PHISHING

Metodika na ochranu pred phishingom a inými e-mailovými hrozbami

Dátum: 10. december 2013

CSIRT.SK
www.csirt.gov.sk

Phishing a iné e-mailové hrozby

Účel dokumentu

Tento dokument je koncipovaný ako stručný návod pre používateľov elektronickej pošty. Cieľom dokumentu je oboznámiť používateľov s hrozbami, ktoré prináša každodenná práca s elektronickou poštou (e-mail), naučiť ich ako majú pristupovať k e-mailovým správam a v neposlednej rade tiež znížiť riziko stania sa obeťami škodlivých aktivít šíriacich sa prostredníctvom e-mailovej pošty.

Čo je Phishing

Phishing je podvodný spôsob, ktorým sa útočník usiluje o získanie osobných údajov ako sú rodné číslo, číslo občianskeho, vodičského preukazu alebo PIN kódu, ale v neposlednej rade aj prihlasovacích údajov do rôznych informačných systémov.

Phishing je formou sociálneho inžinierstva, kde sa útočník snaží oklamať príjemcu za účelom získania jeho súkromných informácií najčastejšie pomocou zaslania e-mailu, ktorý vyzerá ako e-mail z dôveryhodného zdroja.

Základné tipy ako rozpoznať phishingový e-mail

Ako obozretne postupovať pri prijatí e-mailovej správy, aby sa príjemca nestal obeťou:

1. **Krok: Legitimita samotného e-mailu**
    - Kontrola skutočného odosielateľa v detaile e-mailu

    E-mailový klient môže zobraziť meno odosielateľa ako napr. riaditeľ, prípadne s plným názvom riaditel@názov_vašej_organizácie.sk, ale v detaile samotného e-mailu bude uvedené skutočné meno odosielateľa, napr. banditos@companeros.com. Väčšina príjemcov si síce kontroluje meno odosielateľa, ale iba na základe informácií e-mailového klienta.

2. **Krok: Príloha e-mailu**
    - Nikdy neotvárať prílohu s príponou .exe, .src, .com alebo .bat.
    - Pri prílohách s príponou .doc(x), .xls(x), .zip a .pdf je nutné zvýšiť opatrnosť.
    - Taktiež je nutné zvýšiť obozretnosť ak má príloha dlhý názov.
    - Príloha každého e-mailu môže obsahovať škodlivý kód.

    E-mailová príloha je často zneužívaná útočníkom. Zväčša si používatelia dajú pozor na prílohy spomenuté v prvom bode, nakoľko je už v im známe, že po otvorení súborov s príponou .exe, .com alebo .bat sa vykoná ich obsah. Čo znamená, že sa spustí ich kód s právami používateľa, ktorý ich otvoril. Najnebezpečnejšou kombináciou je, ak takúto prílohu otvorí používateľ s administrátorskými právami. Oveľa častejšie sú však zneužívané dokumenty vytvorené v kancelárskom balíku MS Office, nakoľko je pravdepodobné, že potenciálna obeť s nimi prichádza denne do styku. Takéto prílohy môžu obsahovať škodlivý kód, ktorý využíva zraniteľnosť samotnej aplikácie, v ktorej je prezeraný. Následne je možné prostredníctvom takto infikovanej aplikácie nasadiť do operačného systému ďalší škodlivý kód ako je trójsky kôň, backdoor alebo keylogger a prípadne aj iný. Najčastejšie sú takto zneužívané aplikácie spoločností Adobe a Microsoft.

Existujú online služby ako napr. virustotal.com, kde môže používateľ prostredníctvom vloženia podozrivého súboru overiť, či tento súbor obsahuje škodlivý kód. Takéto služby porovnávajú odtlačky analyzovaných súborov s dostupnými databázami antivírových spoločností. V prípade nájdenia zhody je vhodné považovať predmetný skúmaný súbor za potenciálne škodlivý a je potrebné ho zaslať na analýzu antivírovej spoločnosti, ktorej antivírusový balík/program používate. Ale ani tieto služby nezaručujú 100% identifikáciu, nakoľko stále vznikajú nové formy škodlivého kódu s cieľom vyhnúť sa takejto detekcii.

3. **Krok: Samotná forma e-mailu môže vzbudzovať nedôveru a tým by mala u Vás zvýšiť ostražitosť**

Čo je vhodné si všímať:

- Počet prijímateľov
  - Väčšina legitímnych e-mailov je adresovaných priamo jednotlivcovi, prípadne úzkej vybranej skupine.
  - V prípade uvedenia „undisclosed recipients“ je nutné zvýšiť pozornosť.

