MISSION 4: Digitale fodspor

Den online interaktion

De sociale medier er en integreret del af vores daglige liv. Det er her vi kommunikerer, deler nyheder, finder nye bekendtskaber og vedligeholder kontakten med folk, vi ikke ser så tit. At interagere på sociale medier er en essentiel del af vores sociale dannelse og relationer[1].

Den online interaktion betyder, at vi deler mange forskellige typer af data med hinanden, lige fra billeder, til tekst, videomateriale, links, lyd og meget mere. Desværre kan det materiale bruges af cyberkriminelle til at sammenstykke et billede af os og til at finde en sårbarhed, som de kan udnytte. Værktøjerne der bliver brugt af cyberkriminelle kan være alt fra dårlige links, der fører til forkerte websider, hvor vi skal angive vores personlige data og måske betale for noget. Det kan også være en personlig henvendelse på chat eller mail, der fortælle, at man har vundet i en konkurrence om et produkt, man virkelig gerne ville have, og hvor man bare skal oplyse bank, kreditkortoplysninger, data om hvor du bor eller andet. De profiler vi har på sociale medier, kan også i nogle tilfælde blive hacket og overtaget af andre. Når det sker, kan man opleve, at ens venner får underlige tilbud om ting, de har vundet, eller events de bør deltage i, som tilsyneladende er sendt fra dig. I stedet er det en cyberkriminel, der forsøger at få dig til at gøre et eller andet, som for eksempel sende en video af dig selv eller deltage i en falsk konkurrence.

Online kommunikation og interaktion er god for os, men desværre også god for cyberkriminelle, og det gælder om at få en god balance, hvor vi stadig kan være sociale online, men ikke serverer vores oplysninger og data til de cyberkriminelle.

[1] https://www.sst.dk/-/media/Udgivelser/2020/Digital-medie-brug-blandt-boern-og-unge/Digital-mediebrug-blandt-boern-og-unge.ashx

Databeskyttelsesordningen

I EU benyttes Databeskyttelsesforordningen (GDPR)[2] som gælder for alle de online services, vi modtager og bruger i EU. Generelt går forordningen ud på at stille krav til virksomhederne og deres brug af data, vi giver dem, således at de tænker på, hvordan de bevarer data, hvad de gør med det og hvem de deler det med. Samtidig har vi som brugere af de websider og apps bl.a. ret til at sige nej til, at ejerne må dele data med andre.
Som del af Databeskyttelsesforordningen skal virksomheder udarbejde en analyse over deres brug af data, beskrive processerne i og udenfor virksomheden som modtager og modificerer data og beskrive, hvor der er størst risiko for, at der kan ske noget med data (nogen kan få fat på det og bruge det uhensigtsmæssigt). Ligeledes skal virksomhederne overveje, hvad man kan gøre mod de sårbarheder, man finder ved virksomhedens databehandling. Noget data er mere vigtigt at se på end andet, og derfor skal man også se på en kategorisering af det data, man bruger i virksomheden.

Datatyper

Man skelner i Databeskyttelsesforordningen mellem data, der er identificerbar og data der ikke er det. Identificerbar betyder data, hvorfra man umiddelbart kan identificere en person (altså vide at det er præcist dig eller din ven, som data tilhører). Eksempler på identificerbar data er personnummer, adresse, betalingsoplysninger mm. I databeskyttelsesforordningen taler man om almindelige personoplysninger som navn, adresse, telefonnr. osv. og følsomme personoplysninger som helbredsoplysninger, biometrisk data, religion mm.
Det er klart, at man som person skal passe godt på alle typer af data, men at de følsomme personoplysninger skal have mere sikkerhed.

[2] https://www.datatilsynet.dk/hvad-siger-reglerne/lovgiving

Brug data med omhu

I missionen skal I arbejde med eksempler på data, som deles på sociale medier, samt nogle af de cybersikkerhedsangreb, vi kan blive ramt af.
I skal arbejde med forskellige opgaver, der viser, hvordan ukritisk deling af data på sociale medier kan være en stor sårbarhed.
Derefter skal I diskutere forskellige løsninger på, hvordan man kan forhindre at blive hacket, få delt sin data uhensigtsmæssigt eller falde i en "phishing"-fælde, uden at vi sætter vores behov for at være sociale online på spil.

