CYBERMISSIONEN

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

MISSION 5 – (U)SIKKERHED I SMART HOME ASSISTANTS

Smart home assistants som for eksempel Amazon Alexa, Google Assistant eller Appels Siri bliver mere og mere udbredte i hjemmene hver eneste dag. Måske er det også almindeligt for din familie at have sådan en i jeres hjem?

Disse devices lytter til stemmekommandoer og reagerer på dem ved at bruge deres internetforbindelse.

Men vi tænker måske ikke over, at det åbner for nogle sikkerhedsproblemer, når en smart home assistant får en kommando, henter data fra nettet, giver besked til brugere om opkald/beskeder, eller bruges til at kontrollere andre IOT-devices i hjemmet.

I er nu kommet på en mission for at gøre jeres hjem mere sikre ved, at begrænse truslerne mod smart home assistants. Med udgangspunkt i to modeller (dataflow diagram og STRIDE som præsenteres senere) skal I undersøge, hvordan man identificerer sårbarheder i systemerne og derved måden, hvorpå de kan hackes. Ved at identificere sårbarhederne, vil I også være i stand til at komme med forslag til, hvordan sikkerheden i systemerne kan øges.

JERES MISSION

I skal lave en trusselsmodellering af en smart home assistant. Det kan virke som en stor opgave.
Vi har derfor brudt trusselsmodelleringen lidt op, for at gøre det lettere for jer.

For at løse jeres mission skal I besvare de følgende 5 trin, som samlet set udgør jeres trusselsmodellering.

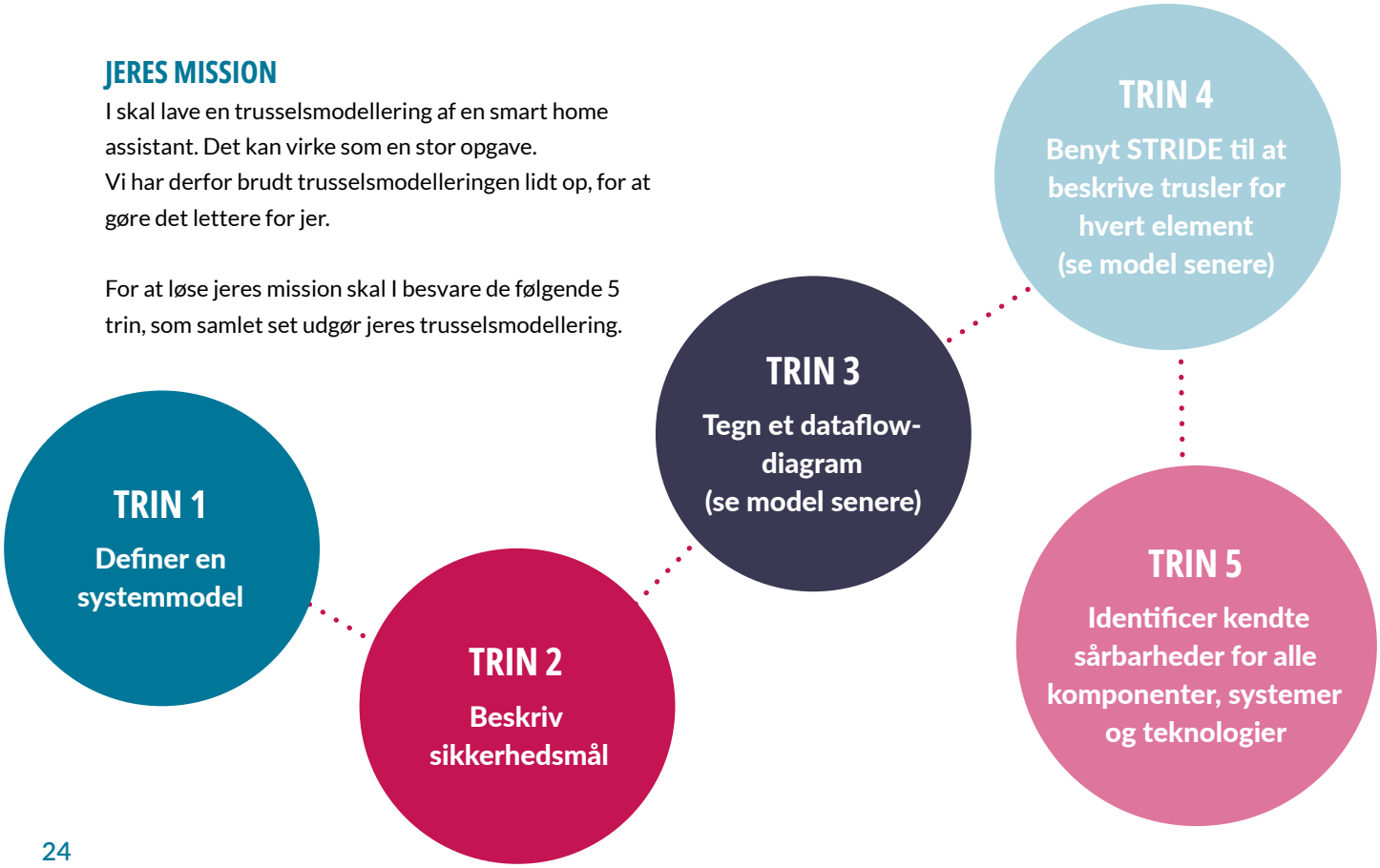
Vi anbefaler, at I udarbejder et STRIDE-framework og et dataflow-diagram til at understøtte jeres besvarelse. De to modeller er beskrevet til sidst i missionen.

