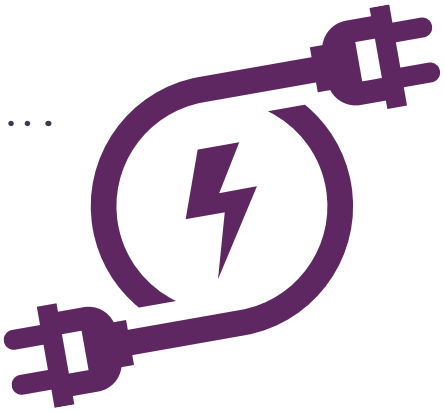
MISSION 2: Operation GridGuard



GridGuard missionen

EnergiSikker er en (fiktiv) førende dansk virksomhed inden for energisektoren. De er blevet ramt af et omfattende cyberangreb, hvilket har resulteret i et nedbrud i det danske elnet. EnergiSikker frygter nu alvorlige konsekvenser for EnergiSikkers ry og økonomi. Jeres mission handler om at forstå, hvordan et hackerangreb kan destabilisere energisektoren. I skal også udvikle en beredskabsplan og en effektiv kommunikationsplan for at bevare tilliden til de danske borgere og sikre, at der fortsat vil være energiforsyning i det danske land.

Fagforslag:
Samfundsfag, dansk, it og kommunikation, sprog (research på engelsk), Informatik m.m.

Energisektoren - en kritisk sektor

Energisektoren hører til det, vi i Danmark definerer som en kritisk sektor, hvilket betyder, at dens funktion er afgørende for opretholdelsen af samfundets grundlæggende funktioner og sikkerhed.

Alle vores elselskaber hører under energisektoren, som forsyner os med strøm. Foruden energi er også sundhedsvæsenet, vandforsyning, transport (på sø og på land) og telekommunikation kritiske sektorer.

Disse sektorer har man defineret som værende hjørnestenene i samfundets infrastruktur - altså de er vigtige for, at samfundet kan hænge sammen.

Et angreb i en af disse sektorer vil have store konsekvenser

Det er vurderet, at angreb eller forstyrrelser i disse sektorer vil have alvorlige konsekvenser for borgernes velfærd og nationens funktion.

Det er derfor yderst vigtigt, at vi formår at beskytte og sikre disse kritiske sektorer, og at virksomheder, der opererer inden for disse sektorer, har lige så godt styr på deres sikkerhed.

Typiske angreb i energisektoren

Energisektoren er en af de sektorer, der står over for et stigende trusselsniveau, hvad angår cyberangreb. Et angreb på vores elselskaber kan have alvorlige konsekvenser for forsyningssikkerheden og samfundet som helhed.
Hackergrupper forsøger f.eks. at få uautoriseret adgang til energivirksomhedernes netværk for at stjæle fortrolige oplysninger eller sabotere driftssystemer. Disse angreb kan bl.a. omfatte **malware**, **ransomware** og **phishingangreb**, hvor angriberne udnytter sårbarheder i systemerne eller forsøger at narre medarbejdere til at frigive adgangsoplysninger.

Distributed Denial of Service / Overbelastningsangreb

Distributed Denial of Service (DDoS)-angreb er også en angrebsmetode, som vi i stigende grad ser blive anvendt i energisektoren. Her får de kriminelle dog ikke adgang til kritisk information.

Denne type angreb går i stedet ind og overbelaster netværk og servere, hvilket resulterer i midlertidige eller langvarige afbrydelser af energiforsyningen. Dette kan sammenlignes med, når alle i Danmark forsøger at logge ind på SKAT.dk på samme tid, hvor systemet, der ikke er gearet til så mange forespørgsler på samme tid, "lukker" ned.

Politiske konflikter påvirker energisektoren

Vi ser også, at angreb, der er motiveret af politiske eller nationale interesser, rettes mod energisektoren. Denne form for angreb har til formål at påvirke nationers energiforsyning og økonomi.

Da Ruslands invasion af Ukraine var på sit "højeste", var adgang til energiforsyning en stor bekymring hos ukrainerne. På samme tid blev trusselsniveauet for cyberangreb mod energisektoren i Danmark opjusteret til at være "meget højt" og mange europæiske lande genbesøgte deres beredskab for at sikre sig, at de kunne modstå disse cyberangreb.

Hvad betyder beredskab?

Beredskabsplaner er planer, der er udviklet på forhånd for at håndtere forskellige former for nødsituationer eller kriser. I cyberverdenen refererer det specifikt til planer, der er designet til at håndtere og reagere på cyberangreb, datasikkerhedsbrud eller andre former for digitale trusler. Disse planer indeholder typisk instruktioner og retningslinjer for, hvordan man identificerer, reagerer på og håndterer situationer for at minimere skade og genoprette drift så hurtigt som muligt.

Beredskabskommunikation handler om, hvordan man kommunikerer under en krise eller i en nødsituation. Det handler altså om kommunikation med relevante interessenter som medarbejdere, kunder, leverandører, offentlige myndigheder og pressen for at informere dem om situationen, hvad man har gjort for at forhindre/afværge angrebet og forventede konsekvenser. Effektiv beredskabskommunikation er afgørende for at bevare tilliden, mindske panik og sikre koordineret handling under en krise.
Ofte vil det være en fordel at være åben, ærlig og regelmæssig i kommunikationen under hændelser, for at undgå misforståelser og skabe mistillid.

