Identifikácia a ochrana pred útokmi typu Phishing

1. Téma, ktorú kapitola prináša

Informáciu o technike podvodného, neoprávneného získavania prístupu k údajom: Phishing. Technika je založená na podvodnej komunikácií s obeťou s cieľom získania citlivých údajov (osobných, bankových,firemných,...) od obetí. Počas phishingu útočník zvyčajne podvrhne falošné stránky, kde následne sa snaží zozbierať citlivé údaje.

2. Okruhy, ktoré vysvetľuje

Popis Phishingu a aj jeho špecifických typov útokov ako sú: Phishing, Spear Phishing, CEO fraud, Vishing, Smishing. Približuje spôsoby útoku, možnosti rozoznania útoku. Definuje dopady útoku. Navrhuje spôsoby ochrany pred útokom.

3. Definície

Najväčšou nevýhodou Phisnigu je jeho jednoduchá vykonateľnosť, pričom často nevyžaduje hlboké programovacie zručnosti.
Phishing je druh podvodného konania, ktorým podvodníci sa snažia získať prístup k citlivým informáciam. Najčastejšie sú to prihlasovacie údaje (napr. do internet bankingu finančného domu), citlivé informácie, ktoré sa dajú ďalej zneužiť alebo speňažiť (napr. špecifické osobné, firemné, údaje z karty, priamy zisk). Phishing využíva slabé stránky obeti. Útočníci sa snažia cielene navodiť situáciu dôvery alebo nájsť slabú stránku obete.

3.1 Popis útoku

Prvým krokom je vytvorenie falošnej správy, najčastejšie je touto správou email. Cieľom falošnej správy je navodiť u obeti pocit, že musí niečo vykonať na svoju ochranu v rámci konkrétnej webovej služby. Toto konanie sa dá naplniť buď priamym vyplnením dotazníka v tele správy alebo presmerovaním pomocou weboveho odkazu v správe na podvrhnutú webovú stránku. Podvrhnutá webová stránka je podobná originálu. Podvrhnutá webová stránka je vytvorená na akejkoľvek existujúcej webovej stránke. Často je vytvorený na stránke podstrom s podobnými názvami, ako je meno stránky, ktorú útočník kopíroval (napr. najlepšie.bankovanie.*dokonalékvetyzababku.sk*)
Phishingova komunikácia je väčšinou posielaná na všetky adresy bez rozdielu, ktoré sú útočníkovi k dispozícii. V takomto prípade počet nehrá rolu, pretože posielanie vo virtuálnom priestore je lacné a rýchle, obete, ktoré nemajú prístup k službe, na ktorú je komunikácia smerovaná sa niekam nebudú hlásiť a žiadne údaje vyplňovať.
Často sa na phishingový útok využíva komunikácia cez sociálne siete, či už prostredníctvom konkrétnych riadených správ alebo pomocou klamlivých kampaní vedených v sociálnych sieťach.
V prípade, ak sa využíva ako nosič informácie osobná správa, využíva sa neoficiálne a skomolené meno známej osobnosti alebo v prípade presne zacielených útokov sa využíva ukradnuté konto konkrétneho človeka. Kampane sú významné tým, že ponúkajú zaujímavú výhru pri poslaní osobných údajov alebo platby.

Analýza phishingových útokov

Navodenie dôvery:

- Firma alebo finančný dom stratila údaje o klientoch, pošle vám správu so žiadosťou o vyplnenie
    - v prípade, že túto správu obdrží klient, ktorý dôveruje konkrétnej firme, nerozmýšľa nad obsahom správy a jeho nereálnosťou, ale vykoná požiadavku. Nereálnosť správy je schovaná v statuse, že firma, ktorá je závislá od osobných údajov klientov má niekoľko úrovní ochrany a je prakticky nemožné, aby prišla o klientské údaje.

