Sociálny inžiniering, útok s obrovským dopadom

1. Téma, ktorú kapitola prináša

Sociálne inžinierstvo je spôsob manipulácie ľudí a účelom neoprávneného získania určitej informácie.

2. Okruhy, ktoré vysvetľuje

Zameranie sociálneho inžinierstva na napadnutie a zneužitie základných osobnostných nastavení človeka.

3. Základné predpoklady:

Sociálne inžinierstvo sú systematicky používané vedomosti ľudského chovania a umenia presviedčať, aby užívateľ urobil to, čo by za normálnych okolností, pri dodržiavaní všetkých bezpečnostných pravidiel nikdy neurobil. Tým sú samotným ľudským faktorom prelomené technologické a organizačné bezpečnostné opatrenia a je umožnený kybernetický útok.[1]
Sociálne inžinierstvo je jedným z najnebezpečnejších spôsobov útoku, napriek tomu, že nevyžaduje veľké technické zručnosti, je zamerané na človeka. Hacker využíva inteligenciu a znalosť osobnosti človeka. Ciele sociálneho inžinierstva sú:

- Spáchanie podvodu,
- Obohatenie sa,
- Narušenie systému alebo siete,
- Priemyselná špionáž,
- Krádež identity,
- Pomsta,

Vhodnými cieľmi sa javia veľké firmy s významným dopadom na obyvateľstvo, ako sú: operátori (internetu a telefonickí), finančné inštitúcie, vládne a vojenské agentúry, nemocnice.
Výhoda útoku je v jednoduchom prístupe k veľmi dobre ochráneným informáciám. Napr. namiesto zložitého prieniku do dobre zabezpečeného systému, hacker zatelefonuje vhodnej osobe a vypýta si prístupové oprávnenia. Základný kameň na naštartovanie útoku sociálnym inžinierstvom je vzbudenie dôvery. Pred samotným útokom si útočník zistí potrebné informácie o obeti prostredníctvom verejne dostupných zdrojov (sociálne siete, blogy, firemné stránky, tlačové správy, webové komunity, reporty, konferencie,...). Prípadne sa snaží dostať do jednotlivých objektov a získať údaje priamo z objektov odpozorovaním, prezeraním košov, ukradnutím. Nasleduje analýza a príprava útoku. Cieľom útoku je zneužitie slabín obete, kam patrí nízke bezpečnostné povedomie, nepoznanie interných pravidiel organizácie, ochota pomáhať, možnosť umiestňovania citlivých informácii na sociálne média.
Techniky sa delia

- Tvrdé – využívajú ľudskú slabosť, labilnosť, frustráciu, pomstychtivosť , škodoradosť, závisť.
- Mäkké – zakladajúce sa na zneužití ľudskej dôverčivosti

Sociálne inžinierstvo sa delí

- Fyzické: prechádzanie cez kancelárie a prehľadávať stoly, odpadky, zabudnuté telefóny,..
- Virtuálne: kontaktovanie potenciálnych obetí vzdialene (telefón, sms, email) a získavanie osobných dát.

Popis útoku technikami sociálneho inžinierstva:

- Zhromažďovanie informácii
- Budovanie vzťahov a dôvery
- Využitie dôvery
- Realizácia a zneužitie

Počas útoku pomocou sociálneho inžinierstva sa využívajú vlastnosti ľudí, ktoré sú pokladané za dobré vlastnosti, napríklad:

- Dôvernosť
- Ľútosť
- Láskavosť
- Zvedavosť
- Ochota pomáhať

3.1 Priblíženie jednotlivých útokov

Trashing

Je to metóda založená na prehľadávaní odpadkových košov a získania citlivých informácii z dokumentov alebo starých nosičov (USB, CD, starý mobil).

Pretexting

Pretexting je spôsob manipulácie obete s tým, že časť informácie je pravdivá a overiteľná. Informácie, ktoré obeť dostáva sú presne adresované a ich súslednosť je kontrolovaná útočníkom. Cieľom je presvedčiť obeť o legitímnosti požiadaviek. Technika narába s technikami rétoriky. Je využívaná nielen útočníkmi, ale aj súkromnými detektívmi a v bežnej životnej a školskej praxi. Na implementáciu je potrebná príprava a zozbieranie vhodných informácii, sú známe prípady, keď nebolo potrebné vedieť priveľa údajov, stačilo využívať autoritatívny tón a presvedčivý obsah konverzácie. Útok je presne cielený so zameraním na konkrétneho človeka alebo malú skupinu ľudí a cieľom je získanie konkrétnych informácii.