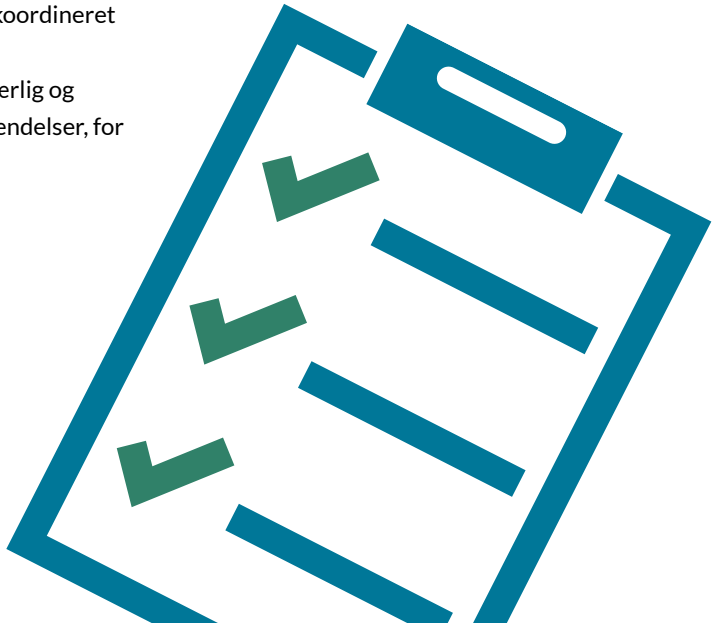
Hvorfor er det et krav at have beredskabsplaner i en energisektor?

Hvis en virksomhed skulle blive ramt af et cyberangreb, er det vigtigt at have en god beredskabsplan, som kan sættes i værk med det samme.
En god beredskabsplan sikrer, at alle ved, hvem der gør hvad, og at man kan reagere hurtigt og effektivt på uforudsete situationer, hvilket et cyberangreb jo er. Sådan en form for beredskabsplan kan sammenlignes med den beredskabsplan for tilfælde af brand, der hænger på jeres skole. Den fortæller jer, hvad I skal gøre, hvis der opstår brand - Hvordan kommer I ud? Hvilke udgange skal I bruge?

En beredskabsplan i en cybersikkerhedskontekst skal altså bidrage til, at man kan bevare energiforsyningens stabilitet, samt minimere negative konsekvenser for virksomheden som helhed. Beredskabsplanen skal også indeholde en plan for kommunikationen - både internt og eksternt.

Hvad skal defineres i en beredskabsplan:

- En beredskabsplan er en detaljeret strategi.
- Planen identificerer potentielle trusler, fastlægger ansvar, og beskriver handlingstrin for at genoprette normal drift.
- Beredskabsplanen skal løbende holdes opdateret, kommunikeres klart til medarbejdere og regelmæssigt gennemprøves for at sikre, at alle ved, hvad de skal gøre den dag, de skal tage den i brug.



Jeres mission

I skal nu på en mission med udgangspunkt i virksomheden EnergiSikker!

Missionen består af to dele, og undervejs i missionen skifter jeres rolle.

Under del 1 befinder I jer på modstandernes side, hvor I skal angribe virksomheden. **I del 2** befinder I jer på EnergiSikker-siden, hvor I skal sørge for, at virksomheden kommer bedst muligt igennem angrebet.

Del 1:
Udfør et cyberangreb på virksomheden EnergiSikker.

Overvej følgende:

- Hvem er I som hackergruppe? Og hvorfor vil I gerne angribe netop EnergiSikker?
- Hvilken type angreb vil I udføre?
- Hvordan lykkes I med at angribe?
- Hvilken skade sker der på EnergiSikker?

VIGTIGT: Des flere detaljer I har på plads om jeres angreb, des lettere bliver del 2 af missionen.

Del 2:
EnergiSikker er blevet angrebet! Hvordan kommunikerer I som virksomhed bedst under og efter angrebet?

- Hvordan vil I informere offentligheden om situationen for at bevare mest mulig tillid hos offentlige myndigheder samt jeres kunder? Hvad skal der siges, hvor meget skal der siges, og igennem hvilke medier? Hvem er jeres talsperson og hvorfor?
- Hvordan sørger I for at minimere forvirring blandt jeres medarbejdere, mindske deres bekymringer og undgå, at der spredes falsk information om hændelsen? Hvor meget ønsker I at kommunikere til dem, hvordan, hvornår og hvem skal sige det?

Jeres præsentation

I skal forberede en præsentation, hvor I redegør for jeres arbejde med missionen - først beskriver I, hvilket cyberangreb I har udført og herefter, hvordan EnergiSikker bedst kommunikerer om angrebet, så de kommer stærkest ud på den anden side af angrebet.

Præsentationen må max tage 5 minutter.

Det er helt op til jer, hvordan I præsenterer: Det kunne f.eks. være med en **PowerPoint** præsentation, gennem et kort **skuespil**, en **videopræsentation** eller noget **helt andet**. Det vigtigste er, at I får formidlet jeres arbejde med missionen tydeligt og grundigt.

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.