Príklad z praxe: Príde Vám e-mail, v ktorom ste informovaný, že ste sa stali výhercom 1 mld. dolárov, ale je potrebné uhradiť poplatok vo výške 50 dolárov. V tele e-mailu následne nájdete formulár požadujúci Vaše meno, priezvisko a údaje o Vašej bankomatovej karte, ktorou chcete požadovaný poplatok uhradiť. Veľakrát je pripojený aj text upozorňujúci Vás, že vyplnenie nepravdivých údajov je trestné. Je veľmi nepravdepodobné, že ste vyhrali 1 mld. dolárov spolu s ďalšími skrytými osobami, ktoré sú taktiež adresátmi tohto e-mailu.

- Podpis odosielateľa
  - Každý legitímny e-mail by mal spĺňať náležitostí platné v písomnom styku, napr. informácie o samotnom odosielateľovi – meno a priezvisko.

Rovnaká situácia ako v predchádzajúcom bode, ale teraz ste adresátom iba Vy. Ak v závere e-mail neobsahuje podpis odosielateľa, napr. lotériovú spoločnosť a jej adresu, prípadne jej právne zastúpenie a adresu, tak s veľmi veľkou pravdepodobnosťou ide o podvod, ktorého obeťou sa môžete stať vyplnením požadovaných údajov.

- Čistý text a absencia loga
  - Väčšina legitímnych e-mailov je vo forme HTML, prípadne sa jedná o mix textu a obrázkov.

Tento bod sa týka hlavne firemných, úradných a služobných e-mailov. Ide hlavne o prípady zneužitia dobrého mena organizácií. V praxi sa vyskytli prípady rozposielania upravených legitímne vyzerajúcich e-mailov, ktoré boli identifikované ako podozrivé až na základe chýbajúceho loga organizácie, ktorej dobré meno zneužívali.

- Telo e-mailu je vo forme obrázku
  - Jedná sa o často používanú techniku spamerov.

Spam je označenie pre nevyžiadanú poštu. Bezpečnostné sieťové prvky (zariadenia) môžu obsahovať tzv. spamové filtre, ktoré sa snažia zachytiť spam a odfiltrovať ho. Touto technikou, je možné takéto zariadenie obísť. Preto existujú zdieľané databázy odosielateľov

spamu, resp. ich e-mailových účtov, na základe ktorých sú potom všetky e-mailové správy z takéhoto e-mailového účtu vyhodnotené ako spam a následne odfiltrované.

4. **Krok: Korektnosť gramatiky a pravopisu**

   - Kontrola textu na správne používanie gramatických zvratov, skloňovania a pravopisu.

   Väčšina zaznamenaných phishingových e-mailov bola strojovo preložená z originálnych cudzojazyčných verzií použitých na vyvíjanie škodlivej aktivity v zahraničí.

   Databázu zaznamenaných phishingových e-mailov je možné nájsť na adrese http://www.millersmiles.co.uk/ .

5. **Krok: Textácia e-mailu**

   - E-mail obsahujúci formulácie tvaru „urgentné“, „kliknite sem/tu“ („clicking here“) , prípadne „je potrebné sa prihlásiť na svoj účet“ („you must click into your account now“) s prepojením na URL odkaz je vhodné považovať za nedôveryhodné.

   - „Je to až príliš dobré, než aby to bola pravda“ platí hlavne v prípade reklamného spam-u (nevyžiadanej pošty).

   Útočník sa snaží zvolenou textáciou škodlivých e-mailov prinútiť príjemcu, aby naň reagoval. Využíva sa pri tom snaha o vyvolanie časového stresu u samotného používateľa, ktorý sa snaží predmetnú požiadavku čo najskôr spracovať. Dôsledkom časového tlaku je unáhlene konanie. Väčšinou sa používateľ ani dlho nezamýšľa nad vykonávanou akciou, pokiaľ požiadavka na jej vykonanie príde od nadriadenej osoby, organizácie alebo známeho.

6. **Krok: E-mail obsahujúci URL odkaz**

   - Základné pravidlo znie: Neotvárať URL odkaz priamo z e-mailu, nakoľko skutočná URL adresa môže byť maskovaná.

