Social Engineering Case: USB-fælden ved højvandslukket

# 🧠 Formål

At illustrere, hvordan social engineering – specifikt et fysisk angreb via impersonation og USB-drop – kan udnytte tillid, teknologisk uvidenhed og sociale relationer til at kompromittere en persons eller virksomheds digitale sikkerhed.

# 📘 Baggrund

Urban Water Solutions (UWS) er en mindre virksomhed, der arbejder med installation og service af højvandslukkere. Lars er tekniker og medejer og har for nylig deltaget i en fagmesse for tekniske løsninger til kloaksystemer.

På messen kommer en observant deltager i snak med Lars og får ubevidst indsigt i hans kundekreds. Ved efterfølgende research finder deltageren frem til Christian Mikkelsen, en formodet velhavende kunde, som har fået installeret en højvandslukker på sin ejendom.

# 🎭 Angrebsscenarie

## 🎯 Mål

• Primært mål: Kompromittere Christians private netværk og evt. få adgang til følsomme oplysninger.

• Sekundært mål: Indsamle data om Urban Water Solutions via Christians kommunikation eller dokumenter.

## 📌 Faser i angrebet

1. Informationsindsamling (Reconnaissance):  
- Research af Lars virksomhed via hjemmeside, LinkedIn, fagfora.  
- Profilgennemgang af Christian Mikkelsen på sociale medier (Facebook, Instagram).  
- På Instagram ser angriberen, at Christian ofte arbejder hjemme om onsdagen. Angriberen planlægger derfor at ringe på en onsdag formiddag.

-Fund af telefonnummer på Christian Mikkelsen på krak.dk via hans navn og adresse

2. Udformning af narrativ (Pretexting):  
Angriberen udgiver sig for at være Lars og ringer til Christian:  
  
"Hej Christian. Det er Lars fra Urban Water Solutions. Jeg ved godt, at det er ved at være noget tid siden, at jeg installerede højvandslukkeren ved dig, men jeg har ledt med lys og lygte efter et USB-stik lige siden. Sidst jeg havde det, var på dagen, hvor jeg var forbi dig. Er du tilfældigvis hjemme og kan tjekke, om der ligger et stik derude?"  
  
(…) Christian finder stikket  
  
"Fedt! - Nu har det lagt der et stykke tid, har du mulighed for at tjekke, om det stadig virker? Det er ret vigtigt, at jeg får dem, så har du mulighed for at tjekke, om de stadig virker og så sende dem til min private mail?"  
  
Angriberen har oprettet en falsk e-mailadresse, der ligner en privat mail. Fx. LarsJes78@hotmail.com

3. Levering (Delivery):  
- USB-stikket er forudprogrammeret med fx HID-malware eller keylogger.

4. Udnyttelse (Exploitation):  
- Når USB-stikket sættes i, aktiveres koden og forsøger at etablere forbindelse til angriberens server.

5. Ekfiltration (Exfiltration):  
- Data sendes til angriberen – fx adgang til dokumenter, netværk, adgangskoder.

# ⚠️ Social Engineering Elementer

|  |  |
| --- | --- |
| Element | Beskrivelse |
| Impersonation | Angriberen udgiver sig for at være en betroet tekniker. |
| Trust Exploitation | Bygger på tidligere møde og Christians tillid til 'Lars'. |
| Authority(identitetstyveri) | Lars har ekspertstatus som tekniker – skaber automatisk tillid. |
| Urgency | Skaber presset situation: tabt data, haster. |
| Human Curiosity | Fristelsen for at se, hvad der er på USB-drevet(hvis det bliver opdaget uden kontakt) |
| Physical Attack(USB-Baiting) | Brug af fysisk enhed til digital kompromittering. |

# 💡 Forslag til udvidelser

1. Teknisk opsætning: valg af malware (Rubber Ducky, keylogger, reverse shell).  
2. Eskalering: Kan malware bruges til at inficere andre systemer?  
3. Forebyggelse: Hvordan kunne Christian have undgået det? Awareness-træning?  
4. Analyse: SWOT-analyse og vurdering ift. CIA-triaden.

# 🔐 Etisk Refleksion

• Hvor går grænsen mellem awareness og manipulation?  
• Hvilket ansvar har virksomheder som Urban Water ift. kundesikkerhed?  
• Hvordan kan samfundet forebygge denne type angreb?