Konkretiser konsekvenserne for et cyberangreb i organisationen

En enkelt case-øvelse for IT-medarbejdere/ledere til visualisering af konsekvenserne

Formål

Formålet for øvelsen er, at synliggøre konsekvenserne ved et cyberangreb for organisationens øverste ledelse/beslutningstagere. Øvelsen skal omsætte faglig viden i IT-afdelingen til noget ledelsen kan forholde sig til, og anvende til at forstå organisationens aktuelle situation og den aktuelle risikoaccept. Casen kan desuden anvendes til dialog med ledelsen ift. om organisationen har en acceptabel risikoaccept, eller om der er behov for investering i sikkerheden for at nedbringe risikoen.

Deltagere

Øvelsen afholdes for IT-chef og -medarbejdere som har fagrelevant viden om IT-miljøet. Det vil typisk være disse medarbejdere, som bliver indkaldt hvis der opstår en alvorlig sikkerhedshændelse. Der kan være overlap mellem denne gruppe og organisationens beredskab – men her er det vigtigt, at det er medarbejdere med teknisk viden.

Der skal være en facilitator af øvelsen, som sikrer tydelig struktur.

Format

Deltagerne indkaldes til et møde fx 1-2 timer. De skal ikke være forberedt til mødet, og skal ikke have snakket sammen eftersom mødet er en dataindsamling/estimater af tid for scenariet.

Deltagerne præsenteres for en case. Det kan fx være denne:

Det er fredag eftermiddag. Vi er blevet mødt af en pop up på pc'erne, som tydeligt viser, vi er blevet ramt af ransomware. Hvad gør vi?

Deltagerne får nu 5-10 min til at diskutere, hvad der skal gøres. Mødelederen skriver notater undervejs, og laver en fælles opsamling på emnerne. Der kan fx være flere tekniske spor som *skal der hentes hardware og servere (nye og rene pc'er som ikke er ramt), skal al kommunikation afbrydes* samt *skal det testes, som vores SIEM er tilgængelig ift. logs.*

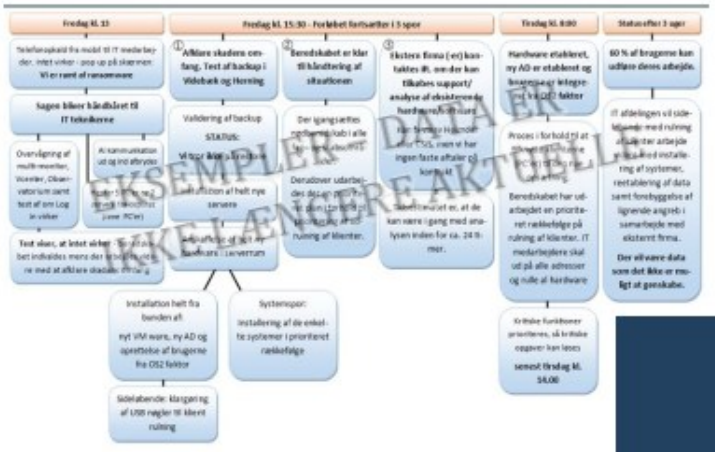
De forskellige spor drøftes, og nogle parkeres mens der laves tidsestimater på andre. Når der laves tidsestimater skriver deltagerne deres bud ned på en post-it, så de ikke påvirker hinandens svar.

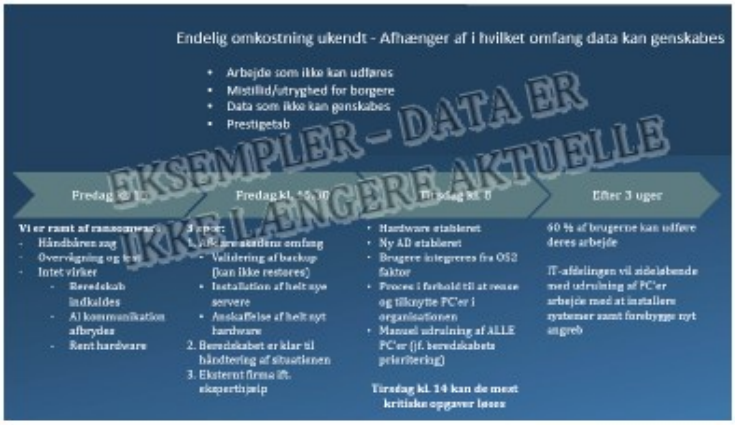
Øvelsen fortsættes fx ved at mødelederen siger: *Status efter den indledende afklaring er, at intet virker. Beredskabet indkaldes mens I arbejdere videre. Hvad vil jeres næste step være?*

Sådan fortsætter øvelsen indtil deltagerne har vurderet, hvornår vi er tilbage ift. at de kritiske funktioner i organisationen kan løses, og hvornår vi vil vurdere at fx 60 % af medarbejderne kan udføre deres arbejde.

Opsamling

Mødelederen/facilitatoren skriver løbende notater undervejs, og beder deltagerne om at lave individuelle skriftlige tidsestimater.
Efter mødet samler mødelederen/facilitatoren data sammen og laver fx en visuel oversigt over det fx som dette:





Visualiseringen kan indgå som en del af drøftelserne med det øverste ledelsesniveau ift. prioriteringer og beslutninger i forhold til cybersikkerhed.