



Strategi for awareness i Haderslev Kommune

Indhold

Indledning.....	2
Formål.....	2
Mål.....	2
Målgrupper.....	2
Principper.....	2
<i>Princip 1:</i>	3
<i>Princip 2:</i>	3
<i>Princip 3:</i>	3
<i>Princip 4:</i>	3
<i>Princip 5:</i>	3
Ansvar og afrapportering.....	3

Indledning

Danmark er et af de mest digitaliserede OECD-lande¹ i verden og har en af de mest effektive offentlige sektorer². Hvis vi skal fortsætte med at digitalisere offentlige services, skal vi kunne fastholde borgernes høje tillid og tilslutning til disse.

Samtidig understreger trusselsvurderinger fra Center for Cybersikkerhed³ at Danmark fortsat udgør et attraktivt mål for ondsindede cyberkriminelle. Trusselsbilledet er hele tiden under udvikling. Nye aktører kommer til, mens andre forsvinder, og hackere udvikler konstant deres angrebsmetoder. Derudover er menneskelige fejl ifølge Datatilsynet den hyppigste årsag til utilsigtede brud på persondatasikkerheden⁴. Medarbejdernes adfærd i forhold til digital sagsbehandling har derfor stor betydning for, at Haderslev Kommune kan beskytte borgernes følsomme data og opretholde en høj grad af tillid blandt borgere, samarbejdspartnere og andre myndigheder.

Det er vigtigt, at medarbejderne forstår vigtigheden af at beskytte borgernes data for at skabe øget tillid blandt borgere og samfund. Et øget fokus på awareness, herunder kontinuerlig sikkerhedstræning, er derfor første skridt mod at skabe stabilitet i organisationen og tydeliggøre de risici, vi som organisation er udsat for, så medarbejdere på tværs af organisationen kan genkende dem og reagere korrekt. En god sikkerhedsadfærd handler dog ikke kun om viden og kompetencer, men i høj grad om at gøre den ønskede adfærd attraktiv og tilgængelig.

Formål

Styregruppen for Digital Fremtid ønsker med denne strategi at styrke Haderslev Kommunes modstandsdygtighed overfor cybertrusler ved at informere, uddanne og engagere medarbejderne i arbejdet med persondata-, cyber- og informationssikkerhed.

Mål

Ambitionen er, at 100% af medarbejderne i Haderslev Kommune gennemfører deres sikkerhedstræning. I praksis betyder det, at Haderslev Kommune har et aktuelt succeskriterie på 80%, hvilket forudsætter, at 80% af organisationens medarbejdere gennemfører 100% af de tildelte kurser med et tilfredsstillende resultat på minimum 80% korrekte svar.

Målgrupper

Alle medarbejdere i Haderslev Kommune bør, uanset organisatorisk placering eller stillingsbetegnelse, modtage sikkerhedstræning, da persondata-, cyber- og informationssikkerhed vedrører alle, om end i varierende grad. Sikkerhedstræningen kan skaleres og planlægges således, at der tages hensyn til medarbejdernes primære arbejdsopgaver i relation til træningsindholdet. Derfor inddeler vi i Haderslev Kommune medarbejderne i træningsgrupper baseret på deres arbejdsfunktion. Disse træningsgrupper danner således grundlag for, hvilken træning den enkelte medarbejder skal modtage.

Yderligere sikkerhedstræning kan derefter, i samarbejde med den ansvarlige leder, tilrettelægges som mikrolæring fordelt hen over året under hensyntagen til den enkelte medarbejders ansættelsesforhold og primære opgaveløsning.

Principper

Arbejdet med awareness skal understøtte en kulturforændrende proces, hvor kontinuerlig sikkerhedstræning bliver en naturlig og integreret del af medarbejdernes hverdag. Herved opnår organisationen en stærkere intern modstandsdygtighed og en bedre fælles forståelse af, hvorfor awareness har stor betydning i forhold til persondata-, cyber- og informationssikkerhed.

¹ <https://www.digmin.dk/digitalisering/nyheder/nyhedsarkiv/2024/jan/oecd-danmark-er-blandt-de-bedste-lande-i-verden-til-offentlig-digitalisering>

² <https://digst.dk/nyheder/nyhedsarkiv/2024/oktober/danmarks-digitale-offentlige-sektor-er-fortsat-verdens-bedste/>

³ <https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/>

⁴ <https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-brud-paa-persondatasikkerheden/typer-af-brud>

Målet med kontinuerlig sikkerhedstræning i Haderslev Kommune hviler derfor på en række principper:

Princip 1:

Løfte medarbejdernes digitale kompetencer og adfærd på tværs af organisationen.

Princip 2:

Alle medarbejdere modtager kontinuerligt træning i persondata-, cyber- og informationssikkerhed.

Princip 3:

Alle medarbejdere onboardes i awareness-løsningen indenfor de første 30 dage af deres ansættelse og gennemfører en grundpakke i persondata-, cyber- og informationssikkerhed.

Princip 4:

Træningsmængde og -indhold følger risikogruppen ud fra en forudsætning om, at jo flere og jo mere følsomme data en medarbejder har adgang til, jo mere kontinuerlig sikkerhedstræning skal vedkommende modtage.

Princip 5:

Medarbejderne gennemfører den træning, de bliver tildelt.

Ansvar og afrapportering

Ansvar for opfyldelse af organisationens målsætning følger personaleansvaret. Afrapportering er en vigtig forudsætning for at den enkelte personaleleder kan følge udviklingen i egen afdeling og sikre sig, at medarbejderne gennemfører den træning, de bliver tildelt.

Afrapportering sker derfor fremadrettet på to niveauer:

- Det overordnede niveau til CLF. Her vil det være muligt at se afdelingens samlede gennemførelsesprocent, samt score i forhold til korrekt besvarelse på de enkelte træningsmoduler.
- Det detaljerede niveau til den nærmeste personaleleder. Her vil det ligeledes være muligt at se afdelingens samlede gennemførelsesprocent, den enkelte medarbejders gennemførelsesprocent samt score i forhold til korrekte svar på de enkelte træningsmoduler.

CLF og Styregruppen for Digital Fremtid modtager én afrapportering årligt. Styregruppen for Digital Fremtid afrapporterer herefter én gang årligt til direktionen. Denne afrapportering vil indeholde organisationens og fagforvaltningernes samlede gennemførelsesprocent. Derudover vil der også være mulighed for at se gennemførelsesprocent og score i forhold til korrekt besvarelse af træningsmoduler på tværs af træningsgrupper.

Styregruppen for Digital Fremtid vedligeholder løbende strategien i forhold til det generelle trusselsbillede og kan igangsætte særlige indsatser på baggrund af dette. Ligeledes kan fagforvaltningerne løbende lave specifik træning i forhold til det aktuelle trusselsbillede.



Red Bull

O'NEILL



Haderslev
Kommune

Haderslev Kommune

www.haderslev.dk