CYBERMISSION 2

TRUSSELSVURDERING OG RISIKOANLYSE

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

CYBERMISSION 2 - TRUSSELSVURDERING
OG RISIKOANLYSE

Design:
Børne- og
Undervisningsministeriet

Børne- og Undervisningsministeriet
Styrelsen for It og Læring
Vester Voldgade 123
1552 København V

CYBERMISSION 2 - TRUSSELSVURDERING OG RISIKOANLYSE

Danmarks sikkerhed er vigtig for os alle, ung som gammel. Men hvordan beskytter vi bedst Danmark mod de mange kriminelle, der findes ude i cyberspace? Og hvad er egentlig vigtigst for os at beskytte i Danmark?

Danmark har udarbejdet en national strategi for cyber- og informationssikkerhed (læs den her: https://digst.dk/strategier/cyber-og-informationssikkerhed/). Strategien afspejler et ønske om at opruste den samlede indsats i kampen mod de digitale trusler, Danmark står overfor. I strategien er der udpeget seks samfundskritiske sektorer, som det kræver en særlig indsats at beskytte mod trusler.

De seks samfundskritiske sektorer er valgt, fordi det vil være meget kritisk, hvis en virksomhed inden for en af disse sektorer blev offer for et hackerangreb.
De seks udvalgte sektorer er: tele-, finans-, energi-, sundheds-, transport- og søfartssektoren. Det omfatter eksempelvis teleselskaber, banker, elselskaber, sygehuse, offentlig transport som DSB og de, som opererer på havet.

SEKTORANSVARSPRINCIPPET

I Danmark er det bestemt, at sektorerne bærer et "sektoransvarsprincip". Det betyder, at den enkelte sektor har ansvar for at sikre et vist beredskab, så de kritiske funktioner kan opretholdes. Det betyder, at virksomhederne skal tage et aktivt ansvar for at være beredt på cyberangreb.

I energisektoren har man eksempelvis stiftet foreningen EnergiCERT (Link: https://energicert.dk/). EnergiCERT har til formål at løfte sektorens cyber- og informationssikkerhedsniveau og støtte sektoren i at agere professionelt mod cybertrusler.

Ansvaret for cybersikkerhed er altså ikke samlet et enkelt sted, men det er placeret i alle sektorer. I Danmark ser man cybertruslen som en samfundsudfordring, der skal løses i fællesskab mellem stat, kommuner, regioner, organisationer, virksomheder og os alle som privatpersoner. Alle har et ansvar.

RISICI VED HACKERANGREB

Man tænker måske ikke over det til hverdag, men det vil være ret alvorligt, hvis den danske telesektor blev lagt ned af et hackerangreb. Det kan få den betydning, at vores telefoner ikke længere kan få adgang til data, og der kan potentielt set blive lukket ned for al kommunikation i landet.

Et succesfuldt cyberangreb mod telesektoren kan medføre økonomiske tab for virksomheder, afsløre fortrolige data og påvirke tilgængeligheden af teletjenester. De angreb, som eksempelvis bliver brugt mod telesektoren, er det, man kalder DDOS-angreb (overbelastningsangreb), ransomware, der rammer kritiske systemer, eller uautoriseret omdirigering af mobil- og internettrafik.
Læs mere om de forskellige typer angreb her: https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed

Center for Cybersikkerhed vurderer, at telesektoren i Danmark står over for en **MEGET HØJ** trussel fra cyberkriminalitet. Så cybertrusler er altså en realitet for telesektoren og noget, de skal forholde sig til hver eneste dag.

RISIKOANALYSER OG TRUSSELSVURDERINGER

Prøv at forestille dig, at du blev nægtet adgang til al mobiltelefoni og internetadgang? Det er ikke kun privat, at folk vil opleve det som en katastrofe, for mobiltelefoni og internetadgang er afgørende for alle dele i samfundet.

Teleselskaber har altså et stort ansvar for at beskytte sine it-systemer og undgå sikkerhedsbrud. De laver løbende trusselsvurderinger, risikoanalyser og analyserer sårbarheder for at forhindre det næste potentielle angreb. De er meget opmærksomme på hvilke typer

angreb, der dominerer sektoren, så de kan forberede sig bedst muligt.

JERES MISSION

På denne cybermission skal I forestille jer, at I er blevet hyret ind af ledelsen i en af Danmarks største televirksomheder. I skal hjælpe dem med at undersøge hvilke forhold og risici, de skal være opmærksomme på i deres omverden, når det kommer til it-sikkerhed. Derudover skal I lave en vurdering af de konsekvenser, der er forbundet med de forskellige risici. Med andre ord skal I lave det, man kalder en trusselsvurdering.

