CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

MISSION 4 – GØR DET MULIGT AT VÆRE EN GOD HACKER

I Denne mission skal I lære, hvordan virksomheder kan skabe de rette rammer for etisk hacking og dermed bidrage til at styrke deres egen IT-sikkerhed.

I skal sætte jer i et firmas sted og hjælpe dem med at lave det, der kaldes et Vulnerability Disclosure Program. Skulle man oversætte begrebet til dansk ville det være noget i retningen af et "Sårbarheds Offentliggørelses Program". I praksis er det dog altid den engelske betegnelse, der bruges og det gør vi også i denne mission.

Et Vulnerability Disclosure Program (VDP) har til formål at give etiske hackere, også kaldet white hat-hackere, klare retningslinjer for, hvordan de indberetter potentielt ukendte og skadelige sårbarheder til de organisationer, der står bag systemet, så de kan blive fixet, til alles bedste.

Hvis ikke der findes et VDP for et system, kan etiske hackere risikere, uforvarende, at komme til at gøre noget ulovligt. Læs for eksempel denne artikel på dr om forælderen Esben, der fandt en sårbarhed i børnehavernes pladsanvisningssystem: https://www.dr.dk/nyheder/penge/it-gigant-anmeldte-esben-hacking-nu-dropper-politiet-sagen

Esben blev meldt til politiet for at hacke, selvom hans intentioner var gode. Hvis sagen var gået videre, kunne Esben have fået alvorlige problemer med loven.

Der var i dette tilfælde brug for at ejeren af systemet havde haft en VDP, så Esben trygt kunne indberette sin viden om den givne sårbarhed – uden at være bange for at ende i fedtefadet.

JERES MISSION

I denne mission skal I se på, hvordan man håndterer hacking i det virkelige liv. I skal forestille jer, at I er blevet hyret af sikkerhedsafdelingen i et stort softwareselskab. I har fået til opgave, at lave et udkast til et Vulnerability Disclosure Program (VDP), da virksomheden ønsker at etiske hackere kan hjælpe med, lovligt, at finde og afsløre sårbarheder i virksomhedens systemer.

I skal vælge hvilket softwareselskab I gerne vil repræsentere – det kan enten være:

1. Det nye system for digital identitet/digital post
2. Et socialt netværk
3. Et videospil

Inden I går i gang med jeres VDP, så læs den følgende sektion for at forstå, hvorfor hacking er blevet et samfundsmæssigt fænomen, og hvordan I kan lave en VDP for det softwareselskab, I har valgt.

HACKING SOM ET SAMFUNDSMÆSSIGT FÆNOMEN

Der opstår hele tiden sårbarheder i software på grund af nye opdateringer, manglende opdateringer, nye funktionaliteter, uhensigtsmæssig brug af software m.m. Hackere har en stor interesse i at udnytte disse sårbarheder for at kunne lave et angreb.

Hacking er et stort samfundsmæssigt problem, hvor virksomheder, offentlige myndigheder og privatpersoner taber milliarder af kroner til hackere. Det kan eksempelvis være igennem virus, ransomwareangreb, phishing.

Hvis vi som samfund skal have en chance for at beskytte os mod hackerangreb, så er det vigtigt, at vi opnår samme faglige niveau som dem, der angriber os.

Vi skal derfor skabe gode rammer for at etiske hackere kan hjælpe med at lukke sårbarheder, fx med det formål at beskytte samfundet, uden at risikere at blive sagsøgt for det og ende i fedtefadet hos politiet.

Som inspiration til at løse jeres mission kan I fx. høre denne episode af DR podcasten Genstart. Her fortæller Jacob, der er studerende og professionel hacker, om den cyberkriminelle gruppe The Dark Side, om sin egen historie som professionel hacker og om, hvordan han sørger for at holde sig på den rigtige side af loven.

Link til podcast – episoden tager 23 min.: https://www.dr.dk/lyd/special-radio/genstart/genstart-2021-05-25

Se videoen om VDP'er under videomateriale på Cybermissionens hjemmeside:
https://cybermissionen.cyberskills.dk/

HVAD ER EN GOD VDP?