Som del af missionen skal I løse en række forskellige opgaver på l**æringsplatformen Haaukins**, der giver mulighed for at arbejde med "etiske cybersikkerhedsangreb". Haaukins er en virtuel platform, der anvender et sikret miljø, og hvor man dermed kan se, hvad cyberkriminelle kan finde på uden at blive angrebet i det virkelige liv. På Haaukins er der et område med opgaver (challenges), der alle er knyttet til brug af kendte sociale medier. Missionen har et teknisk element, men ser dog mest på data og databeskyttelse. Når I arbejder på Haaukins platformen, kommer I ud for at skulle bruge forskellige tekniske redskabet, som I skal kunne anvende for at lede efter det data, som cyberkriminelle vil lede efter.

I denne mission skal I udarbejde en præsentation, der belyser nogen af de cybersikkerhedsproblemstillinger, man har som ung på de sociale medier, diskutere de dilemmaer der kan være med deling af forskellige data samt beskrive løsninger, der kan sikre, at vi kan være online uden at blive ramt af cyberangreb.

TRIN 0:
Registrering i Haaukins

For at kunne arbejde med Haaukins, skal I have et link af jeres underviser. Når I klikker på dette link, skal I registrere jer individuelt på platformen ved at trykke på "Sign Up" oppe i højre hjørne. Gå derefter til oversigten over challenges (Challenges) og vælg challengen i kategorien "Starters" ved navn "Sanity check-static". Når I har læst indholdet i opgaven, skal I trykke på "Connect" oppe i højre hjørne for at tilgå jeres virtuelle lab. I det virtuelle lab, skal I åbne Firefox og gå til siden "sanity-checks.hkn". Kopiér flaget og sæt det ind i submit feltet på challenge siden i jeres egen browser. Når I har gjort dette, er I klar til at starte på de egentlige opgaver i trin 1-3.

TRIN 1:
Log på haaukins og lav (mindst) 5 opgaver

På trin 1 arbejder I med 5 forskellige opgaver, der alle er knyttet til det at dele forskellige typer af data med hinanden på sociale medier. De 5 opgaver er:

1. Certified Secrets

Den første opgave omhandler hjemmesidecertifikater. Hvordan man får adgang til dem, hvilke data de indeholder, og hvad de kan fortælle omkring hjemmesiden. Opgaven skal vise, at der er mere bag hjemmesider, end hvad man kan se.

2. Meta

Vi kan nogle gange dele oplysninger helt uden at vide, at vi deler dem. Metadata er data om data. Når man f.eks. tager et billede, kan der blive lageret metadata i billedet omkring; hvor det er blevet taget, hvilket kamera det er taget med, og hvornår det er blevet taget. Denne opgave handler om, hvordan man kan få adgang til den information.

3. Peacock: En lang rejse

Det er ikke altid gennem tekst, at vi deler oplysninger. Denne opgave omhandler, de billeder vi deler, og de oplysninger som optræder visuelt på dem. Derfor er det også vigtigt at være bevidst om de informationer, som vi deler igennem de billeder, vi deler på sociale medier eller lign. For eksempel visuel information, der kan bruges til at finde ud af, hvor vi er.

4. Peacock: OSINT hack

Det er ikke altid os selv, der deler oplysninger om os. Familie eller venner kan f.eks. dele oplysninger, som kan være værdifulde i de forkerte hænder, da de f.eks. kan bruges til social engineering (hvor man forsøger at overtale personer til at gøre noget, der reelt er dårligt for dem eller andre, som at betale for en pakke man reelt ikke venter på, og hvor de kriminelle får oplysninger om dig og dit kreditkort, de kan bruge i andre sammenhænge). Denne opgave handler om, hvordan du kan få adgang til en brugers profil gennem information, andre har delt om brugeren.