Med grundig forberedelse kan man som firma nemlig styrke sit forsvar og være bedre forberedt på angreb.

I får stillet to værktøjer til rådighed, som danner grundlaget for jeres trusselsvurdering: **1) Omverdensanalyse** og **2**) **Risikoanalyse**, som begge beskrives nedenfor.
Når I har lavet de to analyser, skal I forberede en præsentation til ledelsen, hvor I skal fremlægge det I har fundet ud af og hvilke handlemuligheder virksomheden har.

MODEL 1) OMVERDENSANALYSE

En virksomhed er nødt til at analysere sin omverden for at kunne se, hvad der kan påvirke dens situation og udvikling. Omverdensanalysen er et godt værktøj til at afdække alt fra politiske faktorer til teknologiske forhold, der spiller en rolle og påvirker situationen for virksomheden.
Når man laver en omverdensanalyse kigger man på virksomhedens "afhængige omverden" og den "uafhængige omverden", som illustreret i model 1.
Den afhængige omverden, også kaldet "nærmiljøet", er de forhold, som virksomheden har påvirkning på og direkte kontakt med. Den uafhængige omverden, også kaldet "fjernmiljøet", er de overordnede forhold, som påvirker virksomheden. Selvom virksomheden ikke har direkte indflydelse på den uafhængige omverden, er det vigtigt, at den holder sig orienteret om, hvad der sker.

Jeres opgave er altså at tage plads i sædet som rådgiver for televirksomheden, og analysere dens omverden i forhold til cybertrusler, it-kriminalitet og mulige angreb. I skal se på både den afhængige og den uafhængige omverden.

Følgende spørgsmål kan hjælpe jer på vej med analysen. Spørgsmålene tager afsæt i **Omverdensmodellen**.

Spørgsmål til den afhængige omverden:

- **Kunderne:** Hvordan vil kunderne reagere, hvis virksomheden bliver offer for et cyberangreb
- **Konkurrenter:** Hvordan vil det påvirke konkurrenternes position, hvis virksomheden bliver offer for et cyberangreb?
- **Leverandører:** Hvordan vil det påvirke virksomheden, hvis en af deres leverandører bliver offer for et cyberangreb?

Spørgsmål til den uafhængige omverden:

- **Politik og lovgivningsmæssige forhold:** Hvordan kan politiske, bl.a. internationale forhold, motivere cyberangreb?

- **Politik og lovgivningsmæssige forhold:** Hvordan kan ny lovgivning påvirke måden, hvorpå virksomheden arbejder med informationssikkerhed?
- **Teknologiske forhold:** Hvilke teknologiske forhold skal virksomheden være opmærksom på for fortsat at beskytte sig selv og sine kunder mod cyberangreb?
- **Teknologiske forhold:** Hvordan kan den øgede digitalisering af samfundet have indflydelse på risikoen for, at virksomheden bliver offer for et cyberangreb?
- **Massemedier:** Hvad er massemediernes rolle, når det gælder hackernes motivation for at lave angreb?

MODEL 2)
RISIKOANALYSE

Risikoanalysen bliver ofte anvendt af virksomheder. Man bruger den til løbende at holde styr på hvilke risici, der er de mest alvorlige og til at finde strategier til at reducere, udbedre og overkomme disse risici.
Der vil altid være en lang liste af forskellige risici, men det er langt fra alle, der er lige sandsynlige eller har samme konsekvenser.

En risiko består altid af

1. **En sandsynlighed for hændelsen**
2. **Konsekvenser af hændelsen**

Det er ikke et mål i sig selv at undgå risici, men målet er at sikre, at risici håndteres, eller at man vurderer, at den ikke skal håndteres lige nu, da den ikke er vigtig. Her kan man bruge risikoanalysen til at sikre den rigtige prioritering.

I skal identificere minimum fem risici som televirksomheden står overfor. Nogle tager måske udgangspunkt i jeres drøftelser i forbindelse med jeres omverdensanalyse, andre er måske helt nye.
I må bruge jeres fantasi og finde på 'ekstreme tilfælde" og også gerne nogle som er mere almindelige og dermed mere sandsynlige. En risiko kan være alt fra indførelse af ny lovgivning til risikoen for, at der opstår en "hacker-aktivist-gruppe", der er imod virksomhedens forretningsområde.

Et eksempel på en risici:

"Organiseret netværk af cyberkriminelle fra Kina lægger hele Danmarks mobilnet ned – man mener at angrebet er politisk motiveret."

I skal huske at argumentere for, hvorfor I har indplaceret den pågældende risici I det givne felt.