   - Pokiaľ by to umožňoval e-mailový klient, je vhodné najskôr skopírovať priamo cieľovú URL adresu do nového okna prehliadača ručne (pomocou voľby „kopírovať adresu odkazu“ / „copy link location“).

   - Ak e-mailový klient neumožňuje skopírovať cieľovú adresu samotného odkazu, tak je potrebné nastaviť kurzor myši nad samotný odkaz a v stavovom riadku (spodná lišta e-mailového klienta) sa zobrazí cieľová adresa odkazu.

   - Porovnanie textu URL odkazu v tele e-mailu a skutočnej adresy v prehliadači môže odhaliť snahu a presmerovanie na inú adresu než tú, ktorá je uvedená v texte e-mailovej správy.

   URL odkazy slúžia na prepojenie s „dokumentom“ umiesteným zväčša vo verejnej sieti Internet, ale aj v internej sieti Intranet, alebo priamo ako odkaz na webovú stránku (Internet aj Intranet).

   V prípade „dokumentu“ (spustiteľný súbor, dokument kancelárskeho balíka, ...) je situácia rovnaká ako v prípade prílohy e-mailu.

   V prípade prepojenia na živú webovú stránku existujú ďalšie riziká. Už samotným navštívením webovej stránky, na ktorej môže byť umiestnený škodlivý kód, môže dôjsť k infikovaniu prehliadača a následne celej pracovnej stanice.

Infikovanie prebieha najčastejšie využitím napr. „zero-day“ zraniteľností, ale prípadne aj prostredníctvom neaktuálnej verzie samotného prehliadača, keď sú zneužívané objavené chyby, ktoré sú v novšej verzií už opravené.

Priebeh infekcie môže mať nasledovný scenár:
Prijímateľ e-mailu v dobrej viere klikne na odkaz v tele e-mailu. E-mailový klient alebo webový prehliadač odošle požiadavku na príslušný webový server. Webový server odpovie na požiadavku budúcej obete a zašle mu požadovanú webovú stránku, ktorá bude obsahovať útočníkom vložený škodlivý kód. Po prijatí dát od webového servera sa prehliadač na strane obeti pokúsi tieto dáta interpretovať (vykresliť webovú stránku). Vložený škodlivý kód ale spôsobí chybu v spracovávaní dát, napr. „buffer overflow“, ktorej následkom bude vykonanie útočníkových príkazov, v dôsledku ktorých bude pracovná stanica kompromitovaná a pravdepodobne sa stane aj šíriteľom ďalšej infekcie v sieti.

Aktuálne je pomocou „zlých odkazov“ šírený napríklad ransomware, ktorý zablokuje pracovnú stanicu a požaduje po používateľovi zaplatenie určitej sumy. Najnovšia verzia dokonca šifruje nielen partície pracovnej stanice, ale aj zdieľané disky. V prípade preniknutia tohto škodlivého kódu do internej siete organizácie, môže nastať úplný kolaps organizácie, nakoľko sa zašifrovaním zneprístupnia dátové úložiská.

Napríklad aj chybové stránky zobrazované prehliadačom môžu obsahovať škodlivý kód. Dokonca aj stránka, ktorá Vás upozorňuje na skutočnosť, že nemáte dostatočné oprávnenia a teda máte zamietnutý prístup na požadovanú stránku, môže prostredníctvom prehliadača vykonávať škodlivú aktivitu.

Pod škodlivou aktivitou sa môže rozumieť inštalácia backdooru, prípadne iného malwaru. Často netreba ani zo strany útočníka získať prístup priamo k pracovnej stanici, úplne postačuje inštalácia škodlivého kódu (malware), ktorý z pracovnej stanice urobí účastníka siete botnet, ktorý môže ďalej fungovať ako šíriteľ spamu, DDoS útočník, scanner, bruteforce útočník a podobne. Medzi aktuálne hrozby (označované aj ako trójske kone) z oblasti botnetu patria Zeus, Citadel a Push_do_C.

- Známu URL adresu je ideálne zadávať do nového okna prehliadača ručne.

Zníži sa riziko presmerovania pomocou podvrhnutého odkazu.

- Ak odkaz obsahuje znak „@“, resp. „%40“, tak odkaz neotvárajte.

Odkaz https://www.woodgrovebank.com@nl.tv/secure_verification.aspx smeruje na https://nl.tv/secure_verification.aspx, nakoľko prehliadače ignorujú všetko pred znakom „@“, resp. „%40“.

