CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

MISSION 3: TÆNK SOM EN HACKER

Du har måske hørt om den forhøjede trussel, der er overfor specielt kritisk infrastruktur i Danmark lige nu. Kritisk infrastruktur omhandler sektorer som: sundhedssektoren (herunder hospitaler), energisektoren, IT- og teleområdet, transportsektoren og fødevareområdet. Der er frygt for, at hvis et eller flere af områderne udsættes for hackerangreb, kan dele af det danske samfund bryde sammen.

Det kan have store konsekvenser at blive udsat for et hackerangreb, uanset om man er et transportfirma eller en gymnasieelev. Derfor er det vigtigt at få indsigt i, hvordan cyberkriminelle arbejder, da det giver bedre forudsætninger for at modstå angreb.

HVIS MAN VED, HVORDAN DE CYBERKRIMINELLE ARBEJDER, ER DET LETTERE AT BESKYTTE SIG

Der er mange forskellige veje til at få adgang til en computer, et netværk eller lignende. Typisk gør hackerne det, at de leder efter smuthuller i den måde et stykke software, et netværk eller en computer er sat op på. De ser med andre ord på, hvor svaghederne i systemarkitekturen er, og de forsøger så at finde det svageste punkt og planlægge, hvordan de kan udnytte det til egen fordel. Hackere bruger deres viden om svaghederne til at bryde ind i systemerne og tiltvinge sig adgang til data eller andet som er af interesse. Ydermere arbejder de cyberkriminelle også med at finde sårbarheder, så de kan blokere andres adgang til systemet og måske endda omdirigere til et andet system (for eksempel en falsk hjemmeside), som brugerne tror er den rigtige. På den måde kan man let blive snydt.

JERES MISSION

I denne mission skal I arbejde som hackere for at forstå, hvilke typer af sårbarheder, man som hacker kan lede efter, når man vil finde et godt sted at slå til. Ligeledes skal I reflektere over, hvad I lærer, og se om I kan finde eksempler på løsninger, som allerede bruges. Der arbejdes i denne mission med det, som kaldes "etisk hacking". I skal bruge en virtuel platform som hedder Haaukins, hvor man kan tillade sig at hacke, uden at det kommer ud i den virkelige verden og bliver til en kriminel handling. Man må ALDRIG hacke rigtige hjemmesider, profiler på sociale medier osv., - det er ulovligt! Missionen har et teknisk element og vi anbefaler, at du har motivation for at arbejde med teknologi, programmering (i det små) og forstå lidt om hvordan internettet virker og hvordan IT-systemer er opbygget.

I denne mission skal I udarbejde tre forslag til sikkerhedstiltag, på baggrund af de erfaringer I får når I selv skal prøve at hacke og forberede en præsentation af dem.

MISSIONENS 4 TRIN

På trin 0 lærer I om Haaukins-platformen, som er den digitale cybersikkerhedsplatform, I skal bruge til etisk hacking.
På trin 1, 2 og 3 arbejder I med eksempler på sårbarheder. I bruger Haaukinsplatformen til at forsøge at hacke jer til løsninger mens I reflekterer over, hvad I har lært og hvordan de sårbarheder I ser, kan undgås.

TRIN 0

LÆR HAAUKINS PLATFORMEN AT KENDE

På trin 0 skal I lære om Haaukins-platformen, hvordan den ser ud og hvordan man navigerer på den. I skal også lære om Linux, som er det operativsystem, man bruger på platformen. Eksempler på andre operativsystemer er Windows og MacOS.

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 den første challenge i kategorien "Starters" ved navn "List and Read". 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 en terminal (Kan findes i bjælken i bunden af det virtuelle lab) og følge de instruktioner, som nævnes i udfordringens beskrivelsen. Når I har løst den første opgave skal I løse de næste opgaver i rækkefølge. Følg ellers vejledningen på skærmen. Google er jeres ven! Når alle opgaver er løst, kan I starte på de egentlige opgaver i trin 1-3.

I finder en kort video til, hvordan I kommer i gang med Haaukins under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/

TRIN 1

LOG PÅ HAAUKINS PLATFORMEN OG LAV 2 OPGAVER

På trin 1 får I indblik i, hvad det vil sige at udføre etisk hacking. I lærer om de forskellige muligheder cyberkriminelle har for at hacke et system. I den challenge, der hedder *Cookiesession*, skal I lede efter cookies og se, om der er information i dem, der kan bruges til noget. Og i den challenge, der hedder *Adminlogin* skal I se, hvad der er af muligheder, når man har forsøgt at sætte lidt cybersikkerhed op, men kun har gjort det i cookies.

Når I har løst begge challenges, skal I reflektere over, hvad I har lært og hvilke løsninger, der kan være til at forhindre, det I lige har gjort.

