**Modul 4 – Øvelser**

**Opgaven er beskrevet nedenfor, og vi anbefaler 5 timers gruppearbejde.**

**Step 1** - En i gruppen opretter sig via link med brug af MFA og har dermed adgang til D-mærket (jeres teams-link står i excel)

**Step 2 (4 timer, 1 time til hver øvelse)**

I skal derefter lave de 4 øvelser med tilhørende spørgsmål, som har fokus på hhv:

- Sikkerhedspolitk

- Beredskabsplan

- Awareness

- Foranstaltninger ift vækst

I skal vælge en af de 5 case virksomheder, som er jeres udgangspunkt ift at lave foreslag.

**Step 3**

Skriv refleksionerne ned, så I har det til senere brug.

**Step 4 (1 time)**

Kig rundt i D-mærket som værktøj, hvordan det kan give mening at anvende i virksomheden/praktikken - og se hvad det kan og ikke kan. (

**Øvelse 1: Udarbejdelse af Sikkerhedspolitik**

Formål: At lade deltagerne udvikle en ramme for en sikkerhedspolitik for virksomheden, som adresserer nøgleområderne inden for D-mærkets kriterier.

Metode: Deltagerne får til opgave at formulere en sikkerhedspolitik, der inkluderer retningslinjer for adgangskontrol, datahåndtering, og ansvarlig teknologibrug, som er tilpasset virksomhedens behov og udfordringer.

Diskussion: Grupperne præsenterer deres sikkerhedspolitikker, og sammen diskuterer de potentialer og udfordringer ved implementeringen af disse politikker.

**Øvelse 2: Udvikling af IT-beredskabsplan for virksomheden**

Formål: At styrke virksomhedens evne til at håndtere og reagere på IT-sikkerhedshændelser gennem en detaljeret beredskabsplan.

Metode:

Deltagerne inddeles i små grupper og udarbejder en IT-beredskabsplan, der tager højde for virksomhedens specifikke behov og udfordringer som beskrevet i casen. Planen skal følge de anbefalinger, der er beskrevet i vejledningen fra Sikker Digital og skal omfatte følgende elementer:

Identifikation: Definer metoder og værktøjer til tidlig opdagelse af sikkerhedsbrud.

Rapportering: Etabler klare retningslinjer for, hvordan og til hvem sikkerhedshændelser skal rapporteres internt.

Håndtering: Specificer procedurer for indgriben og begrænsning af skader ved hændelser.

Genopretning og evaluering: Planlæg trin for at genoprette systemer og evaluere hændelsesforløbet for at forbedre fremtidige reaktioner

Diskussion: Hver gruppe fremlægger deres plan, og sammen diskuterer de, hvordan en effektiv respons kan minimere skaden fra sikkerhedshændelser og forbedre virksomhedens resiliens.

**Øvelse 3: Awarenessprogram**

Formål: At styrke sikkerhedskulturen i virksomheden ved at designe et sikkerhedsbevidsthedsprogram, der adresserer de adfærdsmæssige og kulturelle udfordringer identificeret i casen.

Metode: Grupperne udvikler et program, der omfatter træning, kommunikationstiltag og aktiviteter til at øge bevidstheden om cybersikkerhed blandt medarbejderne på alle niveauer.

Diskussion: Præsentation af programmerne efterfølges af en diskussion om, hvordan man kan sikre medarbejdernes engagement og ændre sikkerhedskulturen positivt.

**Øvelse 4: Tilpasning af Sikkerhedsforanstaltninger til virksomhedens vækstambitioner**

Formål: At forberede virksomheden på skalerbar sikkerhed i takt med virksomhedens vækstambitioner.

Metode: Grupperne udarbejder strategier for at skalere virksomhedens cybersikkerhedsforanstaltninger i overensstemmelse med deres planer for øget digitalisering, medarbejderantal, og omsætning.

Diskussion: Diskuter hvordan disse strategier understøtter sikker og pålidelig vækst samt evnen til at efterleve stigende kunde- og lovgivningsmæssige krav.

* - -

**Øvelse 5: Modenhedsvurdering (kan bruges ifb med at se ind i d-mærket, er op til jer om I vil gennemføre med en virksonhed som udgangspunkt)**

Formål: Bruge tid på at kigge på. D-mærkets selvevalueringsværktøj ved at gennemføre en initial selvbedømmelse for en virksomhed baseret på de oplysninger, de har fået.

Metode: Grupperne anvender selvevalueringsværktøjet til at identificere, hvor virksomheden står i forhold til D-mærkets kriterier. De skal specifikt kigge på virksomhedens aktuelle risikobillede, sikkerhedskultur, og eksisterende tiltag.

Diskussion: Efterfølgende diskuterer grupperne deres fundne risikoområder og foreslår prioriterede skridt for at forbedre virksomhedens cybersikkerhedsniveau.