UNGA FORSKARE

PROJEKTINSPIRATION FÖR GYMNASIEARBETET

SKYDDA MOT PHISHING

Teknik, IT, IT-säkerhet, ”social engineering”, cybersäkerhet i samhället, ingenjör, psykologi

Projektidé från **IBM**, International Business Machines Corporation

INTRODUKTION

IT-säkerhet är oerhört viktigt för många företag och organisationer. Speciellt är man orolig för att hackare, tex kopplade till främmande länder och statliga aktörer, ska lyckas komma över känslig information om vårt samhälle och demokrati.

Ett vanligt tillvägagångssätt som en hacker använder sig av för att bryta sig in i en organisation är genom så kallade phishing-attacker. Phishing är en del av det som brukar benämnas ”social engineering” inom IT-säkerhet. I stort så går det ut på att lura en eller flera personer till att till exempel klicka på en länk, öppna en bifogad fil eller dela med sig av känsliga uppgifter. Varianter av Phishing (och även social engineering) som det ibland går att läsa om är till exempel:

- Spear phishing – en riktad phishingattack mot en specifik individ. Ofta måste en hacker lägga mycket förarbete för att kunna göra en sådan attack. Spear phishing är därför ofta ”lyckade” ur en hackers synpunkt och innebär därmed en stor risk för företag och organisationer.
- Smishing – phishing över sms eller meddelandetjänster
- Vishing – fejkade telefonsamtal. Tex någon som ringer och utger sig ringa från en bank eller liknande
- Whaling eller Business Email Compromise (BEC) – där en hacker utger sig för att vara till exempel en chef eller VD för att få anställda på ett företag att utföra någon handling, ofta att överföra pengar till hackerns konto.

PHISHING

Ofta används phishing-attacker mot vanliga användare just för att hackers vet att den mänskliga faktorn är det som vanligen ligger bakom en it-säkerhetsincident. Att utbilda människor i hur dom kan identifiera phishingmail (och social engineering) är därför extra viktigt.

UNGA FORSKARE

PROJEKTINSPIRATION FÖR GYMNASIEARBETET

Det finns ett behov av att ta fram bra och förståelig information på svenska kring hur man kan identifiera till exempel phishingmail, hemsidor eller telefonsamtal. Som förslag så kan utbildningsmaterialet rikta sig till företag, myndigheter och organisationer, eller till elever på gymnasiets olika program.

Undersök några vanliga metoder inom det som kallas social engineering och phishing. Undersök både tekniska sätt och icke tekniska sätt som en person kan identifiera dessa tekniker. Några exempel att undersöka är:

ICKE-TEKNISKT

- Kolla på vad som typiskt brukar utmärka ett phishing eller spear phishing-mail.
    - Språket? Hur är det skrivet? Frågas det efter känsliga uppgifter? Länkar eller bifogade filer? Är det bråttom? Har användaren förväntat sig att få detta meddelande?
- Vad kan en person göra för att verifiera om ett misstänkt phishingmeddelande är riktigt eller ej?
    - Exempelvis ringa upp avsändaren och dubbelkolla?

MELLANTEKNISKT

- Hur kan en användare se på länkar och bifogade filer om det är misstänkt phishing det rör sig om? Vart leder länken? Vad är det för typ av fil bifogad? Är det dem hemsida jag förväntar mig?
- Intervjua en IT-säkerhetstekniker kring social engineering och phishing.
    - Vad för skada kan social engineering och phishing orsaka?
    - Vad kan det kosta för en organisation som blir utsatt?
    - Hur skyddar sig organisationen/företaget?

TEKNISKT

- Mailheaders, domännamn och ip-adresser. Går det att göra ”lookups” för att se var ett mail egentligen kommer ifrån?
- Hur kan en person identifiera att en hemsida är fejk? Tex en fejkad inloggningssida till en bank?

Baserat på det du finner från ovan, ta fram ett utbildningsmaterial bestående av exempel och tips riktade till den målgruppen du väljer. Hitta några testpersoner i målgruppen och utvärdera materialet på dem.

KÄLLOR/MATERIAL

- https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba202/1591164566288/Rapport-Cybersakerhet-Hot-Metoder-Brister.pdf
- https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba203/1591164566364/Rapport-Cybersakerhet-Rekommenderade-Atgarder.pdf

- https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/natfiske-phishing-/
- https://omni.se/tv4-avslojar-brister-i-kriminalvardens-it-system-anmals-av-myndigheten/a/8mynqx
- https://dl.acm.org/doi/abs/10.1145/1242572.1242660
- https://dl.acm.org/doi/abs/10.1145/1124772.1124861
- https://www.aftonbladet.se/nyheter/a/P3ORwR/swedbank-varnar-ny-vag-av-bluffmejl
- https://scholar.google.com/scholar?hl=sv&as_sdt=0%2C5&q=social+engineering+attacks&btnG=&oq=social+engineer

KOPPLING TILL AKTUELLA FORSKNINGSOMRÅDEN OCH ARBETSMARKNAD

Phishing är ofta svårt att skydda sig mot då det kan vara väldigt sofistikerat, till exempel s.k. ”spear phishing”. Oftast är det upp till individen att själv kunna identifiera dessa typer av attacker för att helt enkelt inte låta sig luras av dem. Phishing som är en underkategori under det som kallas social engineering, antas kunna kopplas till en majoritet av alla IT-säkerhetsincidenter. Företag och organisationer har därför mycket att tjäna på att deras anställda (och medlemmar) har kunskap för att inte falla för phishing och andra typer av social engineering-attacker.