TRIN 2

GIV ET BUD PÅ, HVAD CYBERKRIMINELLE SØGER EFTER

Løs nu den challenge, der hedder: *Cross site request forgery*, hvor man skal forsøge at hacke en bank.

Når denne challenge er løst, skal I tænke over, hvad I har lært af denne opgave, samt om I kan pege på sikkerhedsforanstaltninger, som kan forhindre pengebedrageriet.

TRIN 3

UNDGÅ HACKING – HVORDAN?

Løs nu den sidste challenge med navnet: *FTP server Login*, hvor man skal forsøge at gætte et password. Kan denne challenge bruges til at forstå, hvad man kan gøre for at reducere sandsynligheden for hacking? Prøv at snakke om hvorvidt to-faktor-login kan være en måde at sikre, at dette ikke sker. Begrund svarene.

BAGGRUND FOR TRIN 1-3

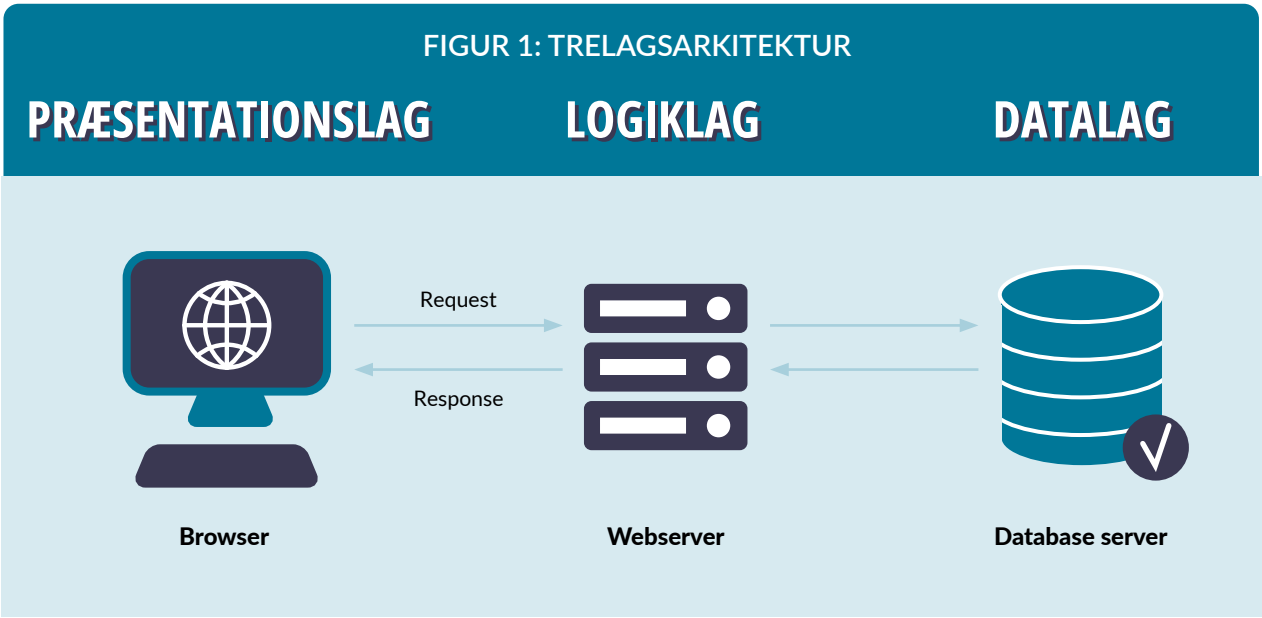
For at I kan arbejde med opgaverne i trin 1-3 skal I vide noget om trelagsarkitektur og om Haaukinsplatformen. Det er beskrevet herunder.

TRELAGSARKITEKTUR

Mange systemer, eksempelvis hjemmesider, består af en trelagsarkitektur: Et præsentationslag, et logiklag og et datalag. Se Figur 1.
Præsentationslaget er den pæne brugerflade med billeder, tekst, grafik osv. som brugeren navigerer i. Det er også her, man eventuelt logger ind på en hjemmeside. Logiklaget modtager information fra præsentationslaget, det kan være indtastninger, klik mm. Afhængig af, hvad kommandoerne er, kan der i logiklaget laves nogle beregninger eller sendes/hentes data fra datalaget. I datalaget opbevares data, man kan søge på data, og data kan sendes til logiklaget.

Hacking kan ske i alle lag. I de opgaver, I møder i denne mission, er der forskel på, hvor svaghederne skal findes. Du skal derfor forvente både at kigge på kode i logiklaget og data fra datalaget.

