HN
obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
29. SEPTEMBRA – 1. OKTÓBRA 2023

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Sociálni inžinieri už na vás striehnu

EURÓPSKY MESIAC KYBERNETICKEJ BEZPEČNOSTI

Práca útočníkov je poznať slabé stránky obetí na základe analýz dostupných dát. FOTO: DREAMSTIME

TÉMA

Najväčšou chybou firiem je predpokladať, že drastický kyberútok vyžaduje sofistikovaný scenár. Naopak. Tie najhoršie útoky majú simplicitný a takmer elementárny scenár. Využívajú stres, emócie a naivitu.

Nepomohli by ste príbuznému v núdzi, keď vám plače do telefónu? Nepomôžete dvom milým, trochu neohrabaným maliarom s rebríkom dostať sa do firmy? Ak vám urgentne volá šéf IT, rýchlo pošlete prístupové heslá. Alebo prijmete človeka so super profilom na sociálnej sieti. A po čase zistíte, že firemné systémy sú nedostupné alebo na predaj na dark webe. Alebo v sieti ste mali záškodníkov a prišli ste o kopu peňazí. Ste obeťou.

Neodolateľná ponuka

Na firemné večierky sa tešia aj technologickí špecialisti. Takže keď sa na nástenke objavila ponuka s QR kódom „drink podľa výberu gratis“, neodolalo veľa zamestnancov. Správne tušíte, že si stiahli do mobilov škodlivý kód a nemôžeme napísať, kde to bolo a aké bolo skóre.

Alebo – povedzme pravdu. Nechávate si firemný notebook v aute? Požičiavate ho na hranie a online nákupy deťom? V tejto chvíli naozaj netreba veľa fantázie, aby ste vymysleli scenár, ako sa dostať k firemným či súkromným údajom.

Sociálne inžinierstvo

Sociálne inžinierstvo v kontexte informačnej bezpečnosti označuje metódy a techniky zamerané na manipuláciu ľudí. Táto „mäkká“ formu útoku využíva dôverčivosť, strach, nevedomosť alebo iné psychologické faktory namiesto technických slabín v systéme.

Samotná prax sociálneho inžinierstva je stará ako ľudská komunikácia a manipulácia. Jeho popularita prudko stúpla koncom minulého storočia s používaním internetu a elektronických systémov, ktoré spravujú citlivé informácie.

Ide o sekundy

Knihy a príbehy jedného z najznámejších hackerov Kevina Mitnicka ukázali, ako sa využíva sociálne inžinierstvo na obchádzanie technologických zabezpečení. Keďže kyberzločinci dnes už môžu ľahko vyrábať zvukové alebo obrazové záznamy, sociálne inžinierstvo je ešte rafinovanejšie.

„Počítaču stačí vypočuť si len 10 až 20 sekúnd vášho hlasu, aby dokázal vytvoriť zvukový deepfake,“ upozorňuje Ondrej Kubovič zo spoločnosti ESET. Sociálnym inžinierom nahráva aj nedostatok IT zručností a bezpečnostných profesionálov a presun konfliktov do kyberpriestoru.

Objem podvodov rastie

Najjednoduchšia a najúčinnejšia metóda, ako získať citlivé údaje alebo infikovať cieľ malvérom, je phishing. Už sa pominuli časy „nigérijských princov“ a phishing sa dynamicky vyvíja. E-mail dopĺňajú multimédiá, sociálne siete a hlasové hovory v reálnom čase. Podľa slov hovorcu Národného bezpečnostného úradu Petra Habaru už aj na Slovensku sme zaznamenali prvé deepfake telefonáty.

Vizuálne sa útoky a ich formy stále zlepšujú, no stále zaberajú aj overené primitívne „klasiky“. Útočníci sa všeobecne snažia obete dostať do časovej tiesne krátkym ultimátom – často pod hrozbou pokuty. Útoky navyše vyzerajú dôveryhodnejšie, keď sa podvodníci vydávajú za políciu, nejaký úrad alebo firmu.

> Počítaču stačí vypočuť si len 10 – 20 sekúnd vášho hlasu, aby dokázal vytvoriť zvukový deepfake.
>
> **Ondrej Kubovič,** špecialista na digitálnu bezpečnosť

Takto to funguje

Profesionáli z Národného centra kybernetickej bezpečnosti upozorňujú na zaujímavý technologický vývoj. Mechanizmus phishingu sa bráni odhaleniu – samotný phishing sa totiž cielene zobrazí len na základe geolokácie, ďalších faktov a v určitom prehliadači.