BAGGRUND: HVAD ER EN 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.

Formålene med en trusselsmodellering er at:

- Forstå de sikkerhedsmål, man søger at realisere
- Forstå det system, man forsøger at sikre
- Forstå de trusselsaktører, man står overfor
- Forstå de teknikker, trusselsaktørerne benytter (angrebsvektorer)
- Forstå de sårbarheder, angriberne udnytter
- Forstå, hvilke modforholdsregler, der er effektive mod disse angreb



VIGTIGE HOVEDTERMER INDEN FOR TRUSSELS-MODELLERING, SOM ER GODE AT KENDE

Trussel. En trussel er en potentiel uønsket begivenhed eller hændelse, der kan skade eller kompromittere et aktiv eller mål. Den kan være af ondsindet natur.

Angreb (eller udnyttelse). Et angreb er en handling, der udnytter en eller flere sårbarheder for at gennemføre en trussel.

Sårbarhed. En sårbarhed er en svaghed, som muliggør et angreb, i en del af et system. Sårbarheder kan findes i niveauet for netværk, host eller applikation og inkluderer operationelle praksisser.

Modforholdsregler. En modforholdsregel tager fat på en sårbarhed for at reducere muligheden for angreb eller reducere et angrebs påvirkning. En modforholds-regel forholder sig ikke direkte til en trussel. I stedet tager den fat på de faktorer, der definerer truslen. Modforholdsregler spænder fra at forbedre en applikations design eller kode til at forbedre en operationel praksis.

Aktiv. Et aktiv er en ressource, der har værdi. Det varierer efter perspektiv. For en virksomhed kan et aktiv være informationer såsom kundedata. Eller det kan være mere uhåndgribeligt, som fx virksomhedens omdømme. Det kan også være muligheden for at misbruge virksomhedens applikation til at få uautoriseret adgang til data, administrative funktioner eller lignende.

SÅDAN LAVER DU EN TRUSSELSMODELLERING TRIN FOR TRIN

Der er fem trin i en trusselsmodellering, som du kan se uddybet i det følgende.

TRIN 1

DEFINER EN SYSTEMMODEL

- Identificer jeres smart home assistentens' system-komponenter og interaktioner mellem dem. Hvad kan systemet, hvem bruger det og hvordan?

TRIN 2

BESKRIV SIKKERHEDSMÅL

- Beskriv de overordnede sikkerhedsmål for systemet som helhed
- Beskriv sikkerhedsmålet for de enkelte komponenter, som systemet består af

TRIN 3

TEGN ET DATAFLOW-DIAGRAM (SE MODEL 1)

Dataflow-diagrammet beskriver, hvordan data bevæger sig gennem et netværk.

- Tegn et diagram, der beskriver alle datastrømme i jeres smart home assistent.

TRIN 4

BENYT STRIDE TIL AT BESKRIVE TRUSLER FOR HVERT ELEMENT (SE MODEL 2)

- Trusselsvurderingen bør indeholde en linje for hvert element (dvs. systemkomponent) som I identificerede i trin 1.
- For alle krydser bør der være en beskrivelse af den specifikke trussel
  - Fx hvorfor er spoofing et problem for bluetooth-parring i en Soundboks? Se en mere detaljeret beskrivelse af STRIDE-modellen nedenfor.

TRIN 5

IDENTIFICER KENDTE SÅRBARHEDER FOR ALLE KOMPONENTER, SYSTEMER OG TEKNOLOGIER

- Analysér systemet for sårbarheder der kan udnyttes.

SÅDAN LAVER DU ET DATAFLOW-DIAGRAM

Det kan være godt at spørge sig selv, hvad der sker med data, når de kommer til et system. Om de omregnes eller konverteres på en eller anden måde, om de gemmes i en database og, hvordan data sendes videre til et nyt system eller til et andet sted i systemet.

Et dataflow-diagram viser, hvordan data strømmer igennem et system eller igennem en række af forskellige systemer. Det bruges ofte i softwareudvikling til at give et overblik over, hvor data er, hvornår og med hvilket formål.

Dataflow-diagrammet viser blandt andet, hvor data kommer fra, hvor de går hen, hvor de bliver gemt og hvor de måske transformeres, eksempelvis fra stemme til skrift. Følgende symboler kan bruges i diagrammet:

MODEL 1: SYMBOLER TIL DATAFLOW-DIAGRAM

TEKST →	En pil angiver den retning, som data bliver sendt i
PROCES	En cirkel (eller oval) angiver, hvor data processeres eller transformeres
KILDE	En firkant angiver, at data sendes til en ekstern kilde (i forhold til hvor data startede)
DATA	To streger med tekst imellem angiver, hvor data gemmes (i en database eller lignende)

Man kan starte med et overordnet billede af, hvad der sker med data for at forstå nogle af de eksterne kilder. Derefter kan man dykke et skridt dybere for at forstå, hvad der sker på et detaljeret niveau.