FIGUR 1: TRELAGSARKITEKTUR



HAAUKINSPLATFORMEN

Haaukins er en virtuel læringsplatform, hvor alle med interesse i 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 challengesiden og flaget indsættes. Dermed bliver en challenge løst.

Haaukins anvender Kali Linux som operativsystem og for at tilgå opgaverne skal man kende lidt til forskellige Linuxkommandoer, der kan være relevante at bruge i opgaverne. Når I arbejder med trin 0 lærer I om operativsystemet Linux og det virtuelle miljø, som Haaukins består af.

FORSKELLIGE TYPER AF HACKERANGREB

De challenges som I arbejder med i denne mission, beskriver forskellige typer af cybersikkerhedsangreb. Herunder kan I læse om angrebene og de forskellige challenges.

I opgaven *cookiesession* leder I efter en mulighed for at logge ind på en hjemmeside med en andens login og password. En af mulighederne er at kikke i cookies. En cookie er et stykke data, som man som bruger på en hjemmeside har med sig og giver til hjemmesiden automatisk. Den kan indeholde diverse informationer om brugeren, som hjemmesiden for eksempel bruger til at give selve brugeren adgang deres profil.

I opgaven *adminlogin* leder I efter en mulighed for at logge ind som administrator på hjemmesiden. Der er forskellige muligheder for det, som for eksempel at prøve sig frem og se, om der er en cookie, som indeholder den nødvendige information.
Både cookiesession og adminlogin illustrerer nogle af de problemer, mange brugere har, når password og login information ikke er sikret godt nok.

Opgaven Cross site request forgery er et eksempel på et cybersikkerhedsangreb med samme navn. Her opretter den cyberkriminelle et websted, som på grund af en svaghed i nogle websider, kan knyttes til en "rigtig" hjemmeside, som alle bruger. Det kan eksempelvis være en hjemmeside, som bruges i en fodboldklub eller en bank. Når den cyberkriminelle har udført sit angreb, kan han/hun eksempelvis tvinge brugeren til at skifte password, som så kan opfanges af den cyberkriminelle. Således kan den cyberkriminelle få adgang til hjemmesiden og begå kriminalitet.

I *FTP server login* kan man se, hvor nemt det er at gætte sig til et password. Dette angreb kaldes "brute force", fordi man bare prøver og prøver indtil man det lykkes.

JERES PRODUKT

For at gennemføre missionen, skal I forberede en præsentation, hvor I redegør for hvordan I har løst opgaverne og samtidig fremlægger jeres tre forslag til, hvordan I ville forhindre ondsindede hackere I at gøre det samme som jer. 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)
- Komme med eksempler på, hvordan I kan overføre den viden, I har fået i opgaverne, til andre systemer/ sårbarheder
- 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 upload-funktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

"VÆR OPMÆRKSOM PÅ, AT HACKING KAN SKE I ALLE TRE LAG AF SYSTEMARKITEKTUREN."

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

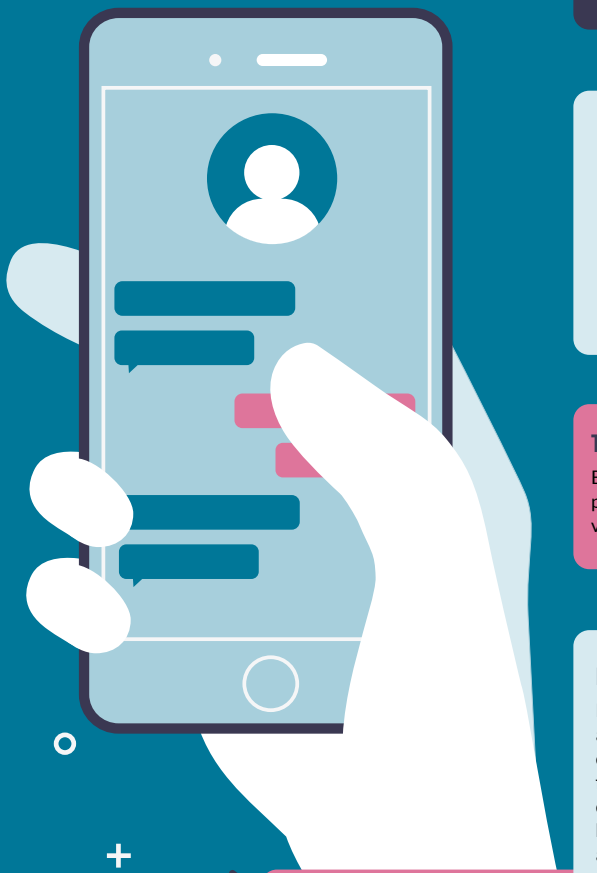
Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationssikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

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