Špecificky bankové phishingy robia naozaj hlboký „odtlačok“, čiže mapujú všetky dostupné informácie o používateľovi. Ak chcú totiž zneužiť kartové dáta alebo prihlasovacie údaje do internetbankingu, tak banky tam majú behaviorálnu analýzu. Ak ju chce útočník obísť, musí trafiť typ prehliadača, štát, poskytovateľa internetu a ďalšie parametre. Bankový phishing dokáže zaznamenávať aj spôsob, ako používateľ kliká rozhraním.

Ešte presvedčivejší podvod

Obyčajné phishingové správy cielia na čo najviac používateľov. Útočníci sa spoliehajú na to, že z veľkej skupiny adresátov naletí aspoň určitá časť. V prípade spearphishingu však kyberzločinci cielia na konkrétne organizácie, prípadne na špecifické skupiny.

„Autori spearphishingových správ si obete vopred podrobne zmapujú z informácií dostupných online či pri iných útokoch a na základe získaných poznatkov nastavia komunikáciu,“ vraruje Ondrej Kubovič.

Útočníci si napríklad zistia, kedy a ako firma vypláca finančné bonusy. V tom čase potom rozpošlú všetkým zamestnancom v mene firmy e-mail, že ak chcú odmenu, majú vyplniť osobné či finančné údaje na priloženom odkaze. Treba pokračovať?

Nekončiaci súboj

Útok, obrana, vylepšenie a zas znova. „Pri technológiách, ktorými sa informácie vynášajú, vidíme, že phishingové mechanizmy posúvajú exfiltráciu od e-mailov a súborov skôr k real-time komunikačným platformám,“ hovorí Ján Doboš z NCKB. Niekedy majú útočníci aj vlastné riadiace rozhranie v reálnom čase cez špecifický komunikačný protokol, čo umožňuje útočníkom aktívne hneď overovať a testovať uniknuté údaje. Napriek zvyšovaniu povedomia používatelia stále „naletia“, a to aj mladí trénovaní ľudia, keď sú v strese.

Obeť? Ktokoľvek

„Možno pred rokom by som odpovedal, že na phishing sú mimoriadne zraniteľní ľudia vo vyššom veku alebo tí, ktorým nie sú blízke technológie a moderné bankovníctvo,“ priznáva Tibor Szabo, audítor kyberbezpečnosti z VÚB.

„Poznám však osoby znalé problematiky, ktoré majú v tejto oblasti povedomie na nadpriemernej úrovni a dali sa zmanipulovať k činom, ktoré by nikdy za bežných okolností neurobili. Útočník sa zameral na to, ako vyvolať u obete maximálny stres, reálnu obavu o blízkych či hrozbu straty kontroly nad svojimi financiami.“

Veľa dôvodov na paniku

Proti útokom sociálneho inžinierstva nie je imúnny nikto. Široké spektrum cieľov siaha od jednotlivcov až po veľké korporácie a vládne organizácie. Techniky sú často veľmi presvedčivé a podvody ťažko rozpoznať.

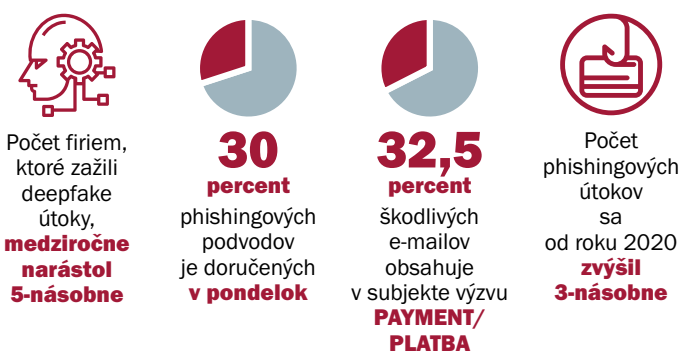
Ľudia sú sociálne bytosti, náchylné na dôveru v iné osoby a organizácie, čo zneužívajú práve zločinci. Útoky vedú či už priamo alebo nepriamo k finančným stratám, nehovoriac o reputačných stratách. Úspešnosť útokov podkopáva dôveru v organizácie alebo systém, čo môže mať v spoločnosti dlhodobé následky.