5. Bad librarian

HTTPS der bruges i forbindelse med hjemmesider er en krypteret version af HTTP. Det vil sige, at hjemmesider der bruger HTTPS skaber en sikker forbindelse mellem din computer og en server, så andre ikke kan opsnappe f.eks. password eller bankkontoinformationer. Det gøres med nogle krypteringskoder, som smides væk efter brug, men hvad sker der, hvis de ikke smides væk og hvordan kan de udnyttes?

Når I har løst disse challenges, skal I diskutere, hvad I har lært og reflektere over andre typer af data, som I deler med andre.

TRIN 2:
Lav en sårbarhedsanalyse over jeres brug af forskellige typer af data på sociale medier

I gruppen skal I undersøge, hvor meget information I kan finde om hinanden ved kun at bruge offentligt tilgængelig information som f.eks. sociale medier og Google. I kan også undersøge, hvad familie/venner har delt om personen. Gem den information, I finder.

Gå derefter sammen og lav en sårbarhedsanalyse for hver af jer, hvor I identificerer, om I deler sårbar data eller ej, og om man kan identificere jer direkte fra data. Lav en sårbarhedsanalyse over forskelligt data, I deler, sender, downloader, producerer osv. og beskriv hvor det data sendes hen og hvem I deler det med. Overvej også hvilke virksomheder, som opbevarer din data, udfører dine kommandoer mm. Overvej, om den/de virksomheder deler dit data med andre virksomheder, og hvordan det kunne foregå. Tag udgangspunkt i jeres profil på et socialt medie og anvend det som eksempel. Brug gerne den indsigt, som I har opnået i trin 1 i analysen. Diskuter derefter, hvilke anbefalinger, I vil give unge på jeres egen alder, således at de både kan være sociale online og være bedst muligt beskyttet mod cyberangreb.

Haaukins

Haaukins er en virtuel læringsplatform, hvor alle med interesse for cybersikkerhed kan træne og forstå mere om emnet i et sikkert miljø. Filosofien bag platformen er, at man skal lære at tænke som en hacker for at forstå, hvad og hvordan man skal gøre for at komme de cyberkriminelle i forkøbet. I Haaukins skal man finde såkaldte flag. Flagene er visualiseret som en kode, og ser sådan ud: HKN{et_eller_andet_text}. Flagene kan findes i tekst, i koden på skærmen. Når man har fundet flaget, kopieres flaget til challenge-siden og flaget indsættes. Dermed bliver en challenge løst.

Sårbarhedsanalyse

Sårbarhedsanalyser kan udføres på forskellig vis. For at efterleve lovkravene i Databeskyttelsesforordningen, undersøger virksomheder typer af data, der bruges og sendes til andre, hvad der kan ske med det, og hvad sandsynligheden er for, at der sker noget, der ikke bør ske. Samlet set identificeres alle risici, og der arbejdes med dem, hvor risikoen for at data kommer i andres hænder er størst – altså de største sårbarheder. Dette kan bruges til at arbejde med forskellige løsninger, der kan mindske risikoen.

Udarbejd et skema over forskellige typer af data, I deler på sociale medier. Skemaet kan se ud som herunder:

SÅRBARHEDSANALYSE

Data og datatype	Proces (beskriv, hvad der sker med data – deles den til mange, til få, er der andre elementer, man skal tænke på)	Hvad kan der ske (giv eksempel på, hvad der kan ske)	Risiko for at der sker noget i processen (vurder gerne sandsynligheden for, at det sker og forklar, hvordan I er kommet frem til det)	Hvad skal der ske for at sikre, at det ikke sker (eller at det sker mere sjældent)
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-

Jeres præsentation

For at gennemføre missionen, skal I forberede en præsentation, hvor I redegør for, hvordan I har løst opgaverne. I skal også fremlægge jeres forslag til, hvordan I vil forhindre cyberkriminelle I at bruge jeres data på sociale medier, samtidig med, at I stadig kan være sociale online. I præsentationen skal I:

- Redegøre for jeres mission
- Fortælle, hvordan I kom frem til jeres endelige løsningsforslag
- Præsentere jeres løsninger (gerne med billeder, video, skærmoptagelse mm)

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.