MISSION 3: FIND STØRRELSEN PÅ DINE DIGITALE FODAFTRYK

Vi hører ofte, at vores digitale handlinger på internettet afsætter spor, som andre kan registrere og fortolke. Mange af disse spor registreres passivt af søgemaskiner, sociale medier og lignende for at kunne bruges til målrettet markedsføring. Men de informationer, der registreres og gøres tilgængelige på internettet, kan også bruges aktivt, for eksempel i forbindelse med "**social engineering**" og "**spear phishing"**, hvor personlige informationer om offeret kan hjælpe med at målrette angrebet.

SOCIAL ENGINEERING

Social engineering er en metode, hvor en person manipulerer eller udnytter psykologiske og sociale faktorer for at få adgang til fortrolige oplysninger eller til at udføre uønskede handlinger. Det er en form for angreb, der fokuserer på at udnytte menneskelig adfærd i stedet for tekniske svagheder.

SPEAR PHISHING

Spear phishing er phishing, der er målrettet og personlig. I stedet for, at en phishing-e-mail sendes til mange mennesker, retter spear phishing sig mod specifikke enkeltpersoner eller organisationer. Angriberne bag spear phishing bruger ofte indsamlede oplysninger om deres mål, for eksempel navn, stilling, arbejdsgiver eller tidligere aktiviteter for at skabe en mere troværdig og målrettet phishing-kommunikation.

Mængden af direkte og indirekte personlige informationer, der er registreret om en person på internettet, kaldes ofte **personens digitale fodaftryk**; jo flere informationer, jo større fodaftryk.

JERES MISSION

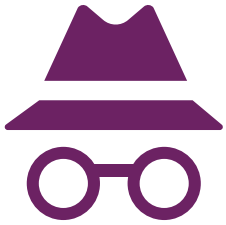
I denne mission skal I finde jeres digitale fodaftryk, dvs. de informationer, en angriber kan benytte til at fremstå imødekommende, have samme interesser eller på anden måde få offeret til at sænke sine parader overfor angriberens sociale manipulation.

Vi er alle forskellige og kan have meget forskellige digitale fodaftryk. Så i denne mission skal I finde jeres eget digitale fodaftryk, men I skal også sammenligne det med en jævnaldrende (for eksempel en af jeres venner) samt en meget ældre person, det kan for eksempel være et ældre medlem af jeres familie. Husk at spørge vennen og familiemedlemmet om lov først, da jeres interesse ellers kan virke som digital stalking.

Endelig skal I for hvert af de tre individer, I har undersøgt, identificere mindst én nøgleinformation, som I mener en angriber ville kunne benytte til at skabe en forbindelse og få jer selv, jeres ven og jeres familiemedlem til at sænke paraderne og være mere åbne overfor en henvendelse.

SOCIAL MANIPULATION

Vi har som mennesker en stærk trang til at høre til en gruppe, hvilket gør os modtagelige overfor henvendelser fra andre, der udnytter en fornemmelse af fællesskab, for eksempel tilhører samme gruppe eller befinder sig i en lignende situation. Sociale manipulatorer benytter ofte denne lighed til at skabe forbindelse til offeret og få dem til at tro på den baggrundshistorie, der benyttes til manipulationen. Eksempler kunne være, at angriberen har nogle sjældne sneakers til salg, leder efter nogen til at lufte sin hund, har gået på samme skole som offeret, er fan af offerets yndlingsband, der skal spille på Roskilde Festival, o.lign. Der er mange muligheder, men det gælder for angriberen om at finde noget, offeret er passioneret omkring, og som antyder fælles interesser og værdier, som kan danne en åbning til offeret.



SÅDAN KAN DINE INFORMATIONER BLIVE UDNYTTET

Når hackere bruger social manipulation til at indsamle informationer om enkeltpersoner, kan de have flere formål med disse oplysninger:

Identitetstyveri: Hackere kan bruge de indsamlede oplysninger til at stjæle en persons identitet. Dette kan være at bruge personlige oplysninger til at oprette falske konti, åbne kreditkort i offerets navn eller udføre andre økonomiske svindelnumre.

Økonomisk svindel: Ved at kende offerets personlige og finansielle oplysninger kan hackere udføre forskellige former for økonomisk svindel. Dette kan være at tømme bankkonti, foretage falske transaktioner eller begå bedrageri i offerets navn.

Adgang til systemer: Hackere kan bruge indsamlede oplysninger til at få adgang til beskyttede systemer eller netværk. Ved at kende brugernavne, adgangskoder eller andre autentificeringsoplysninger, kan de narre eller omgå sikkerhedsforanstaltninger og få ulovlig adgang til følsomme data eller ressourcer.

Phishing-angreb: Med personlige oplysninger i hånden kan hackere skræddersy phishing-angreb og forsøge at narre offeret til at afgive yderligere fortrolige oplysninger eller udføre skadelige handlinger. Dette kan omfatte at sende målrettede e-mails eller oprette falske websteder, der ligner legitime tjenester eller organisationer.

Det er vigtigt at være opmærksom på disse risici og være forsigtig med at dele oplysninger!

DIREKTE OG INDIREKTE INFORMATIONER

Nogle informationer fortæller direkte, hvad offeret er interesseret i, for eksempel hobbyer, kæledyr, yndlingsmusik samt billeder og videoer taget på ferie eller af bedste venner, der har det sjovt sammen i en eller anden aktivitet. Disse informationer findes ofte på sociale medier, i vlogs eller blogs, hvor offeret fortæller om sig selv og sine oplevelser. Disse informationer kan angriberen bruge direkte til at skabe den ønskede åbning. Andre informationer fortæller indirekte noget om offeret og skal derfor fortolkes, for at angriberen kan udlede de informationer, der skal bruges til angrebet. Det kan eksempelvis være, at angriberen finder et offentligt tilfængeligt referat fra en generalforsamling i den lokale golfklub, hvor det er beskrevet, hvem der blev valgt til bestyrelsen. Dermed kan det forventes, at offret er en passioneret golfspiller, ligesom bestyrelsesposter i skoler eller daginstitutioner fortæller, at offeret har mindre børn.

