Concepte legate de securitate

1.3. Securitate personală

1.3.1. Înţelegerea termenului de inginerie socială şi a implicaţiilor sale

- **Ingineria socială** (cunoscută sub numele de *social engineering)* este o metodă de manipulare a oamenilor în vederea obţinerii unor informaţii confidenţiale.
- De obicei, un atac social începe cu o cercetare amănunţită a persoanei ţintite, după care se realizează diverse scenarii de abordare a acesteia, se anticipează întrebările victimei şi se pregătesc răspunsurile adecvate. Una din tehnicile de bază include crearea simţului de încredere din partea victimelor. Iniţial inginerul social crează o problernă, pe care ulterior o rezolvă miraculos, impunând prin înşelăciune victima să divulge informaţii.

- Principalul scop al unui inginer social este să obţină acces neautorizat la date, să culeagă informaţiile confidenţiale pe care ulterior să le folosească în scopul comiterii diverselor tipuri de fraude.
- Pentru a preveni aceste situaţii, companiile trebuie să-şi întărească politicile de securitate, inclusiv împotriva tehnicilor de inginerie socială.
- De asemenea, este recomandată instruirea angajaţilor pentru a monitoriza diverse tipuri de inginerie socială (de exemplu recepţionista sau agentul de pază sunt cei mai expuşi acestor tipuri de atacuri).

1.3.2. Identificarea metodelor ingineriei sociale

Tehnicile folosite de inginerii sociali pentru a obţine accesul la informaţii securizate sunt:

- **Phone Fishing** - prin această metodă inginerul social va telefona unei persoane, asumându-şi o altă identitate şi va solicita informaţii confidenţiale (parole de la computer, coduri PIN, CNP, detaliile cârdului de credit etc).
- **Phishing** - Atunci când vă publicaţi adresa de email pe Internet, când completaţi formulare Online, accesaţi newsgroup-uri sau site-uri web, datele dumneavoastră pot fi furate de către aplicaţii de indexare pentru Internet şi apoi folosite fraudulos. Phishing-ul (derivat din termenul din limba engleză pentru "pescuit") se referă la o formă de activitate frauduloasă care constă în obţinerea unor date confidenţiale, cum ar fi datele folosite în aplicaţii bancare (online banking), aplicaţii de comerţ electronic sau informaţii referitoare la cardurile de credit, folosind tehnici de manipulare a datelor identităţii unei persoane sau unei instituţii. Un atac de tip phishing constă în trimiterea de către atacator a unui mesaj electronic în care utilizatorul este sfătuit să divulge date confidenţiale pentru a câştiga anumite premii sau este informat că, datorită unor defecţiuni tehnice ce au dus la pierderea datelor originale, este necesară retransmiterea acestor date confidenţiale Informaţiile cerute sunt de obicei:
    - Numărul cardului de credit/ debit;
    - codul PIN pentru ATM;
    - informaţii despre contul bancar; codul numeric personal/ contul de asigurare;
    - conturi de email, parole etc.
- în mesajul electronic primit, utilizatorul este direcţionat spre un site clonă (un site ce pare identic cu site-ul unei instituţiei bancare, licitaţii online etc) unde este invitat să completeze un formular cu datele confidenţiale. Trebuie să ţineţi cont de faptul că organizaţiile oficiale nu trimit niciodată astfel de mesaje, care solicită informaţii personale.
- **Shoulder Surfing** reprezintă un set de tehnici de observare directă (cum ar fi uitatul peste umărul cuiva) pentru a obţine informaţii. Shoulder Surfing este o modalitate eficientă de a obţine informaţii în locuri aglomerate întrucât este destul de uşor să staţi lângă cineva şi să urmăriţi cum persoana respectivă introduce un cod PIN la telefon, la un bancomat sau la un POS sau cum introduce o parolă la un cont de email. Acest proces se poate face şi de la distanţă, cu ajutorul unui binoclu sau altor dispozitive specializate. Pentru a preveni acest tip de atac, se recomandă să acoperiţi tastatura cu o mână atunci când introduceţi aceste informaţii.
- **Dumpster diving** reprezintă o tehnică de aflare a unor informaţii confidenţiale care apoi vor fi utilizate pentru a obţine accesul la o reţea de computere. Inginerii sociali caută până şi în tomberoane unde găsesc post-it-uri, hârtii, calendare, nume, facturi, corespondență etc conţinând informaţii confidenţiale. Pentru a preveni acest tip de atac, se recomandă companiilor să toace hârtiile nefolositoare la un tocător de hârtie.

1.3.3. Înţelegerea termenului de furt de identitate şi a implicaţiilor sale

- Furtul de identitate reprezintă frauda de a-ţi însuşi datele personale ale altei persoane, în scopul de a fura bani sau de a avea alte beneficii. Furtul de identitate apare atunci când cineva foloseşte informaţiile dvs. de identificare personală (nume, CNP, numărul cardului de credit, adresă de email) fără permisiunea dvs, pentru a comite fraude sau alte infracţiuni.
- Implicaţiile furtului de identitate sunt:
  - Datele dvs personale, profesionale, financiare, juridice pot fi accesate fără știrea dvs
  - Datele dvs personale vor fi utilizate în activităţi frauduloase (obţinerea de credite în numele dvs, obţinerea de tratamente medicale, obţinerea de servicii financiare, asumarea identităţii dvs. în viaţa curentă).

1.3.4. Identificarea metodelor de furt de identitate

- **Pretexting** constă în crearea unui scenariu sau pretext prin care persoana ţintă este abordată şi manipulată pentru a divulga informaţii confidenţiale.În funcţie de gradul de dificultate al procesului de manipulare, inginerii sociali sunt dispuşi să obţină uniforme sau legitimaţii aparent veritabile pentru a pretinde că sunt persoane autorizate (precum poliţişti, jandarmi, agenţi de la Administraţia Financiară etc.) să primească informaţiile solicitate.
- **Information diving** constă în recuperarea informaţiilor de pe calculatoarele sau dispozitivele de stocare aruncate la gunoi. Atunci când un computer nu mai funcţionează sau s-a învechit, acesta este aruncat la gunoi sau vândut, pentru a putea fi înlocuit cu unul nou. Însă, multe persoane uită să formateze hard disk-ul computerului înainte de a-l arunca. Astfel, inginerii sociali pot obţine foarte uşor informaţii confidenţiale recuperând hard disk-ul de la tomberon.
- **Skimming-ul** reprezintă procesul de obţinere a detaliilor contului bancar în vederea efectuării diverselor tranzacţii. Obţinerea informaţiilor se realizează folosind un dispozitiv, numit skimmer, ce se montează peste gaura de acces în bancomat astfel încât, atunci când victima introduce cardul în bancomat, acesta trece prin acel dispozitiv ce preia automat informaţiile cardului, acestea fiind apoi automat copiate pe un cârd gol. Skimmer-ul se montează împreună cu o cameră video foarte mică ce va filma şi introducerea codului PIN, oferind astfel infractorului acces total la contul dumneavoastră. Această metodă a creat foarte multe victime deoarece skimmer-ul este destul de greu de observat.