale aj vrcholový manažment, ktorý nebýva až taký obozretný.

Obranou je zvýšená pozornosť voči nezvyčajným požiadavkám alebo nepravidelným žiadostiam, ktoré prichádzajú napríklad z iných oddelení či partnerských firiem.

Útočníci sa týmto spôsobom tiež usilujú presmerovať obete na podvodné weby, a to zahrnutím odkazov na dokumenty uložené na zdieľaných úložiskách, prípadne získať prihlasovacie údaje žiadosťou o prihlásenie používateľa.

Nápomocné sú technológie obmedzovania prístupov na nebezpečné či podozrivé webové stránky, úložiská alebo nástroje na kontrolu a riadenie prístupov do IT systémov a firemných aplikácií.

Nevyhnutné technológie

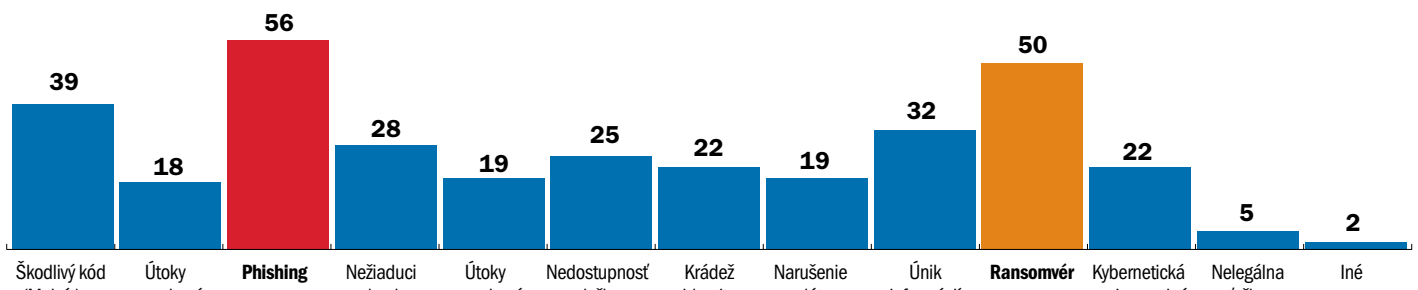
Spoločným menovateľom prevencie pred akýmkoľvek phishingom je byť prirodzene podozrievavý a ostražitý voči e-mailom, správam alebo telefonátom. Stopercentnú ochranu však ani týmto spôsobom nikto nezíska, preto je pre organizácie dôležité aj technologické zabezpečenie.

Vhodným je napríklad nástroj na monitorovaný šifrovaný prenos informácií (Secure Manage File Transfer), ktorý umožňuje bezpečne posielať aj prijímať citlivé dáta voči externým partnerom alebo systémom alebo ich zdieľať v zabezpečenom adresári, kam majú prístup iba oprávnení používatelia. Ak sa eliminuje nekontrolovaná výmena súborov, znižuje sa aj riziko phishingu.

Ak už útočník sociálne inžinierstvo zneužije a akýmkoľvek spôsobom prenikne do siete alebo kompromituje zariadenie, neostáva nič iné ako mať efektívny monitoring v reálnom čase, systém na okamžitú detekciu podozrivej komunikácie a nástroje na automatizovanú odozvu a blokovanie útokov. Teda technológie, ktoré umožnia podozrivé udalosti nielen zachytiť, ale na ne aj včas a správne reagovať.

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

Ktoré kybernetické hrozby považujete pre vašu organizáciu v najbližších 12 mesiacoch za najaktuálnejšie?
(odborníci mali možnosť uviesť viacero hrozieb)



Prieskum: Progress | Flowmon, Synapsa Networks, SecTec a Qubit Security, 2021

SERVIS

Dovolenky sú v plnom prúde a spolu s nimi kybernetické útoky

Ako uvádza štatistika bezpečnostného tímu Check Point Research, obdobie od mája do augusta prináša najviac kyberbezpečnostných ohrození v oblasti cestovného ruchu. Už v júni tohto roka zaznamenali výskumníci v súvislosti s dovolenkami a prázdninami 60-percentný nárast útokov v medziročnom porovnaní.

Pre mnohých nastáva vytúžený oddych od utíšenia pandémie, a preto je možné, že strácajú obozretnosť v súvislosti s kybernetickou bezpečnosťou. Či už ide o podvodné maily, ktoré ponúkajú online check-in, alebo neodolateľné zľavové ponuky na hotely a letenky. Hackeri kradnú identitu známych spoločností a skúšajú, ktorý nedočkavý dovolenkár klikne na phishingový e-mail.

Šírka dostupných zariadení a technológií, ktoré často využívame bez uváženého zabezpečenia, zároveň významne zjednodušuje kybernetické útoky kedykoľvek a kdekoľvek. Hackeri sú si aktuálnych zraniteľností veľmi dobre vedomí a neváhajú ich využiť.

Asi málokto si želá počas dovolenky získať suvenír v podobe „vybieleného účtu“, nabúraného telefónu a straty prihlasovacích údajov do mailov, sociálnych sietí a iných aplikácií.

Nehovoriac už o situácii, ak máte ešte aj nainštalované pracovné aplikácie v súkromnom telefóne, čím pravdepodobne porušujete interné smernice a zároveň aj ohrozujete zamestnávateľa.

Na to, aby ste sa chránili pred kybernetickými hrozbami, nemusíte byť certifikovaný bezpečnostný expert. Tieto základné odporúčania vám pomôžu znížiť pravdepodobnosť, že sa stanete obeťou kybernetického útoku.

Čo odporúčame ako jednoduchú bezpečnostnú prevenciu

- **Vypnutie automatického pripojenia na WiFi aj bluetooth.** Tým sa zariadenie automaticky nepripojí do verejne dostupnej nezabezpečenej siete.
- **Zálohu všetkých súborov.** Ak sa stanete obeťou kybernetického útoku, stále budete mať prístup k svojim dôležitým súborom.
- **Zmenu často používaných hesiel.** Vyhnite sa používaniu jednoduchých fráz, osobných informácií alebo číselných sekvencií 123.
- **Nastavenie platobných limitov na bankových kartách a pohybov na účte.** Bankové aplikácie už poskytujú klientom možnosť prispôsobiť si v aplikácii limity na kartách a notifikácie o pohyboch na bankových účtoch.

Na čo dbať počas dovolenky

- **Nanajvýš opatrné zaobchádzanie s verejnými sieťami.** Ak je to možné, vyhnite sa verejným pripojeniam, ktoré nie sú chránené heslom. Ak nie, vyhnite sa aspoň aplikáciám, kde je nutná identifikácia.
- **Obmedzenie používania verejne dostupných nabíjačiek.** Tieto nabíjacie stanice môžu byť vystavené škodlivému softvéru. Môžu uzamknúť mobil a následne exportovať citlivé informácie, ako sú heslá, fotky, správy a informácie o bankových účtoch.
- **Prednostne využívanie kreditnej karty pri platení.** S kreditnou kartou sa dosiahne pri platení dodatočná bezpečnosť, keďže karta sa neviaže priamo na bankový účet.
- **Nákup iba cez webovú stránku HTTPS.** Posledné písmeno „S“ znamená bezpečnostnú funkciu, ktorá chráni vaše zariadenie pri online nákupe pred vírusmi a malvérom.

Zločinci dovolenku nemajú. Práve naopak. FOTO: SHUTTERSTOCK

Monika Filingrová,
biznis analytička
Aliter Technologies, a. s.