Neprepadajte zúfalstvu

Technológie sa neustále vyvíjajú, takže je dôležité pravidelne aktualizovať zabezpečovacie riešenia a byť oboznámený s najnovšími typmi hrozieb. To je oblasť, ktorú môžete zveriť profesionálom. Druhú radu však musíte zvládnuť najmä vy, či už ste veľká alebo mikrofirma.

Nezverejňujte o svojej organizácii, respektíve o zamestnancoch nadbytočné informácie, z ktorých by mohli čerpať útočníci pri vytváraní phishingových podvodov na mieru. A rozhodne vzdelávajte zamestnancov o ochrane súkromia na sociálnych sieťach.

Sociálne inžinierstvo v číslach



Zdroje: DARKreading, ENISA

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · auditori.it · CHECK POINT · eset · Progress · SOITRON · SK CERT Národné centrum kybernetickej bezpečnosti

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 29. SEPTEMBRA – 1. OKTÓBRA 2023

Napredujeme alebo sa iba motáme?

ANKETA

Máme tretie výročie špecializovanej prílohy Hospodárskych novín. V ankete sme už oslovili vyše stovky respondentov a dnes sa pýtame tých najlepších: Posunulo sa Slovensko za tri roky v kyberbezpečnosti?

Milan Pikula,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Na vládnej úrovni máme schválenú stratégiu kybernetickej bezpečnosti z roku 2021 a naša legislatíva patrí medzi tie prepracovanejšie v Európe. Téma kybernetickej bezpečnosti už rezonuje nielen u odborníkov, ale aj vo firmách a verejnosti. Problémom je slabá viditeľnosť incidentov. Organizácie nemajú kapacity, takže mnohé incidenty zostanú nepovšimnuté. Riešené incidenty sú navyše často nedostatočne hlásené.

Július Selecký,
senior technický špecialista
ESET

Ak neberiem do úvahy, že aj vďaka nášmu členstvu v EÚ sa neustále sprísňujú povinnosti v oblasti kyberbezpečnosti, tak u zákazníkov badať výraznú zmenu v myslení. Cítiť snahu o vytváranie bezpečného prostredia. Väčšina už došla na to, že nestačí len zapojiť „krabičku“ do siete, ale kontinuálne budovať bezpečnosť tak, ako sa mení svet okolo nás.

Tomáš Zaťko,
etický hacker, CEO
Citadelo

Pozorujeme, že čoraz viac klientov začína chápať, že kyberbezpečnosť je cesta či proces, a nie cieľ. Úspešné firmy si nájdu partnera, ktorý im tento proces dokáže nastaviť, reflektujúc limitované zdroje, a tento nastavený plán potom napĺňajú malými, ale konzistentnými krokmi.

Róbert Mramúch,
manažér kybernetickej bezpečnosti
MH Teplárenský holding

Bez ohľadu na sektor k posunu vpred nás tlačili najmä legislatívne míľniky. Nie je tajomstvom, že mnohé výrobné a priemyselné podniky práve za posledné obdobie dobiehali svoj dlh z minulosti. Ďalšie významné zmeny môže priniesť očakávaná transpozícia smernice NIS2 do našej legislatívy. Verím, že už aj s ohľadom na špecifiká sveta výrobných a riadiacich technológií.

Ivan Kopáčik,
bezpečnostný expert
Gordias

Pred vyše tromi rokmi vstúpili do platnosti kľúčové právne predpisy, ktoré sa začali implementovať do praxe. A priniesli praktické výsledky. Za všetky spomeniem ako príklad audity kybernetickej bezpečnosti u prevádzkovateľov základných služieb. Táto systematická aktivita naštartovala riešenie kyberbezpečnosti aj tam, kde sa ňou predtým zaoberali len minimálne.

Ján Grujbár,
generálny riaditeľ
Aliter Technologies

Dnes je de facto štandardom, že aspekty kyberbezpečnosti predstavujú dôležitý parameter takmer pri všetkých biznisových rozhodnutiach. Samozrejme, to neznamená, že samotná prítomnosť pri rozhodovaní je dostatočná – kybernetická bezpečnosť v podnikoch a organizáciách ešte musí svoje miesto obhájiť a čakajú ju náročné vojny, no konečne jedná so správnymi ľuďmi na správnom mieste.

