Securitate cibernetică pentru IMM-uri

Inginerie socială - utilizatorii sunt veriga cea mai slabă

De CTS Customized Training Solutions & CASE

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Obiective și scopuri:

La finalul acestui modul, veți putea să:

- definiți ingineria socială
- recunoașteți și distingeți cele mai frecvent folosite tehnici de inginerie socială
- înțelegeți mecanismele de manipulare folosite de către atacator
- localizați potențialele surse de atac
- analizați riscul unui atac de inginerie socială asupra companiei dumneavoastră

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Index

Unitatea 1: Ce este ingineria socială?

1.1: Definiție
- Sunteți în siguranță?
- Cea mai slabă verigă

1.2: Ce este un atac de inginerie socială?
- Ce tip de date este considerat sensibil?

1.3: Principiile atacurilor de inginerie socială
- Ce se întâmplă în timpul unui atac?

1.4: Cine poate deveni o victimă?

Unitatea 2: **Tehnici de inginerie socială**

2.1: Mesaj de la un prieten
- De ce v-a făcut John acest lucru?
- Când puteți fi atacat cu această tehnică?

2.2: Phishing
- Cum poate arăta acest scenariu?

2.3: Vishing
- Cum poate arăta acest scenariu?
- Când puteți fi atacat cu această tehnică?

.4: Baiting
- Cum poate arăta ac

2.5: Rezumat

Unitatea 3: **Prevenirea ingineriei sociale**

3.1: Ce să faceți și ce să nu faceți

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.1: Definiție

Ingineria socială în contextul IT este un termen folosit pentru diferite activități rău intenționate realizate prin interacțiuni umane. Se bazează pe manipulare psihologică. Scopul este de a împinge un utilizator să facă o greșeală de securitate. Cu alte cuvinte, atacul de inginerie socială este posibil numai dacă utilizatorul nu este conștient de intenția dăunătoare.

Sunteți în siguranță?

Atacurile de inginerie socială vă pot lovi oricând, indiferent de mărimea afacerii pe care o construiți.

Cea mai slabă verigă

Veriga cea mai slabă este utilizatorul: dumneavoastră, angajații, partenerii de afaceri. Pentru a minimiza riscurile, trebuie să maximizați gradul de conștientizare. Cum faceți acest lucru?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.2: Ce este un atac de inginerie socială?

Înțelegerea atacurilor de inginerie socială este primul pas pentru a crește gradul de conștientizare în rândul angajaților dumneavoastră. În primul rând, trebuie să rețineți că infractorii cibernetici și escrocii organizează aceste atacuri. Cu toate acestea, nu întotdeauna este vorba despre bani. Orice cantitate de informații (cum ar fi accesarea unor parole) sau de date sensibile este suficientă pentru a determina o fraudă.

Ce categorie de date este considerată sensibilă?

- date personale care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice
- apartenența politică
- date genetice, date biometrice prelucrate exclusiv pentru a identifica o ființă umană
- date legate de sănătate
- date referitoare la viața sexuală sau orientarea sexuală a unei persoane *

*Source: European Commission > What personal data is considered sensitive?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.3: Principiile atacurilor de inginerie socială

În general, un atac de inginerie socială implică trei pași

pasul 1: atacatorul vizează o victimă

- identificarea victimelor
- cercetare
- alegerea metodelor de atac

pasul 2: atacatorul câștigă încrederea victimei

- angajarea victimei într-o poveste
- preluarea controlului asupra interacțiunii
- câștigarea punctului de sprijin

pasul 3: atacatorul își atinge obiectivul, furând date sau încălcând practicile de securitate

- executarea atacului
- eliminarea urmelor
- dispariția

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.3: Principiile atacurilor de inginerie socială

Într-un atac de inginerie socială, atacatorul folosește manipularea psihologică. De aceea, este chiar mai periculos decât un atac cibernetic asupra sistemului dumneavoastră. De ce? Pentru că trebuie să fiți sigur că dumneavoastră și angajații puteți discerne între manipulare și publicitatea standard. Nu este ușor pentru că suntem doar oameni.

Ce se întâmplă în timpul unui atac?

Atacatorul se bazează pe slăbiciunile victimei. Deci, să ne gândim la atacul de inginerie socială ca la un joc murdar, în care o singură persoană cunoaște regulile, și chiar le creează uneori. Ca orice joc, și acesta are câteva mecanisme generale care ar trebui să crească șansele de câștig.