MODEL 2

RISIKOANALYSE

KONSEKVENSER

SANDSYNLIGHED

	1 Ubetydelige	2 Mindre	3 Alvorlige	4 Meget alvorlige	5 Katastrofale
5 Ofte	5	10	15	20	25
4 Sandsynlig	4	8	12	16	20
3 Sjælden	3	6	9	12	15
2 Usandsynlig	2	4	6	8	10
1 Meget usandsynligt	1	2	3	4	5

INSPIRATION

Inden I går i gang anbefaler vi, at I ser følgende videoer, hvor I møder en række super dygtige folk, som arbejder med området til daglig. De vil hjælpe jer med at forstå missionen, modellerne og give jer gode tips. Videoerne varer mellem 8-12 minutter.
Videoerne til **CYBERMISSION 2- TRUSSELSVURDERING OG RISIKOANLYSE** finder I her:
https://cybermissionen.cyberskills.dk/mission-2/

VIDEO 1)
Hvordan beskytter vi Danmarks kritiske infrastruktur?

VIDEO 2)
Hvad påvirker trusselsbilledet i Danmark?

VIDEO 3)
Hvad er en risikoanalyse?

VIDEO 4)
Sådan laver man en omverdensanalyse

"NÅR CYBERKRIMINELLE GÅR EFTER KRITISK INFRASTRUKTUR SOM FX HOSPITALER, FORSYNINGSSELSKABER OG TELENETVÆRK, KAN DET BRINGE BÅDE SIKKERHED OG SUNDHED I FARE."

JERES PRÆSENTATION

I skal forberede en præsentation til ledelsen i virksomheden, hvor I fremlægger jeres analyser, gerne med brug af visuelle virkemidler

I præsentationen skal I:

- Præsentere de forhold I har fundet frem til i jeres omverdensanalyse
- Fremlægge de risici I har udvalgt til jeres risikoanalyse, vise hvordan I har indplaceret dem i jeres risikoanalyse (sandsynlighed/konsekvenser) og forklare hvorfor
- Fortæl kort, hvorfor det er vigtigt, at virksomheder forholder sig til deres omverden når det kommer it-sikkerhed og cyberangreb.

I må meget gerne underbygge jeres præsentation med aktuel viden og kilder.

Præsentationen skal have karakter af et kort pitch, ligesom det de laver i Løvens Hule og må max tage 10 minutter.

DELTAG I EN NATIONAL KONKURRENCE

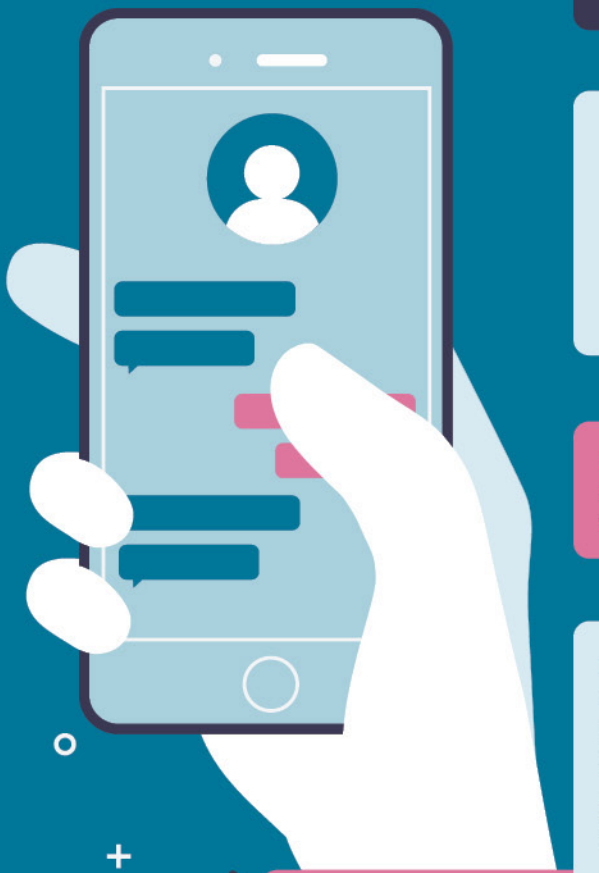
Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den ind til Styrelsen for It og Læring. Alle videoer 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?



INCOGNITO / PRIVAT BROWSER

Når du sætter din browser i 'inkognito' gemmes dine indtastninger ikke i din browser eller lokalt på din computer. Men hjemmesider, din skole eller internetudbyder kan stadig se din aktivitet.

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.

GDPR

GDPR står for General Data Protection Regulation og er en lov, som er indført af EU for at passe på dine og alle andres data og personoplysninger.

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.

MALWARE

Malware bruges om ondsindet software - fx virus eller andet, der skader din computer.

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