En god VDP hjælper virksomhederne, fordi den motiverer etiske hackere til, at indrapportere de sårbarheder de finder – fordi de ved, at de kan gøre det på lovlig vis uden at havne på den forkerte side af loven.

Hvis ikke man har en god VDP, betyder det måske, at sårbarhederne ikke bliver indrapporteret eller endnu værre, at de bliver solgt på det sorte marked.

En VDP hjælper også med at vise, at virksomhederne er ansvarsbevidste i forhold til deres egen sikkerhed, og ofte vil brugernes tillid blive øget.

Der findes flere metoder til at lave en VDP. I denne mission anvender vi "A Framework for a Vulnerability Disclosure Program for Online Systems" fra det amerikanske Justitsministerium. I kan læse hele framworket i pfd'en her: https://www.justice.gov/criminal-ccips/page/file/983996/download

VDP'en skal tydeligt beskrive tilladt adfærd vedrørende opdagelse og offentliggørelse af sårbarheder, således at risikoen for strafbare overtrædelser af loven reduceres.

Processen med at udarbejde en VDP består af fire trin, som beskrives nedenfor. I kan lade jer inspirere af processen og følge anbefalingerne til, hvordan man som virksomhed udarbejder en god VDP.

DE FIRE TRIN I EN VDP

TRIN 1

LAV EN PLAN FOR OFFENTLIGGØRELSE AF SÅRBARHEDER

Ved udarbejdelsen af en VDP skal I hjælpe virksomheden med at beslutte, hvilke aktiver, altså det der har værdi for virksomheden, der skal medtages i planen. Skal det være alle aktiver eller udvalgte?

Denne beslutning kan være påvirket af flere faktorer, herunder om det undersøgte system behandler følsomme oplysninger, om nogle sikkerhedsforanstaltninger allerede er på plads, virksomhedens evne til at opdele netværket, lovgivningsmæssige og kontraktlige forpligtelser osv.

Virksomheden bør afgøre, om VDP'en skal skelne mellem typer af sårbarheder, fx softwarefejl, dårlig adgangskodestyring, fejlkonfigurerede systemer, social engineering.

TRIN 2

PLAN FOR ADMINISTRATION AF VDP

I trin 2 skal I beslutte, hvordan sårbarheder skal rapporteres. Først og fremmest hvilken e-mailkonto inde i virksomheden, de etiske hackere skal kontakte. Det skal helst være en mailadresse med et alias i stedet for en personlig konto, for eksempel security@example.org.

Desuden bør I beslutte, hvordan sårbarhederne skal indberettes. Hvilke oplysninger skal der gives? Hvad er rapportens forventede kvalitet? Skal der fremlægges et proof of concept, som viser, hvordan man udnytter sårbarheden?

Sammen med oplysninger om selve rapporten skal I angive tidsrammen for rapportering. Skal det ske ved opdagelse, eller når sårbarheden er fuldt valideret?

Endelig bør I beslutte, hvordan I ønsker at håndtere overtrædelser af VDP'en, både dem der er sket i god tro og bevidste overtrædelser i ond tro.

TRIN 3

LAV ET UDKAST TIL JERES VDP

Når I laver udkastet til jeres VDP-dokument, er det vigtigt, at I får beskrevet autoriseret og uautoriseret adfærd i enkle, letforståelige betingelser, så udefrakommende kan forstå det.

I skal derfor identificere netværkskomponenter eller data i den politik, der er inden for rammerne af planen, så specifikt som muligt. I skal beskrive, hvordan man identificerer oplysninger, der ikke er inden for rammerne af programmet.