PRIVATE OG OFFENTLIGE INFORMATIONSKILDER

Som antydet ovenfor er der mange forskellige informationskilder, som kan fortælle om det påtænkte offers interesser.

Mange af disse informationskilder stammer fra private virksomheder eller enkeltpersoner, der opsamler og formidler informationer om individer. Disse informationer stammer ofte fra personen selv, enten direkte gennem sociale medier, blogs og vlogs, eller indirekte gennem profilering af deres adfærd, for eksempel deres lokationsdata, søgehistorik eller cookies.

Andre informationskilder er offentlige systemer, der registrerer forskellige informationer om borgerne, som herefter offentliggøres. Dette kan eksempelvis være telefonbøger (for eksempel krak.dk), som kan vise

12

offerets adresse, tingbogen, der indeholder informationer om ejerskab og værdi af ejendomme, som fortæller noget om offerets indtægt (hvis ejendomsværdien er høj), kommunens weblager, som fortæller om bolig og byggesager, eller virksomhedsregistre (virk.dk eller proff.dk), som kan fortælle noget om virksomheder, som offeret kan eje eller lede. Der er mange andre typer offentlige registre, som offentliggør informationer, der kan bruges til at danne sig et billede af det påtænkte offer for social manipulation. Det drejer sig bare om at finde dem gennem forespørgsler til forskellige søgemaskiner.

Mange af de informationer, man kan finde gennem private informationskilder, kan offeret minimere gennem privatlivsfremmende teknologier eller ved simpelthen ikke at have profiler på sociale medier. De offentlige informationskilder drives ofte af myndigheder, som stiller informationer til rådighed, der ved lov skal være offentlige tilgængelige, så disse informationer er umulige for det påtænkte offer at holde hemmelige. Som privatperson er det derfor nyttigt at vide, hvilke typer af informationer myndighederne offentliggør om ens person og ejendomsforhold. Med den viden, kan man som borger bedre gennemskue om en, der udgiver sig for fra at være fra en offentlig myndighed, faktisk også er det, eller om vedkommende bare udnytter offentlig tilgængelige informationer.

JERES MISSION

Denne mission består af tre trin, som dokumenteres med en præsentation.

1

Find størrelsen af jeres digitale fodaftryk. Start med at se på, hvilke digitale informationer I selv lægger på nettet gennem sociale medier eller andre private informationskilder. Prøv så at se, om I kan finde jer selv i andre private informationskilder, for eksempel om I er tagget i billeder på Instagram, i videoer på TikTok eller blandt jeres "venner" på Facebook. I kan også kigge på likes på billeder og videoer, I har lavet. Endelig skal I undersøge, hvilke informationer I kan finde i offentlige informationskilder, ekesempelvis via en søgemaskine, på Aula eller jeres skoles hjemmeside, jeres fritidsaktivitet. Husk på, at Aula kræver login, så angriberen har måske ikke adgang til mange af disse informationer, mens skolens hjemmeside normalt er offentligt tilgængelig. Sammenlign jeres undersøgelser i gruppen og diskuter, hvad I er kommet frem til.

2

Der er typisk ikke mange informationer fra offentlige informationskilder i jeres aldersgruppe, men prøv at gennemføre de samme tre trin med et ældre medlem af jeres familie. Husk at spørge om lov først, da det ellers vil være at betragte som stalking.

3

Nu skal I analysere de informationer I har fundet om jer selv. Hvilke direkte informationer kan en angriber bruge til at udlede jeres præferencer? Hvad fortæller jeres online tilstedeværelse om jer selv og jeres liv? Og hvordan kan en angriber udnytte det til at blive fortrolig med jer og få jer til at sænke jeres parader? Er der også nogle indirekte informationer, for eksempel billeder fra en ferie, en koncert eller en festival, hvor en angriber kan komme tættere på ved at lade, som lade som om de har været til samme begivenhed? Det kan også være informationer om jeres præferencer gennem farven af jeres tøj (yndlingsfarve), plakater med musikere, sportsidoler eller lignende på billeder fra jeres værelser, osv.

4

Overvej, hvordan I ville bruge disse informationer til at indsmigre jer på jer selv. Skriv en dialog med jer selv, hvor I viser, hvordan angriberen benytter informationer fundet i jeres digitale fodaftryk og får jer til at sænke paraderne. Opfør evt. denne dialog som et rollespil, og lad det være en del af jeres præsentation.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres undersøgelse, hvor I redegør for missionen, fortæller om jeres proces med at finde frem til informationen om jer selv, samt præsenterer den information, I har fundet, og hvilke tanker I gør jer om det.

I præsentationen skal I:

- Redegøre for jeres mission og hvordan I har grebet opgaven an.
- Fortælle, hvilke typer af information I har fundet i jeres research, hvad der overraskede jer mest, og hvor I efterfølgende har gjort noget for at gøre information om jer selv mere privat.
- Analysere hvordan en evt. angriber vil kunne bruge den information, I har fundet, imod jer. Lav evt. en skærmoptagelse af den dialog, I har lavet, eller fremfør dialogen.
- Fortælle hvis I har anvendt nogle særlige metoder eller analyseredskaber etc.
- Præsentationen må max tage 5 minutter.

DELTAG I EN NATIONAL KONKURRENCE

Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den til Styrelsen for It og Læring. Alle videoer vurderes af Cybermissionens dommerpanel. Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.