Majoritatea atacurilor de inginerie socială se bazează pe 5 principii: autoritate, dovadă socială, deficit, urgență, familiaritate.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.3: Principiile atacurilor de inginerie socială

autoritate:
atacatorul se prezintă ca o figură care are autoritate

deficit:
atacatorul folosește mecanismul pe care victima nu-l va sesiza dacă nu va face nimic

familiaritate:
atacatorul convinge victima să execute anumite acțiuni prin câștigarea încrederii sale

dovadă socială:
atacatorul folosește presiunea socială pentru a forța victima să demareze o acțiune

urgență:
atacatorul se bazează pe ideea că victima va rata atacul dacă nu acționează cât mai repede

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.4: Cine poate deveni o victimă?

Tocmai ați cunoscut 5 principii ale atacurilor de inginerie socială. Aceste principii sunt legate de factorii psihologici și de motivația oamenilor. Acestea, desigur, există în subconștientul nostru. Robert Cialdini, psiholog și autor al cărții intitulate „Influență: Știință și practică” a descris modul în care oamenii pot fi influențați de alții. Potrivit lui Cialdini, factorii cheie sunt:

Reciprocare

În general, oamenii se simt obligați să returneze ajutorul primit. Această caracteristică pare firească pentru toate culturile, astfel încât nu ne simțim incomod când cineva ne cere să returnăm favoruri.

Cialdini a menționat că așa-zișii profesioniști în conformitate oferă adesea un mic cadou potențialilor clienți, profitând de această trăsătură. Studiile arată că până și un cadou nedorit îl va influența pe destinatar să întoarcă favorul.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.4: Cine poate deveni o victimă?

Angajament și consecvență

Oamenii își păstrează adesea obiceiurile și alegerile inițiale, dorindu-și să pară consecvenți din punct de vedere comportamental. Totodată, apreciază consecvența celorlalți. Cialdini a menționat că acest lucru este strâns legat de dorința oamenilor de a respecta angajamentele asumate, oferind argumente suplimentare și motivare pentru a le susține.

Dovadă socială

Am menționat deja mecanismul referitor la principiile ingineriei sociale. Dovada socială înseamnă că oamenii au încredere în persoane similare cu ei înșiși în luarea unor decizii. Acest lucru este mult mai evident în situații nesigure.

Cialdini a menționat și că așa-zișii profesioniști în conformitate oferă informații false despre ceilalți valorificând această trăsătură. De exemplu, pregătesc interviuri, date false sau studii de vaz.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.4: Cine poate deveni o victimă?

Aprecierea

Nu e un secret că oamenii au nevoie să fie apreciați, iar acest lucru îi determină pe oameni să accepte oferte de la oamenii pe care îi apreciază.

Cialdini a menționat că aprecierea oamenilor se poate manifesta în mai multe moduri (de ex. poate fi o atracție fizică sau alegerea unei persoane similare).

Autoritatea

Acesta este probabil cel mai periculos factor de influență, oferind atacatorului cea mai mare putere. În general, oamenii îi urmează pe cei care par a fi cei mai puternici, mai buni, mai încrezători în ochii lor; care au ceva ce ei nu au. Studiile arată că oamenii reacționează de obicei într-un mod automat la instrucțiunile autorității și chiar la simbolurile autorității (cum ar fi mașini scumpe, uniforme, diplome, diplome academice etc.). Asta se întâmplă chiar și atunci când instinctul sugerează că instrucțiunile ar trebui respinse.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Ce este ingineria socială?

1.4: Cine poate deveni o victimă?

Deficitul

Din nou, am menționat acest mecanism vorbind despre principiile atacurilor de inginerie socială. Deficitul se bazează pe dorința oamenilor de a poseda lucruri mai puțin disponibile, care pot fi fie exclusiviste, fie limitate în timp. Această trăsătură ajută de exemplu agenții de publicitate să promoveze bunuri cu „disponibilitate limitată” sau „doar pe timp scurt”.

Deci, cine poate deveni o victimă a atacurilor sociale?

În general, oricine. Cu toate acestea, psihologia unei persoane și condiția actuală sunt importante. Rețineți că ingineria socială se bazează mereu pe manipulare.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Tehnici de inginerie socială

2.1: Mesaj de la un prieten

Imaginați-vă că sunteți la serviciu, scrieți niște rapoarte în Excel în cloud-ul companiei și, între timp, aruncați o privire la conturile de social media. Deci, într-un singur browser ați deschis atât Excel-ul, cât și Facebook-ul. În timp ce completați diagrame plictisitoare, cel mai bun prieten al dumneavoastră (să-i spunem John) vă scrie pe Messenger. John v-a scris că niște fotografii în care apăreți dezbrăcat sunt disponibile pe site-ul web atașat - și a trimis link-ul. Dați click pe link și...