Det er også vigtigt at forklare konsekvenserne af at overholde og ikke overholde politikken. Det er f.eks. nyttigt at overveje følgende formuleringer:

1. Organisationen vil ikke anlægge sag for utilsigtede overtrædelser af sin politik i god tro eller indlede en klage til retshåndhævelse for utilsigtede overtrædelser.
2. Organisationen anser aktiviteter, der udføres i overensstemmelse med politikken, for at udgøre "autoriseret" adfærd i henhold til loven om computerbedrageri og misbrug.
3. Hvis der anlægges sag af en tredjepart mod en part, der har overholdt politikken for afsløring af sårbarhed, vil organisationen tage skridt til at gøre det kendt, enten for offentligheden eller for retten, at personens handlinger blev udført i overensstemmelse med politikken.

Endelig skal I huske at nævne at etiske hackere skal kontakte organisationen for at få en afklaring, før de deltager i en adfærd, der kan være uforenelig med eller ikke er adresseret af politikken (VDP'en).

TRIN 4

IMPLEMENTÉR PLANEN OG SKAB KENDSKAB

Når I har et dokument, der klart beskriver jeres VDP, skal I hjælpe virksomheden med at gøre det bredt tilgængeligt. Der kan for eksempel linkes til den direkte på virksomhedens hjemmeside. Det anbefales også at reklamere for VDP´en på passende steder. Det skal I også hjælpe virksomheden med. Hvordan vil I kommunikere og gøre jeres VDP tilgængelig for relevante parter?

Et brugbart sted at reklamere for virksomhedens VDP er de såkaldte URI'er eller "well-known URIs". Velkendte URI'er er en standardplacering på et websted for at gemme brugbare oplysninger om virksomhedens sikkerhedspolitik. Hvis virksomhedens hjemmeside er www.example.com, kunne det eksempelvis være på følgende URL at man gemte sin VDP: https://www.example.com/.well-known/security.txt.

INSPIRATION FRA ANDRE VDP'ER

Når I udarbejder virksomhedens VDP, kan I lade jer inspirere af de allerede eksisterende politikker om vulnerability disclosure. I kan google jer frem til en del på hjemmesiderne HackerOne eller BugCrowd.

I kan starte med at kigge på Dropbox vulnerability disclosure document på linket her: https://hackerone.com/dropbox

JERES PRODUKT

Det er op til jer, hvordan I udformer virksomhedens VDP. Det kan være et skriftligt produkt, en slide-præsentation, en video-præsentation eller noget helt andet.
Forsøg at følge de fire trin så godt som I kan. I må meget gerne inkludere jeres argumenter for, hvordan I er nået frem til den givne VDP.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres VDP, hvor I redegør for missionen og fortæller om jeres proces med at udarbejde VDP'en. I præsentationen skal I:

- Redegøre for jeres mission og den virksomhed, I har valgt at arbejde for
- Præsentere jeres VDP (gerne med billeder, video, skærmoptagelse m.m.)
- Fortælle, hvordan I har anvendt alle eller dele af de fire trin til at lave jeres VDP
- Argumentere for, hvilken effekt I tror, at jeres løsning kan få hos jeres virksomhed
- Præsentationen skal være kort og 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 ind 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.

"EN VDP GIVER ETISKE HACKERE RAMMER FOR AT HJÆLPE VIRKSOMHEDER MED AT FORBEDRE DERES IT-SIKKERHED."

CYBERMISSIONEN

BEGREBSLISTE

Hvor mange begreber kender I?

TRUSSELSMODELLERING

Trusselsmodellering handler kort fortalt om at identificere sårbarheder i et system og dermed også uønskede hændelser, så man eksempelvis som udvikler af et stykke software kan være bedre forberedt.

COOKIES

En cookie er en fil, der bliver gemt på din computer, når du besøger en hjemmeside. Nogle cookies er nødvendige for at hjemmesiden virker, andre husker hvad du klikker på, så hjemmesiden kan sende reklamer, som passer til dig. Når du besøger en hjemmeside, kan du vælge hvilke cookies du vil acceptere.