Phishing

Podvodná technika, ktorá využíva internetové prostriedky na získavanie citlivých údajov ako sú heslá, čísla kariet, osobné údaje. Princípom je dostať adresátovi podvodnú správu s cieľom vymámenia citlivých údajov, častom sa ako odosielateľ vydáva samotná firma, ktorej klienti sú terčom útoku. Phishing je orientovaný primárne na klienta firmy, nie na firmu samotnú. Príprava útoku je jednoduchá a útok je vedený plošne na všetky dostupné kontakty s malou mierou správneho smerovania komunikácie, v prípade zasiahnutia dôverčivej obete sa počíta s vysokým ziskom.

IVR phishing

Útočníci vytvoria falošný odpovedací telefónny automat, s podobnou štruktúrou ako konkrétna firma (napríklad odpovedajúca služba finančnej organizácie). Automat je vystavený na podobnom čísle ako originálna inštitúcia a obeť je vyzvaná na zavolanie do banky na priložené telefónne číslo. Počas komunikácie sú od obete vylákané prihlasovacie údaje a následne zneužité. Príprava útoku je zložitá, následne záleží na výbere obete, na ktorú bude vedená komunikácia, útok sa využíva len vo veľmi špecifických prípadoch.

Spear phishing

Útočník vytvára komunikácie prostredníctvom elektronických komunikačných prostriedkov a vydáva sa za dôveryhodnú osobu. Útočník sa vydáva za prepravné spoločnosti, finančné inštitúcie, či iné dôveryhodné organizácie (ako napríklad pošta), posiela adresné emaily sc ieľom zasiahnuť klienta a potenciálnu obeť, vmanipulovať ju do stavu, že prezradí citlivé údaje. Všetky informácie v emaile musia byť uveriteľné a napísané a doručené spôsobom, ktorý je používaný organizáciou. Často ide o priamy útok s cieľom zmanipulovať obeť do poslania peňazí na určené konto (*CEO fraud – spear phishing*, pri ktorom sa útočník vydáva za riaditeľa firmy a manipuluje obeť do poslania peňazí na konkrétny účet). Útok s veľkým dopadom je, keď obeť vmanipuluje útočník k inštalácii, či spusteniu vírusu na zariadení organizácie. V tomto prípade ide útočníkovi o získanie prístupu na pracovnú stanicu alebo to robí s cieľom urobiť organizácii čo najväčšiu škodu, napríklad zašifrovaním pracovných diskov. Útok je orientovaný na úzku skupinu potenciálnych obetí. Úspešnosť útoku závisí od dôverčivosti obete.

Baiting

Útočník nechá záznamové médium (CD, DVD, USB) na mieste, kde ho obeť ľahko nájde, využije zvedavosť obete, ktorá toto médium vloží do svojho počítača a nakazí ho nežiadúcim kódom. Nežiadúci kód sa automaticky snaží prihlásiť do internetu. Cieľom útočníka je získať prístup do

počítačovej siete. Príprava útoku je stredne zložitá, útok je vedený plošne na všetky dostupné kontakty konkrétnej firmy s malou mierou správneho smerovania komunikácie. Správna funkcia závisí od bezpečnostnej ochrany počítačového prostredia konkrétnej firmy (ak sa nespustí vírus z USB, nebude útok fungovať).

Quid pro quo (niečo za niečo)

Útočník zistí telefónne čísla spoločnosti a začne telefonovať na všetky, pričom sa tvári ako technická podpora a pýta sa, ako vie pomôcť zamestnancovi. S vysokou pravdepodobnosťou nájde zamestnanca, ktorému sa nedostáva pomoc a preto rád pomôže technickej pomoci/útočníkovi spustením programu alebo špeciálnou akciou v informačnom systéme organizácie. Príprava útoku je stredne zložitá, útok je vedený na všetky dostupné kontakty konkrétnej firmy s malou mierou správneho smerovania komunikácie, používajú sa techniky rétoriky.