Roman Čupka,
hlavný konzultant
Progress a CEO Synapsa Networks

Vnímam oveľa širší záujem o kyberbezpečnosť ako celok a posun nastáva najmä z troch dôvodov. Profesionálna komunita sa rozširuje o mladšie ročníky aj vďaka medializácii. Legislatívne a regulačné požiadavky okrem ochrany kyberpriestoru „nakopli“ aj biznis v tejto oblasti. Pribudlo množstvo kyberincidentov, kde sa okrem veľkých firiem stávajú obeťami rôznych podvodov aj bežní používatelia na dennej báze.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies na Slovensku

Posun v kyberbezpečnosti je výsledkom systematickej práce osobností a firiem, ktoré sa tomuto segmentu venujú. Rozhodne však stále zaostávajú zdravotníctvo a školstvo. Slovensko má pred sebou ešte dlhú cestu k perfektnej kyberodolnosti a najhoršie, čo nám hrozí, je zaspať na vavrínoch.

Radoslav Rosiar,
senior bezpečnostný konzultant
konzultanti.it

Prevádzkovatelia základných služieb vrátane tých štátnych začali brať veľmi vážne oblasť kyberbezpečnosti. Ovplyvňujú to hlavne zvýšené počty cielených kybernetických incidentov, ktoré prevádzkovateľov za ostatné obdobia u nás zasiahli, ďalej závery z absolvovaných auditov kybernetickej bezpečnosti, postupná implementácia bezpečnostných opatrení a časté budovanie bezpečnostného povedomia.

Stanislav Smolár,
manažér oddelenia bezpečnosti
Soitron

Vďaka „ostrej“ účinnosti zákona o kyberbezpečnosti badať od roku 2020 výrazný posun dôležitosti tejto témy aj u vrcholového manažmentu takých organizácií, ktoré jej historicky nevenovali primeranú pozornosť. V posledných troch rokoch je tiež badateľne vyšší záujem o kyberbezpečnosť medzi mladými ľuďmi formou ich účasti na odborných konferenciách či záujmom o vzdelávanie v oblasti kyberbezpečnosti.

Jaroslav Oster,
predseda správnej rady
Preventista.sk

V rámci činnosti nášho občianskeho združenia sa počas troch rokoch vďaka dobrovoľníckej práci členov podaril zásadný posun v podpore stredného i základného školstva pri vzdelávaní informačnej a kybernetickej bezpečnosti. Vytvorili a vydali sme štyri učebnice a k nim prináležiace metodiky, ktoré dnes v rade slovenských škôl pomohli naštartovať či skvalitniť výučbu tém bezpečnosti žiakov i pedagógov.

Richard Kiškováč**,**
generálny riaditeľ
Elkan

Posledné tri roky boli poznačené rôznymi turbulenciami a zmenami paradigiem. Slovensko sa v kyberbezpečnosti aj vďaka legislatíve postupne začalo uberať nejakým smerom. Avšak iba veľmi pomalým tempom. Premárnenou príležitosťou je fakt, že sa nepodarilo efektívnejšie využiť všetky dostupné zdroje pre rozvoj a zachytiť dynamiku. Do budúcnosti je preto potrebné zamyslieť sa nad vytvorením takého prostredia a ekosystému, ktorý dokáže preniesť väčšinu dobrých ideí aj do praxe.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Zriadené bolo Kompetenčné centrum, vzniklo nové znalecké odvetvie, plní sa akčný plán, väčšina prevádzkovateľov vykonáva audity kyberbezpečnosti, zlepšuje sa úroveň odolnosti, zvyšuje sa bezpečnostné povedomie, sme prvým členským štátom, ktorý európske znalostné štandardy implementoval v právnom predpise, sme najúspešnejší v počte schválených európskych projektov. To vôbec nie je zlé.

Dominik Procházka,
riaditeľ odboru bezpečnosti
AGEL SK

Za posledné tri roky vnímam posun k lepšiemu. Povinné audity a medializácia udalostí posilňujú povedomie o kybernetickej bezpečnosti aj medzi verejnosťou. Na základe vlastných skúseností sa domnievam, že v oblasti top manažmentu nastal zásadný zlom. Kybernetická bezpečnosť sa už nevníma len ako nepotrebný náklad, ale ako kľúčová položka rozpočtu pre stabilnú prevádzku spoločnosti.

Diana Legdanová,
vedúca úseku bezpečnosti
Vychodoslovenská energetika Holding

Slovensko sa od účinnosti kyberbezpečnostného zákona posunulo, dokonca – skokovo. Kyberpovedomie vo firmách je na neporovnateľnej úrovni. Aj laická verejnosť je vzdelanejšia a vnímavejšia voči kyberhrozbám, často „vďaka“ vlastným či nepriamym zlým skúsenostiam. Ďalším drajverom bol ukrajinsko-ruský konflikt a kybervojna. Najväčší posun však vidím vo významnom rozšírení a v posilnení odbornej komunity, za ktorým stojí niekoľko ľudí – aj tu na tejto platforme. Realitou však je, že vo väčšom meradle je Slovensko stále len na začiatku svojej cyberjourney.