- Ako kontrolná aktivita sa odporúča vykonávanie kontroly hodnovernosti odkazu pomocou reputačnej databázy napr. pomocou služby na stránke *virustotal.com* alebo aspoň vytvorenie nadhľadu webovej stránky pomocou služby *thumbalizr.com*.

Žiaľ, 100% ochrana neexistuje pokiaľ má byť zachovaná funkčnosť, ale stále je možné znižovať samotné riziko pomocou voľne dostupných nástrojov a služieb.

7. Krok: Požiadavka na osobné informácie

- Forma výzvy:
  - Navštívenie webovej stránky prostredníctvom odkazu uvedenom v tele e-mailu a následného vyplnenie požadovaných údajov.

- Stiahnutie prílohy e-mailu, ktorá môže obsahovať škodlivý kód, za účelom jej vyplnenia (vytlačenie, vyplnenie a naskenovanie) a následného odpovedanie na e-mail.

Vzhľadom na vyššie uvedené, nikdy neposkytujte osobné údaje po výzve prostredníctvom e-mailu.

Všeobecné zásady:

- Nepredpokladajte, že e-maily od priateľov alebo kolegov obsahujú bezpečné odkazy alebo prílohu.
- Neodpovedajte na e-mail, ktorý požaduje osobné, finančné alebo prihlasovacie informácie.
- Navštevujte Vám známe webové informačné systémy a webové stránky písaním URL adresy priamo do prehliadača.
- Prihlasujte sa pravidelne na svoje kontá v informačných systémoch za účelom kontroly ich stavu.
- Kontrolujte zabezpečenie spojenia v prípade zadávania prihlasovacích údajov. URL adresa by mala začínať **„https“** a nemala by obsahovať žiadnu IP adresu.
- Žiadny správca systému od Vás nikdy nebude chcieť Vaše heslo.

Všeobecné tipy:

- Ak nie ste klientom spoločnosti, ktorá sa tvári ako odosielateľ e-mailu, tak ho ignorujte.
- Ak aj ste klientom spoločnosti, ktorá sa tvári ako odosielateľ e-mailu, tak nikdy neodpovedajte priamo na e-mailovú výzvu spoločnosti pokiaľ sa jedná o Vaše osobné alebo finančné informácie.
- Nikdy neotvárajte odkaz na webovú stránku priamo v tele e-mailu, ale skopírujte ho ručne.
- Ak sa na legitímnej webovej stránke, ktorú ste už v minulosti navštívili, objaví výzva na zadanie hesla, tak najskôr vložte neplatné prihlasovacie meno a neplatné heslo. Podvrhnutá webová stránka bude neplatné prihlasovacie meno a heslo akceptovať, zatiaľ čo legitímna nie.
- Ak ste aj nevedomky poskytli osobné alebo finančné údaje, tak neodkladne informujte príslušnú organizáciu.
- Snažte sa sledovať triky, ktoré využívajú phishingové e-maily, iba tak môžete hneď spozorovať podvodné e-maily.

Technické tipy:

Nasledujúce tipy poskytujú technické možnosti ako znížiť riziko ohrozenia používateľa a celej organizácie v dôsledku phishingového útoku.

- Obmedzenie práv samotných používateľských účtov na pracovných staniciach.
- Poučenie používateľov ohľadne spamu a phishingových e-mailov.
- Čiastočné obmedzenie prístupu používateľov do siete Internet.
- Blokovanie škodlivých domén priamo na proxy serveri.
- Používanie prehliadačov využívajúcich reputačné databázy v rámci kontroly prístupu na webové stránky obsahujúce škodlivý kód.
- Sprísnenie anti-spamových pravidiel.
- Zavedenie e-mailových šablón v rámci organizácie.
- Dôsledná a pravidelná aktualizácia operačného systému, e-mailového klienta, webového prehliadača, kancelárskeho balíka a iných používaných aplikácií.
- Používanie pravidelne aktualizovaného antivírusového balíka/programu.

Záver:

V rámci organizácie vždy reportujte podozrivé aktivity. Ak sa stanete napr. príjemcom podozrivého e-mailu, tak bezodkladne kontaktujte zodpovednú osobu vo Vašej organizácií. Ak sa predmetný e-mail týka aj inej organizácie, napr. zneužitie dobrého mena a podobne, tak poverená osoba by mala kontaktovať aj dotknutú tretiu stranu.