Watering holes

Jedno z technicky zložitejších foriem sociálneho inžinierstva. Podmienkou je vytipovať si vhodný typ obetí, následne nájsť webovú stránku s vysokou mierou dôvery pre danú skupinu a infikovať / kompromitovať webovú stránku vírom. Využíva sa hlavne technika „drive-by download“, t.j. technika stiahnutia víru bez potreby alebo len s minimálnou potrebou interakcie s obeťou. Príprava útoku je stredne zložitá, útok je vedený plošne na všetky dostupné kontakty konkrétnej firmy s malou mierou správneho smerovania komunikácie. Úspešnosť útoku závisí od bezpečnostnej ochrany počítačového prostredia konkrétnej firmy (ak sa nespustí vírus z USB, nebude útok fungovať).

Reverzné sociálne inžinierstvo

Štandardné sociálne inžinierstvo znamená kontakt útočníka s obeťou, reverzné sociálne inžinierstvo vytvára podmienky tak, aby obete vyhľadali útočníka. Cieľom je zmanipulovať obeť tak, aby sama pokladala útočníka za osobu z dôveryhodnej organizácie a vie pomôcť s problémom, ktorý sám útočník vytvoril. V tomto prípade obeť úplne dôveruje útočníkovi a preto je náchylná na poskytnutie dôverných údajov.

Príprava útoku je veľmi zložitá, následne záleží na výbere obete, na ktorú bude vedená komunikácia, útok sa využíva len vo veľmi špecifických prípadoch.

Podvodné lotérie

Sú to lotérie, najmä „vyskakovacie“ okná, kde sa aplikuje útok na dôverčivosť obete. Útočník ponúkne výhru (napr. nový iPhone), obeť sa musí prihlásiť do systému pomocou svojich pravých údajov, poprípade zaplatiť kartou účastnícky poplatok. Útočník získa prístup k osobným aj platobným dátam.

Lotérie sa prenášajú v súčasnosti do sociálnych médií a orientujú sa na obete z radov detí. Príprava útoku je veľmi zložitá, úspešnosť závisí od spôsobu komunikácie s obeťou. Útok s rozšírením sociálnych sietí sa objavuje stále častejšie.

4 Bezpečnostné odporúčania

Neexistuje komplexná, priama ochrana pred jednotlivými typmi útokov. Ochrana sa zameriava na ochranu technického perimetra, tak, aby sa zabránilo prieniku škodlivého kódu do vnútra organizácie. Hlavnou ochranou je sústavné zvyšovanie bezpečnostného povedomia členov organizácie a nastavením pravidiel a procesov pre všetkých členov organizácie. V prípade útoku by mal každý zamestnanec vedieť, kam a komu sa má ozvať, v prípade pochybností pri komunikácii s externou osobou.

4.1 minimálne

Technická ochrana

- Používať len autorizované (známe zariadenia)
- Mať aktualizovaný antivírusový softvér, spamové filtre a posledné patche,
- Blokovanie neautorizovaných zariadení,
- Používanie len bezpečných sietí na pripojenie počítača a mobilných zariadení,

Procesná ochrana

- Sústavné zvyšovanie bezpečnostného povedomia dotknutých osôb
- Pripraviť vo firme bezpečnostné procesy na riadenie správania zamestnancov a nastavenie základnej úrovne bezpečnosti.
- Pripraviť a implementovať proces Incident menežmentu aj so zaučením pracovníkov na identifikovanie hrozby a rýchlom a správnom nahlásení hrozby.

4.2 základné

Nevyhnutným prostriedkom pre zabezpečenie ochrany je zadefinovanie kritických aktív a informácii v organizácii. Tieto údaje budú vstupnými informáciami pre vytvorenie komplexnej analýzy rizík. Na základe tejto analýzy je nevyhnutné implementovať ochranné technické prvky do prostredia a vytvoriť vzdelávaciu aktivitu, aby zamestnanci chápali dôležitosť aktív a informácii a spôsob ich ochrany, musia vedieť rozoznať útok a reagovať naň.