Miroslav Chlipala,
riadiaci partner
BCH Advokáti Chlipala

Pohľadom právnika? Právne rámec pre kyberbezpečnosť podstatným spôsobom narástol. Štyri novely a dve vyhlášky k zákonu a novela dôležitej vyhlášky, Národná stratégia do roku 2025 a akčný plán. Nepodarilo sa však vyriešiť zdvojenú reguláciu pre podsektor Informačných systémov verejnej správy. Očakávame návrh novely zákona, ktorou bude transponovaná Smernica NIS 2!

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Vysoko hodnotím zriadenie Národného koordinačného centra ako súčasť siete pod kuratelou Európskeho kompetenčného centra a rozvoj európskej spolupráce. Negatívom je nízka angažovanosť malých a stredných podnikov v kyberbezpečnosti, čo je prekážkou celkovej národnej bezpečnosti a odolnosti. Slovensko sa posunulo v niektorých kľúčových aspektoch kyberbezpečnosti, ale stále má pred sebou veľa práce na odstránení slabín a využití plného potenciálu moderných technológií a prístupov.

Tomáš Hettych,
viceprezident
ISACA

Za posledné roky urobilo Slovensko v kyberbezpečnosti obrovský posun. Prebehla prvá vlna auditov s očakávanými výsledkami. Nasledovali implementácie bezpečnostných opatrení a akurát prebieha druhé kolo opakovaných auditov. Prvé výsledky ukazujú dramatický posun k lepšiemu nielen v organizačných, ale aj v technických opatreniach. Kyberbezpečnosť už je konečne vážna téma, ktorú majú na programe vedenia organizácií.

Ján Andraško,
SOC manažér
Binary Confidence

Organizácie sa konečne začali zaoberať kyberbezpečnosťou v dôsledku kyberbezpečnostného zákona a opakovaných auditov po dvoch rokoch. Mnohé štátne a pološtátne organizácie, s ktorými sme spolupracovali, zamestnali motivovaných a schopných ľudí, ktorí majú záujem veci riešiť, žiaľ, narážajú na obrovskú a frustrujúcu rezistenciu.

Ján Golais,
poradca bezpečnosti
Slovak Telekom

Stále vidíme nízke kyberbezpečnostné povedomie. Premárnili sme šancu investovať do modernizácie kybernetickej infraštruktúry a najmä vzdelávania v tejto oblasti. Negatívom stále zostáva aj laxný postoj manažmentov prevádzkovateľov základnej služby. Pri GDPR aj pri kybernetickej bezpečnosti nám vzniklo niekoľko „rýchlokvasených“ spoločností kopírujúcich riešenia. Najsmutnejšie je, že nikto voči nim nezasiahne. Naozaj sa to nedá, páni?

Peter Dufek,
manažér kybernetickej bezpečnosti
Procare a Svet zdravia

Po dlhých rokoch stagnácie v chápaní závažnosti kyberhrozieb je posun v tejto oblasti viditeľný. Okrem prijatia dôležitého zákona a vyhlášok treba vyzdvihnúť prínosy najmä Kompetenčného a certifikačného centra, SK-CERT, realizáciu množstva auditov skutkového stavu ochrany u prevádzkovateľov, ako aj neoceniteľnú možnosť čerpania finančných prostriedkov z operačných programov EÚ na kyberbezpečnosť.

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

Z hľadiska agendy osobných údajov sme sa posunuli hlavne v tom, ako dramaticky rastú bezpečnostné incidenty. Štát stále slabo reaguje na aktuálny stav. Dnes dokáže aj relatívne neznalý útočník použiť umelú inteligenciu na vytvorenie útoku. Stále nevidím povinné školenia a tréningy pre zamestnancov štátnej správy.