- Váš známy pošle správu pomocou emailu alebo cez sociálne siete a varuje Vás pred nebezpečenstvom, proti ktorému sa dá obrániť iba prihlásením sa na konkrétnu stránku a vyplnením údajov.
    - v takomto prípade je útok zamierený na využitie dôvery klienta v konkrétneho človeka. Útoku zvyčajne predchádza napadnutie a získanie dát od konkrétneho používateľa a zneužitie jeho údajov (napr. počítač klienta, emailový klient, sociálne siete klienta,...). Následne sú tieto údaje zneužité na podvodnú komunikáciu s ďalšími potenciálnymi obeťami.

Tlak na sociálne cítenie obete:

- Obeť potrebuje rýchlo poslať peniaze do inej krajiny, pretože je v sociálnej tiesni, alebo je iba krátkodobo v meste, kde sa nachádza finančná inštitúcia, z ktorej je možné vybrať peniaze.
    - tieto správy pôsobia na sociálne cítenie, ale zároveň aj na zlepšenie finančného postavenia obete, pretože za preposlanie peňazí obeť získava aj možnosť získať percentuálnu odmenu z preposlanej sumy. Tento útok je najnebezpečnejší, pretože peniaze vždy pochádzajú z trestnej činnosti a zapojením sa do preposielania sa obeť zároveň stáva členom organizovanej skupiny, ktorý zároveň získa neoprávenné obohatenie z trestnej činnosti. Nebezpečenstvo spočíva v dvoch rovinách:
        - Zapojením do organizovanej trestnej činnosti obeť je zodpovedná a súdne trestateľná a sadzby sú vyššie.
        - Zároveň aj vymáhanie od poškodených sa javí v tomto prípade ako významná vec, pretože obeť je jediné známe ohnivko v organizovanom zločine a preto sa od obete nárokujú všetky škody, či straty ktoré sú s touto činnosťou spojené.

Vytvorenie tlaku na obeť

- Útočník vytvorí tlak na obeť, napríklad prostredníctvom navodenia pocitu, že správu poslala vyššia, nadradená autorita. V takomto prípade sa útočník pripravuje aj niekoľko týždňov, získava údaje o firme a konkrétnych osobách a jednotlivých závislostiach. Príklad: vlastník firmy pošle príkaz na zaplatenie na konkrétny účet účtovníčke. V tomto prípade účtovníčka ako podriadená, ak je takýto spôsob posielania príkazov prirodzený môže podľahnúť klamu a zaplatiť na podvrhnutý účet. Peniaze po prevode sú okamžite vybrané z účtu po prevode a preto je skoro nemožné získať peniaze späť.

3.2 Popis útokov a technológii, ktoré sa témy týkajú (napr. mobil, email,...)

- **Smishing –** patrí do kategórie phishingových útokov, vykonaných pomocou SMSkových správ. V rámci správy je uložená (väčšinou skrátená) linka, ktorá odkazuje na stránku, kde útočník sa snaží získať podvodné informácie. SMS využíva symboliku urgencie ako je výkričník, často s podvrhnutého čísla, aby sa správa javila ako odoslaná konkrétnou organizáciu.
- **Vishing –** technika založená na útoku cez telefón. Buď je podvrhnuté falošné číslo, napríklad ako číslo Call centra konkrétnej firmy, pričom podvrhnuté číslo je presmerované na útočníka, ktorý sa snaží vymámiť od útočníka citlivé údaje. Niekedy je útok vedený zo strany útočníka, ktorý sa snaží vyvolať dojem, že volá dôveryhodná organizácia.
- **Phishing**
- **Spear phishing –** je skupina útokov, ktorá vyžaduje dlhodobejšiu analýzu prostredia konkrétnej firmy a následne je na klientov spustená cielená phishingova kamaň. Pôvodne boli správy rozosielane plošne na klientov, v súčasnosti sa dá na základe ďalších štatistických veličín nasmerovať útok pomerne presne na klientov danej organizácie.
- **Whalling -** je obmedzenie phishingového útoku na konkrétnych ľudí špecifickej organizácie, resp. vo vysokom menežmente. Útočníci si pripravia organizačnú štruktúru špecifickej organizácie, pomocou ďalších metód sociálneho inžinierstva ako je Vishing sa snažia dostať k presnejším informáciam, zároveň sa snažia odchytiť správu z firmy, aby sa naučili písať správy presne v štandardoch a rozmeroch firmy.