5 Psychologické faktory

V prípade útoku systémom Sociálneho inžinierstva je veľmi dôležité používať psychologické prístupy, ktoré zjednodušia nájdenie si cesty k obeti. Jednotlivé prístupy je nevyhnutné poznať, aby obeť mohla identifikovať prípadné použitie techniky.

Silný afekt

Ak obeť cíti silný hnev, alebo je prekvapená, rozrušená, či v panike, bude s menšou pravdepodobnosťou rozmýšľať o prezentovaných argumentoch. Afekt sa spúšťa vyslovením výroku, ktorý spustí príval emócii. Na tejto istej báze funguje kontrafaktuálne myslenie, v tomto prípade obeti je ponúknutá veľká výhra, následne obeť riskuje skutočný tovar, pričom ignoruje myšlienku, že pravdepodobnosť výhry je minimálna.

Preťaženie

Útočník rýchlo za sebou odovzdá veľa informácii naraz, pričom zahltí obeť a tá nevie rozlíšiť mylné predpoklady od presvedčivých banalít a postaví sa do polohy, radšej absorbuje informáciu, akoby ju vyhodnotila. Rovnako funguje argumentácia z nečakanej perspektívy. Obeť potrebuje čas na vytvorenie argumentácie, má veľa informácii, nedostatok argumentov a je ochotná prijať aj argumenty, ktoré by normálne odmietla.

Opätovanie

Opätovanie alebo reciprocita – útočník presvedčí obeť, že jej niečo dal a vyžaduje spätne vrátenú vec. Obeť často nevie rozlíšiť alebo nerozlišuje, že dar bol vynútený a že vrátená vec je oveľa hodnotnejšia. V korporátnom svete je to nastavenie: ak niekto zatelefonuje a požiada o pomoc s problémom volajúci mu ochotne pomôže, dokonca je k tomu firmou nabádaný, využíva to hlavne inverzné sociálne inžinierstvo. Druhý prístup: ak majú obeť aj útočník vážne požiadavky a útočník ustúpi, obeť bude mať tendenciu ustúpiť tiež. Útočníkovi stačí vytvoriť viac ako jednu požiadavku.

Klamlivé vzťahy

Útočník nadviaže kontakt s obeťou, ak komunikáciu nastaví tak, aby obeť uverila, že má s útočníkom podobné vlastnosti bude cítiť silný element komunikovať a jednať s útočníkom kladne a dôverovať mu bez opodstatneného dôvodu. Iným spôsobom je odhaľovanie obeti útočníkom svojho vnútorného nastavenia , prerozdelenie „tajných“ informácii, či diskutovanie o nepriateľoch.

Rozšírenie zodpovednosti a morálne povinnosti

Obeť je vmanipulovaná, že svojou činnosťou a rozhodovaním ovplyvní úspech, či zlyhanie spoločnosti. Alebo zamestnanec, ktorý volá vie ovplyvniť zotrvanie v spoločnosti. V týchto prípadoch je pre obeť veľmi ťažké urobiť akékoľvek rozhodnutie a zamestnanec sa poddá útočníkovi.
Často je útok rozšírený o morálne povinnosti, t.j. útočník, ktorý volá robí niečo pre záchranu obete, preto obeť pomáha útočníkovi, často sa chce vyhnúť pocitu viny.

Autorita

Útočník sa vydáva za vysoko postavenú osobu, ak obeť nevyužije overenie útočníka alebo ak overenie nie je k dispozícii, bude útočník považovaný za kompetentnú osobu, ktorá môže získať citlivé údaje.

Bezúhonnosť a dôslednosť

Zamestnanci majú sklon pokračovať v práci na pracovisku aj keď majú podozrenie, že požiadavka nie je oprávnená. Ľudia majú tendenciu veriť ostatným, ak rozprávajú o svojich skutočných názoroch a rozhodnutiach, tendencia je primárne založená na ich čestnosti a vyjadrovaní pocitov.

6 Pohľad na obete

6.1 pohľad psychológa vzhľadom na obete

6.2 ako rozoznať obeť?

6.3 ako pomôcť obetiam?

Literatúra

[1] Rak, R. – Kummer, R. 2007. Informační hrozby v letech 2007-2017. In: Magazín Security, 2007, č. 1, s. 2 – 5.