Marián Trizuliak,
architekt kybernetickej bezpečnosti
Západoslovenská distribučná

Máme legislatívu a dozorné orgány, plejádu podporných a rozvojových aktivít, a to najmä vo vzdelávaní, ale útoky a incidenty sú stále tu. Tlak regulátora na aplikovanie požadovaných opatrení musia priniesť pozitívny efekt v podobe zvýšenia odolnosti voči útokom. O kyberbezpečnosti sa viac hovorí v médiách aj cez túto anketu. Len ľudia sú nepoučiteľní – reagujú na škodlivé e-maily, inštalujú neautorizovaný softvér, aj nelegálny, a poskytujú citlivé údaje komukoľvek.

Roman Varga,
manažér kyberbezpecnosti
Dôvera zdravotná poisťovňa

Nevyužité príležitosti v sektorovej kyberspolupráci v zdravotníctve sú mementom pre ďalšie obdobie. Čo sa musí stať, aby sme si uvedomili, že chránime to najcennejšie? Národná stratégia kyberbezpečnosti pritom jasne definuje cieľový stav ako „vybudovanie dostatočného odborného personálneho základu v tejto oblasti“. Zatiaľ márne. Stále hľadáme ihlu v kope sena a tvárime sa, že je to v poriadku.

Nasadíme do boja technológie

Ochrana a obrana sú rovnako ako kybernetický zločin založené na technologických trendoch. FOTO: DREAMSTIME

RIEŠENIA

V prípade phishingu platí čoraz viac, že spoliehať sa iba na bežnú ochranu ako antivírus nie je ten najlepší nápad.

Na to, aby sme chápali, ako sa brániť, musíme porozumieť, ako sa k nám phishing dostáva.

Prvotný je emailový kontakt a ten obvykle obsahuje link na webovú stránku. Druhým, následným vektorom je webová stránka, ktorá sa tvári dôveryhodne, aby ste citlivé údaje odovzdali dobrovoľne.

Bežný používateľ

Väčšina populácie je veľmi zraniteľná týmito útokmi aj preto, že nemá obvykle dostatočné vlastné prostriedky na ochranu. Pre bežného používateľa je preto ultimatívnou ochranou predovšetkým kvalitná softvérová ochrana koncovej stanice, ľudovo povedané antivirák. Moderné softvérové prostriedky ponúkajú aj ochranu, akými sú plugin do prehliadača na izoláciu prevádzky či adaptívne riešenia na báze strojového učenia pre kategorizáciu webovej prevádzky a správania používateľa a jeho počítača.

Ochrana proti phishingu môže byť aj formou predplatenej služby ako proxy alebo vlastného klienta v prehliadači. Prehliadače chrome a edge už dnes ponúkajú základnú ochranu proti phishingu. Vzhľadom na to, že sú založené na signatúrach a sú globálneho charakteru, majú malú účinnosť proti aktívnym rýchlym kampaniam, lokálnym kampaniam alebo cieleným útokom.

Súčasné parametre

Detekcia phishingu sa uskutočňuje pomocou modulu, ktorý na webovej stránke kontroluje, či nevyzerá podobne ako nejaká iná, či neobsahuje jazykové prešmyčky, či má správny certifikát a aké dáta vyžaduje. Samotné bezpečnostné riešenie používa na modelovanie prvky umelej inteligencie, aby dokázala spoznať aj také pokusy o phishing, ktoré nikto zatiaľ nevidel alebo nepoužil. Je to až neuveriteľné, ale stále treba pripomínať, že používateľ by mal chrániť aj svoj mobilný telefón. Aj tu by mal vyžadovať rovnaké technológie ako na pracovnej stanici a niektoré aj navyše – ochranu proti smishingu, proti neautorizovaným WiFi sieťam alebo neautorizovanými prístupovými bodmi a proti pokusom o útok v sieti typu Man-in-the-Middle.

> Používame umelú inteligenciu, aby sme dokázali spoznať pokusy o phishing, ktoré nikto zatiaľ nevidel, alebo nepoužil.
>
> **Tomáš Vobruba**
> Check Point Software Technologies

Korporátny používateľ

Zdanlivá výhoda je, že zamestnanci sa okrem bežnej edukácie nemusia o nič aktívne starať. Alebo predsa? Aj tu platí, že používateľ by mal byť v strehu pri firemnom e-maile. Aj tam môže smerovať pokus o útok. Preto okrem ochrany pracovných staníc alebo dostupných verejných služieb môžeme použiť aj ochranu pre poštové služby. Väčšina používateľov O365 alebo M365 predpokladá, že ochrana proti phishingu je tam zaistená. Prax ukazuje, že nie je to tak úplne pravda. Preto špecializované riešenia na ochranu proti zero-day hrozbám dokážu pomocou umelej inteligencie rozpoznávať aj tie najšpecifickejšie pokusy o phishing.