Probabil tocmai ați pierdut accesul la contul dumneavoastră de Facebook și/sau la site-ul companiei. Probabil ați compromis și unele date stocate pe computer.

De ce a făcut John acest lucru?

Să fim sinceri, persoana respectivă nu era John...

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Tehnici de inginerie socială

2.1: Mesaj de la un prieten

Probabil a fost un bot creat pentru a fura date. John a fost, de asemenea, o victimă. Atacatorul i-a folosit identitatea (în acest caz, contul de socializare) pentru a vă câștiga încrederea. La urma urmelor, îl cunoașteți foarte bine pe John, ați crescut împreună și sunteți cei mai buni prieteni. De unde poate ști atacatorul asta? Poate aveți multe poze împreună, vorbiți mult prin Messenger sau poate a fost o coincidență — dar a funcționat. Acum sunteți următoarea victimă din lanțul lung numit phishing.

Când puteți fi atacat cu această tehnică?

Atunci când utilizați rețelele sociale, mesageria instant, chat-urile, e-mailurile, SMS-urile etc.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Tehnici de inginerie socială

2.2: Phishing

În zilele noastre, cea mai populară tehnică de inginerie socială este phishingul. Phishingul este orice fel de campanie de mesagerie planificată pentru a redirecționa victima către un anumit formular sau website. Atacatorul falsifică o sursă de încredere (de exemplu, un prieten, o bancă, o agenție de asigurări, fonduri de investiții) și pregătește un scenariu rezonabil. Tema emoțională puternică ajută de obicei la suspendarea neîncrederii.

Cum poate arăta un scenari?

ca o cerere urgentă de ajutor

„Prietenul” dumneavoastră a rămas blocat în străinătate, a fost jefuit, bătut și este în spital. Are nevoie de bani și vă îndrumă cum să faceți un transfer.

SAU

„Prietenul” dumneavoastră v-a văzut pozele în posturi indecente pe internet și v-a trimis un link.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Tehnici de inginerie socială

2.2: Phishing

acțiuni cu un context aparent legitim

„Banca” dumneavoastră v-a trimis un SMS cu linkul în care vi se solicită să confirmați soldul.

SAU

„Furnizorul dumneavoastră de hosting v-a trimis un e-mail în care susține că stocarea datelor a fost piratată și trebuie să-i contactați prin formularul atașat.

cereri de donații caritabile

O anumită autoritate vă cere ajutorul pentru repararea efectelor unui teribil dezastru natural, campanie politică sau act de caritate.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Tehnici de inginerie socială

Section 2.3: Vishing

Vishing este o variantă a phishing-ului efectuată folosind tehnologia vocală, cum ar fi un apel telefonic, un apel Messenger/Zoom sau un mesaj vocal fraudulos. Mecanismele de manipulare sunt aceleași ca în phishing, dar atacatorul folosește mesaje vocale urgente sau apeluri pentru a convinge victima să acționeze.

Cum poate arăta un scenariu?

pericol uriaș →

După declarația atacatorului despre un pericol enorm, precum piratarea conturilor bancare sau taxele neplătite, simte victima are tendința de a acționa rapid, împărtășind datele și parolele sensibile în timpul apelului.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Tehnici de inginerie socială

2.3: Vishing

Când puteți fi atacat cu această tehnică?

Când aveți un profil/site public al companiei cu numărul tău de telefon (nu doar al dumneavoastră, ci și al angajaților), când distribuiți numărulde telefon în rețelele de socializare, când utilizați mesageria instantanee și aplicațiile cu opțiune de apel vocal etc.

2.4: Baiting

Uneori, în loc de pericol, există o oportunitate uriașă. Sunteți câștigător, puteți investi o sumă mică de bani și în scurt timp se transformă într-o avere! Este bine de reținut că atacatorii folosesc adesea momeala sub acoperirea diferitelor fonduri europene. Este posibil să fiți atacat prin formulare online, apeluri telefonice sau chiar în persoană.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Tehnici de inginerie socială

2.4: Baiting

Cum poate arăta scenariul?

există ceva ce vă doriți

Atacatorul alege ceva ce își doresc oamenii, de exemplu descărcarea un film nou. Mulți oameni înghiți momeala pentru a intra în posesia lucrurilor respective.

o afacere grozavă!