- **CEO fraud –** v tomto prípade ide o špecifickú implementáciu Whallingu, kde autorom podvrhnutej, falošnej správy sa javí byť CEO špecifickej organizácie.

Špeciálne útoky

- **Tabnabbing –** tento prístup vyžaduje spojenie dvoch prístupov exploitu stránky konkrétnej organizácie a phishingového útoku. Obsahuje upravenie stránky konkrétnej organizácie alebo vytvorenie vírusu, tak aby sa pri prihlasovaní na konkrétnu stránku organizácie objavilo okno, ktoré imituje okno organizácie, ktoré vyžiada d obete prihlasovacie údaje. Útok využíva nepozornosť obete a možnosť internetových prehliadačov, prepísať načítaný obsah na stránke dlho po načítaní.
- **Evil twin -** útok je založený na vytvorení WiFi siete a donútení presmerovania komunikácie cez túto WiFi sieť. Cieľom je analyzovať sieť a získavať z komunikácie citlivé údaje, poväčšine vhodné na ďalšiu komunikáciu a prihlasovanie pod identitou obete.

3.3 Prvotný bezpečnostný nástrel identifikovania phishingu

Čo si všímať na phishingovej správe?

1. Všeobecné oslovenie, z ktorého vyplýva, že útočník nepozná obeť (napr. Vážený klient)
2. Správa vyžaduje osobné alebo bankové údaje (dáta z karty, meno/heslo)
3. Neštandardná komunikácia, komunikácia, ktorú konkrétny odosielateľ nikdy neviedol a takúto správu ani neposiela. Snaží sa vytiahnúť dáta od obete, ktoré by daná firma nikdy si nepýtala.
4. Pocit naliehavosti alebo výhodná ponuka – phishingový útok prebieha rádovo v dňoch, je nevyhnutné aby sa prípadná obeť zapojila v prvých dňoch útoku.
5. Neštandardná doména – doména na kde sa vypĺňajú údaje nepatrí konkrétnemu odosielateľovi alebo je len vzdialene podobná aleo obsahuje preklepy. Kontrolujte správnosť URL adries navštevovaných adries.
6. Zlá jazyková úroveň
7. Používajte aktualizovaný operačný systém

V prípade, že si nie ste istí, že konkrétna správa je phishingová, kontaktujte adresáta a opýtajte sa, či je to žiadosť, ktorú poslal. Nepoužívajte možnosť Odpovedať/Reply na email, ktorý ste dostali, kontakt získajte na oficiálnych webových stránkach, aby kontakt nebol nadviazaný s útočníkom. Obozretnosť je nadôležitejšia pri pravotnom rozoznávaní phishingového útoku.

3.3. Vyššia ochrana pred phishingom

Vyhýbajte sa klikaniu na odkazy v neznámych správach. Útočníci využívajú populárne skrátené názvy domén, na zakrytie útoku. Pri kliknutí, okrem získania údajov, útočníci zároveň sa snažia napadnúť počítač obete.

Zabezpečenie konkrétnej Webovej stránky je ochránené bezpečnostným certifikátom, ktorý musí patriť odosielateľovi, skontrolujte vlastníka certifikátu.

Majte antivírus aj s kontrolou emailového klienta a rozšírením o ochranu pred phishingom (*antiphishing solution*).

Nepoužívate neznáme programy alebo programy, ktoré boli stiahnuté z neznámeho úložiska.

Používajte zdravý sedliacky rozum.