Používatelia v menšine

Ak nie ste M365 alebo O365 pozitívni, používajte na ochranu perimetrický firewall. Urobí presne to isté ako kombinácia ochrany pracovnej stanice a ochrany poštovej schránky. Len to musí urobiť na ceste ešte predtým, než to dorazí k používateľovi. K tomu je nutné vykonávať aj takzvanú http inšpekciu, ktorá je na Slovensku ešte stále veľmi málo nasadená v praxi. Čo je veľká škoda.

AI opäť

Zaujímavou kapitolou aktuálneho smerovania vývoja je detekcia AI generovaného obsahu, opäť pomocou AI a jeho rozpoznanie v porovnaní s bežne písaným textom. Súčasťou obrany na emailovom perimetri sú napríklad technológie, ktoré proaktívne prepisujú url linky tak, aby boli kontrolované na chybovosť, ak na ne niekto klikne. Patrí sem aj vyhodnocovanie reputácie zasielaných emailov, spamov, phishingov z domén, ktoré by mali byť partnerské, a kontrola obsahu príloh, keďže aj tie môžu obsahovať skrytý phishingový útok. Vstupnú bránu chránia technológie, ktoré využívajú filtrovanie url adries na základe kategórií a signatúr či reputačnú databázu cloudových služieb poskytovateľov antimalvérových a antiphishingových riešení.

O krok vpred

Ak včas zabránite zverejneniu uniknutých emailových adries a firemných hesiel do internetu, výrazne znižujete riziko útoku. Skúste teda pouvažovať nad tým, že do siete na perimeter integrujete technológie, ktoré na základe porovnávania hashov a domén zabránia, aby sa zadávali firemné citlivé údaje na verejné internetové stránky, akými sú napríklad e-shopy. Na záver by som rád zopakoval, že účinná ochrana proti phishingu je viacvrstvová. Mala by zahŕňať pracovné stanice, ktoré sú často mobilné, aj vstupné brány, poštové servery a mobilné telefóny, na ktoré zabúdame najviac.

PORADŇA

Načo nám je phishingový tréning pre zamestnancov?

Pozrime sa spolu, prečo práve phishingové tréningy a zvyšovanie povedomia v tejto oblasti predstavujú neoddeliteľnú súčasť bezpečnostných opatrení.

Politika informačnej bezpečnosti, respektíve jednotlivé nastavenia v organizácii by mali do značnej miery tkvieť v technických opatreniach. Ak sú tieto opatrenia navyše zosúladené aj s biznis požiadavkami, máme správne predpoklady na správne definovanú bezpečnostnú politiku. Navyše – budeme ju môcť dlhodobo udržiavať a rozvíjať.

Hoci sa na tomto tvrdení zhodnú bezpečnostní experti, nemôžeme povedať, že sme pokryli všetky oblasti a možnosti zabezpečenia. Tak poďme k tomu, prečo investovať čas a rozpočty do phishingových tréningov.

Hlavným argumentom, ktorý zdôrazňuje nutnosť samotného tréningu, je fakt, že phishing, ktorý prejde až ku koncovému používateľovi, spĺňa všetky technické opatrenia kladené na zabezpečenie e-mailovej komunikácie.

V podstate je to niečo ako list v obálke, ktorá má všetky potrebné náležitosti, aby ju pošta kvalifikovane prebrala a doručila – je tu adresát aj uhradená známka.

Druhým argumentom je, že phishingové e-maily nevyužívajú zraniteľnosti technických prvkov, ale zraniteľnosť koncového používateľa. Vytvárajú pocit urgentnosti a využívajú iné techniky psychologického nátlaku.

V tomto prípade sa teda rozprávame, že podstatná časť phishingového útoku tkvie v tom, ako je samotný „list v legitímnej obálke“ napísaný.

Takže si predstavte, že vyberáte ten list z legitímnej obálky, čiže používateľ klikne na link. Aj pri dodržaní prísnych technických opatrení môže takto používateľ kompromitovať systémy. Aj to aj napriek tomu, že princíp minimálnych oprávnení bol správne implementovaný, pretože používateľ konal v rámci svojich definovaných oprávnení.

Potvrdzujú to aj štatistiky. Ľudský faktor je prítomný v 82 percentách všetkých bezpečnostných incidentov. Adresáti si otvoria až 70 percent phishingových e-mailov. Opomínanie phishingového tréningu, respektíve jeho bagatelizovanie by preto mohlo pripraviť veľmi nebezpečný kokteil.