Atacatorul poate crea un anunț care informează despre o afacere uimitor de mare pe site-uri clasificate, site-uri de licitații etc. De obicei, atacatorul deschide un cont de vânzător cu o evaluare bună pentru a minimiza suspiciunea dumneavoastră.

Dacă victima muscă momeala, va fi infectată cu software rău intenționat. De obicei, acest lucru generează acțiuni suplimentare împotriva victimei și a persoanelor de contact ale acesteia.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 3: Prevenirea ingineriei sociale

2.5: Rezumat

Desigur, toate scenariile menționate sunt doar exemple de tehnici de inginerie socială. Trebuie să ne amintim că atacatorul este o persoană inteligentă, orientată spre tehnologie, care a explorat tehnici de manipulare. Phishing, vishing și baiting sunt tehnici care pot avea scenarii nesfârșite. Totul depinde de ingeniozitatea și creativitatea atacatorului.

Verificați în mod regulat știrile pentru tehnicile actuale de inginerie socială pentru a rămâne la curent.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 3: Prevenirea ingineriei sociale

3.1: Ce să faceți și ce să nu faceți

După cum puteți vedea, tehnicile de inginerie socială sunt eficiente deoarece se bazează pe manipulare psihologică, lipsă de conștientizare și cunoaștere adecvată. Întregul atac se poate întâmpla numai dacă victima este susceptibilă la mecanismele alese.

Deci, ce puteți face pentru a preveni atacurile de inginerie socială?

Creșteți gradul de conștientizare a activităților rău intenționate în rândul dvs., al angajaților, al partenerilor și al clienților. Amintiți-vă că tehnicile de inginerie socială se schimbă în timp și spațiu, așa că este necesar să vă actualizați cunoștințele în mod regulat.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 3: Prevenirea ingineriei sociale

3.1: Ce să faceți și ce să nu faceți

Învățați-vă angajații, partenerii și clienții cât de valoroase sunt parolele și datele sensibile. Amintiți-vă că o postare amuzantă pe Facebook în care sunteți întrebați despre data nașterii poate fi folosită împotriva dumneavoastră. Gândiți-vă de câte ori ați folosit data nașterii într-o parolă.

Nu păstrați toate datele sensibile și informațiile cruciale într-un singur loc. Dacă atacatorul este capabil să le fure cu un simplu printscreen, trebuie să lucrați la sistemul dvs. de securitate.

Nu accesați niciun link și nicio imagine înainte de a verifica sursa.
Chiar dacă sursa pare familiară, nu vă grăbiți. Aruncați o a doua privire la un e-mail adresă, IP, link etc.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 3: Prevenirea ingineriei sociale

3.1: Ce să faceți și ce să nu faceți

Pregătiți standarde transparente de securitate pentru compania dvs. Planificați protocolul în caz de atac și învață-ți angajații, partenerii și clienții ce să facă.

Nu provocați teamă inutilă în rândul angajaților, partenerilor și clienților. Frica îl ajută pe atacator să manipuleze oamenii. Conștientizarea și cunoașterea sunt opusul.

Sunteți pregătit să faceți față tehnicilor de inginerie socială?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bibliografie și link-uri utile

European Commission > **What personal data is considered sensitive**

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Webroot > **What is Social Engineering? Examples & Prevention Tips**

https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Seon > **What is Social Engineering? Attacks, Techniques & Prevention**

https://seon.io/resources/protect-against-social-engineering-attacks/?utm_term=&utm_campaign=%5BS%5D%20Blog%20-%20dynamic%20%5BEMEA%5D&utm_source=google&utm_medium=cpc&hsa_acc=9367189488&hsa_cam=12655034312&hsa_grp=119030291966&hsa_ad=511148698722&hsa_src=g&hsa_tgt=dsa-41475539813&hsa_kw=&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwvuGJBhB1EiwACU1AibG5GowOFa1Q_FazH8_RDbrb3OEI7k7fQacOcLKrty9ZFQw-b7i_7hoCDWcQAvD_BwE

Imperva > **Social Engineering**

https://www.imperva.com/learn/application-security/social-engineering-attack/

Verizon > Data Breach Investigations Report > **2021 DBIR Master's Guide**

https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Terranova Security > **9 Examples of Social Engineering Attacks**

https://terranovasecurity.com/examples-of-social-engineering-attacks/

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Mulțumim pentru atenție!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.