CYBER AWARENESS

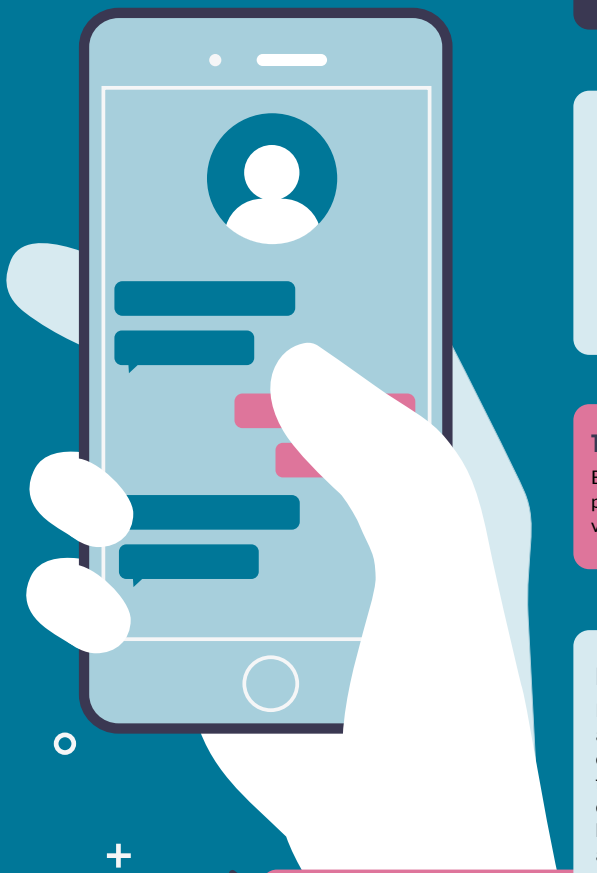
Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationssikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

DIGITALE FODSPOR

Når du søger på Google, sender en snap eller uploader en video på TikTok efterlader du dig spor på nettet, som bliver gemt. Det kaldes digitale fodspor, og de kan være meget svære at slette igen.

HACKING

Hacking er, når nogen ulovligt skaffer sig adgang til andres data - eksempelvis via en computer. Hackere udnytter svagheder i systemer. En svaghed kan eksempelvis være passwords, der er nemme at gætte.



DDOS-ANGREB

DDos-angreb står for Distributed Denial of Service. Det er et digitalt angreb, hvor en hacker med vilje overbelaster en hjemmeside eller en it-service, så siden i en periode er utilgængelig eller bryder helt sammen. Angrebet udføres ved, at hackeren gennem et netværk af virusinficerede computere, et såkaldt botnet, sender en stor mængde forespørgsler til hjemmesiden og dermed får siden til at bryde sammen.

VULNERABILITY DISCLOSURE PROGRAM

En VDP giver etiske hackere klare retningslinjer for, hvordan de indberetter potentielt ukendte og skadelige sårbarheder til de organisationer, der står bag systemet.

TO-FAKTOR LOGIN

To-faktor login er en dobbelt lås, som typisk består af dit password og en kode, du får tilsendt - ofte på sms. Hvis andre får fat i dit brugernavn og password og forsøger at logge ind på din konto, kan det derfor ikke lade sig gøre, fordi de mangler den anden kode, som er sendt til din mobil.

TROLL

En troll (på dansk: internettrold) er en person, som bevidst forsøger at fremprovokere vrede og had på internettet.

RISIKOANALYSE

En risikoanalyse er et værktøj, som har til formål at afdække potentielle risici ved at kategorisere dem ift. den mulige konsekvens og sandsynlighed for, at de indtræffer. Risikoanalysen anvendes dernæst til at prioritere ressourcer og beslutte hvilken handling, der skal sættes ind for at sikre, at det ikke går galt.

PHISHING

'Phishing' er, når it-kriminelle bruger falske e-mails, links eller hjemmesider til at få fat i andres private oplysninger, eksempelvis til banken. Det er tit svært at se forskel på, hvad der er falske links, mails og hjemmesider, og hvad der er ægte.

Kan I finde flere ord?

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING

CYBER SKILLS

CYBERMISSIONEN

BØRNE- OG
UNDERVISNINGSMINISTERIET
STYRELSEN
FOR IT OG LÆRING

CYBER SKILLS