Niektoré štúdie idú ešte ďalej a zdôrazňujú, že najdôležitejšie, čo vieme v oblasti kybernetickej bezpečnosti podniknúť pre zvýšenie jej úrovne, je zabezpečiť kultúru a povedomie v tejto oblasti.

Rozhodne nie je vhodné urobiť plošný tréning – poslať rovnaký e-mail na všetkých a sledovať, koľko ľudí na to klikne. Aj tu by sme mali zohľadniť rôzne úrovne. Skladníci, operátori, účtovníčky, marketéri, personalisti, ítečkári či riaditelia zvládajú rozdielne témy a kompetencie.

V prvotnom delení treba zohľadniť aspoň tri úrovne, cez úplne zjavný phishing až po spearphishing kampane, aby sme vedeli, komu treba aký tréning ušiť na mieru. Samozrejme, je nutné si tieto kampane aj správne vyhodnocovať, a to cez rôzne metriky. Môžeme hodnotiť, koľko e-mailov bolo otvorených, koľko používateľov kliklo na link alebo koľko bolo zadaných bezpečnostných incidentov a cez aké kanály.

Správne dizajnovaný phishingový tréning, ktorý zohľadňuje individuálne potreby organizácie, patrí medzi neoddeliteľnú súčasť komplexnej ochrany organizácií.

Navyše, nové trendy s využitím umelej inteligencie na jednej strane zvyšujú účinnosť detekčných mechanizmov, no na druhej strane aj zvyšujú efektivitu útočníkov. Kto bude v tejto preťahovačke úspešnejší, uvidíme.

Súhrn? Synergia uvedených faktorov vytvára čoraz silnejší tlak na zvyšovanie povedomia o kybernetickej bezpečnosti. A keďže e-mail je jeden z hlavných vektorov útokov, tým sa zvyšuje aj nutnosť povedomia o praktikách sociálneho inžinierstva.

Michal Srnec, CISO
Aliter Technologies

SCENÁR

Piliere útoku

Techniky sociálneho inžinierstva sa spoliehajú na psychológiu a používajú rôzne taktiky a scenáre.

Pred samotným útokom si útočník zistí informácie potrebné o obeti alebo o organizácii z verejne dostupných zdrojov. Na základe informácií nadviaže útočník s obeťou kontakt, vybuduje si u nej dôveru a zmanipuluje ju. Na konci je zvyčajne odovzdanie citlivých údajov či finančná transakcia.

Pretexting:
Vytvorenie fiktívnej identity alebo presvedčivého scenára s cieľom získania dôvernej informácie.

Predstieranie:
Útočník sa predstaví ako dôveryhodná osoba alebo inštitúcia, aby získal dôveru obete.

Dôvera:
Budovanie dôverného vzťahu s obeťou cez sériu interakcií alebo zdieľaných skúseností, ktoré pôsobia autenticky.

Zvedavosť:
Poslanie infikovaného súboru s lákavým názvom, ktorý obete otvoria.

Strach alebo naliehavosť:
Útočník vytvorí falošný pocit, aby prinútil obeť k okamžitej akcii.

Zneužitie autority:
Fejk osoby s autoritou, napríklad vedúceho pracovníka alebo technickej podpory.

Niečo za niečo:
Útočník ponúkne niečo hodnotné výmenou za informácie alebo prístup.

Sociálny dôkaz:
Príklady alebo odporúčania od iných osôb, ktorým obeť dôveruje, aby útočník legitimoval žiadosť alebo akciu.

Technické šarlatánstvo:
Použitie technických alebo odborných termínov na vytvorenie zdania autority alebo na zamlčanie pravdy.

Záplava informácií:
Množstvo informácií, výhovoriek alebo zdôvodnení, aby útočník zahltil obeť a znejasnil situáciu.

Tieto piliere môžu byť kombinované alebo upravené podľa konkrétnej situácie alebo cieľa. Hlavnou obranou proti sociálnemu inžinierstvu je vzdelanie a povedomie o týchto technikách a príznakoch.
Obrana zahŕňa školenia a osvetu zameranú na zvyšovanie povedomia používateľov o rizikách a typoch sociálneho inžinierstva. Kľúčový je však výcvik v identifikácii podozrivých požiadaviek a komunikácií.

ESET Príručka o technikách sociálneho inžinierstva, CSIRT.SK, Wikipedia