Under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/ finder I en video, som viser, hvordan man kan lave et dataflow-diagram.

SÅDAN LAVER DU EN STRIDE-MODEL

STRIDE-modellen er et nyttigt værktøj, som kan hjælpe med at klassificere trusler. Modellen er oprindeligt udviklet for at hjælpe sikkerhedsingeniører.

HVAD STÅR STRIDE FOR?

STRIDE er et akronym for seks trusselskategorier:

- **Spoofing**: agenter udgiver sig for at være en anden
- **Tampering**: uautoriserede ændringer af systemer eller data
- **Repudiation**: agenter nægter at have sendt en besked eller udført en handling
- **Information leakage**: fortrolighed brydes, fordi information lækkes til udenforstående
- **Denial of Service (DoS)**: systemer eller data gøres utilgængelige for autoriserede brugere
- **Elevation of Privilege**: agenter opnår højere privilegier, f.eks. administratorrettigheder

Her er et eksempel på, hvordan man bruger STRIDE:

STRIDE tager udgangspunkt i de elementer, man har identificeret i dataflow-diagrammet. Vi har indsat følgende element " #1 Parring mellem telefon og Soundboks" i STRIDE-modellen nedenfor.

MODEL 2: STRIDE

	ELEMENT	INTERACTION	S	T	R	I	D	E
1	BT forbindelse	Parring mellem telefon og Soundbox	X				X	
2		Afspilning af musik	X	X			X	
3		Kontrol af Solundbox (tænd/sluk, volumen, ...)	X	X			X	X
4								

Under videomateriale på Cybermissionens hjemmeside: https://cybermissionen.cyberskills.dk/ finder I en video, som gennemgår STRIDE-modellen.

S: Spoofing kan tillade at uautoriserede telefoner parres med Soundboks eller at en telefon parres med uautoriseret Soundboks.

D: Spoofing tillader direkte DoS ved at slukke for boksen, skrue ned for lyden, spille noget helt andet eller afbryde parring.

Lav jeres eget STRIDE skema og start med at indsætte de elementer i identificerede i trin 1. Herefter kan I bruge modellen til, at hjælpe med at skabe et overblik over trusler og dermed også eventuelle sårbarheder jeres system måtte have.

Når I har lavet alle punkterne i trusselsmodelleringen har I gennemført missionen.

JERES PRÆSENTATION

I skal forberede en præsentation af jeres analyse, hvor I redegør for missionen, fortæller om jeres proces med at lave jeres trusselsmodellering samt præsentere selve trusselsmodelleringen. I præsentationen skal I:

- Redegøre for jeres mission og hvad I har valgt at fokusere på
- Fortælle, hvordan I kom frem til jeres endelige trusselsmodellering
- Præsentere jeres modellering (gerne med billeder, video, skærmoptagelse m.m.)
- Fortælle, hvordan I har anvendt modeller/analyseredskaber
- Præsentationen skal have karakter af et kort præsentation 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.

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

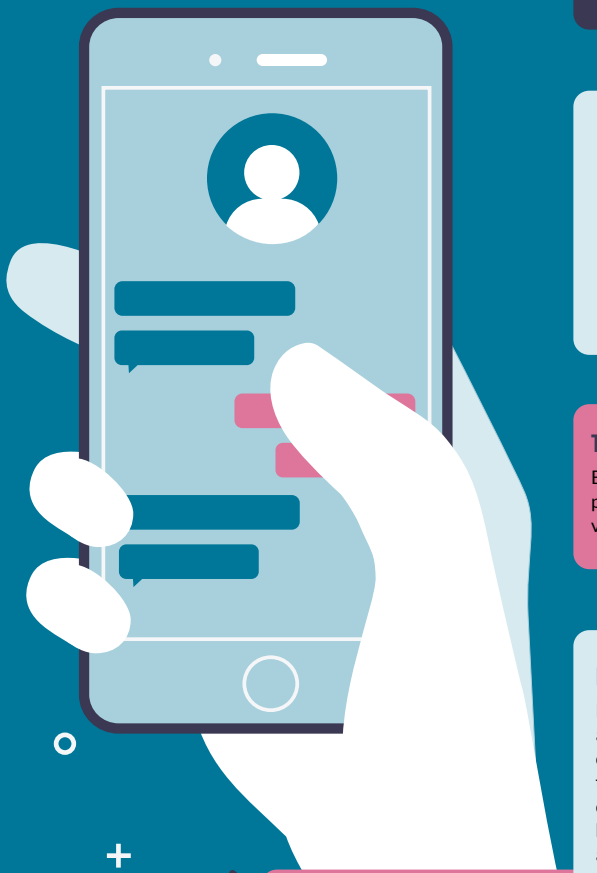
Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationssikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

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