Cybersikkerhedsøvelser vedrørende phishing

24/277 Åben Sag

Sagsfremstilling

Chef for Borgerservice, IT og digitalisering Tonny Olsen deltager på punktet.

Informationssikkerhedsudvalget har den 15. december 2023 aftalt, at der skal laves forslag til cybersikkerhedsøvelser vedrørende henholdsvis phishing og cyberangreb. Forslag behandles i HU med henblik på orientering, drøftelse og inspiration til kommunikation efter øvelsen.

Hvad er phishing og cyberangreb?

Phishing betyder, at hackere eller it-kriminelle prøver at lokke en person til at afgive fortrolige oplysninger f.eks. via henvendelser på mail eller falske hjemmesider. Oplysningerne misbruges til it-kriminalitet, og målet er oftest at stjæle eller afpresse sig til penge.

Cyberangreb er angreb, hvor brugerens pc bliver direkte angrebet f.eks. af ransomware, hvor cyberkriminelle krypterer brugerens data, så man ikke kan tilgå eller læse data. Data frigives først, når der er betalt løsesum.

Hvorfor vil Informationssikkerhedsudvalget lave rigtige øvelser?

Formålet med øvelser er at øge medarbejdernes opmærksomhed på risikoen for phishing og cyberangreb. Øvelserne skal medvirke til at skabe øget fokus på de phishing-mails og cyberangreb, som man kan blive udsat for som almindelig it-bruger, og give viden om, hvordan disse trusler skal håndteres. Cybersikkerhedsøvelser vedrørende phishing og cyberangreb er velkendte redskaber i arbejdet med informationssikkerhed og anvendes jævnligt af arbejdsgivere på det private arbejdsmarked og i stigende grad i kommunerne. Det er erfaringen fra sammenlignelige cybersikkerhedsøvelser, at ca. 20 % af medarbejderne i en organisation vil 'falde i' og dele deres fortrolige oplysninger via phishing-mails eller blive ofre for cyberangreb. Ved senere øvelser falder denne procentdel.

Center for Cybersikkerhed (CFCS) vurderer, at der er en stigende trussel mod cybersikkerheden i Danmark, og dette gælder også for kommunerne. It-afdelingen i Norddjurs Kommune har da også

registreret en øget mistænkelig trafik rettet mod kommunen. Derfor vurderer Informationssikkerhedsudvalget, at det vil være hensigtsmæssigt at gennemføre cybersikkerhedsøvelser.

Vores nabokommune i Syddjurs, har for nylig gennemført en lignende cybersikkerhedsøvelse vedrørende phishing. Vi vil lade os inspirere af deres materiale og gode erfaringer.

Hvordan forløber cybersikkerhedsøvelserne?
Forløb 1: Phishing kampagne – alle IT-brugere.
I forbindelse med øvelsen udsender it-afdelingen simulerede phishing-mails ved hjælp af et specialiseret it-system, der er designet til at efterligne virkelige phishing-angreb. Mailen indeholder et link, der opfordrer medarbejderne til at klikke. Formålet med øvelsen er at teste medarbejdernes evne til at identificere og undgå phishing-forsøg. De medarbejdere, der klikker på linket, vil efterfølgende blive informeret om, at de har deltaget i en phishing-simulation. Det understreges i situationen, at der ikke er sket nogen reelle skader, da det blot var en øvelse. Efterfølgende vil medarbejderne modtage e-læringsmateriale, som har til formål at forbedre deres kompetencer inden for cybersikkerhed og forebyggelse af phishing-angreb.

Varighed: Hvis brugeren trykker på linket, så vil det tage 3 – 5 minutter at læse, at man er faldet i en phishing fælde.

Forløb 2:
Simuleret Cyberangreb – målrettet 10 - 20 medarbejdere i et endnu ikke fastlagt fagområde.
Som led i øvelsen vil medarbejderne opleve, at der pludselig vises en besked eller en pop-up på deres skærm, som kræver deres opmærksomhed. Denne besked er designet til at ligne en reel sikkerhedstrussel, og har til formål at simulere et cyberangreb. Øvelsens formål er at observere, hvordan medarbejderne reagerer på en potentiel sikkerhedstrussel. Efter øvelsen vil de berørte medarbejdere blive informeret om, at der har været tale om en planlagt simuleringsøvelse udført af it-afdelingen.
Varighed: 30 til 60 minutter.

Hvornår foregår cybersikkerhedsøvelserne?

Øvelserne vil blive gennemført i første kvartal af 2025. Den præcise dato vil kun være kendt af it-afdelingen.

Hvilke udfordringer kan cybersikkerhedsøvelserne give?
Kampagnens formål er at øge sikkerheden fremadrettet. Formålet er ikke at 'hænge' medarbejderne ud. Man kan dog ikke udelukke, at der kan være medarbejdere, der vil opfatte det som skamfuldt at være "gået i fælden", og som vil være kritiske over for metoden, hvor arbejdsgiveren afprøver om medarbejderne handler hensigtsmæssigt.

I informationskampagner inden øvelserne bliver det oplyst, at interne øvelser vil indgå i vores arbejde med awareness, og at der ikke vil være nogen konsekvenser for de medarbejdere, som f.eks. afgiver deres oplysninger via phishing-mailen

Sammenhæng til andre politikker/strategier og fagområder
Informationssikkerhedspolitik som godkendt i Kommunalbestyrelsen den 25. august 2020. Tværgående retningslinjer for informationssikkerhed som godkendt i Direktionen den 27. januar 2021.

Indstilling
Formanden indstiller, at Chef for Borgerservice, IT og digitalisering Tonny Olsen informerer om cybersikkerhedsøvelserne, og Hovedudvalget drøfter indhold samt fordele og ulemper ved fremgangsmåden i cybersikkerhedsøvelserne. Hovedudvalget drøfter endvidere kommunikationsopgaven i forbindelse med øvelserne.

Beslutning i Hovedudvalget den 27-02-2025
Chef for IT, digitalisering og borgerservice Tonny Olsen præsenterede overvejelserne omkring cybersikkerhedsøvelserne. Der sker meget omkring cybersikkerhed nu og de kommende år, og trusselsbilledet udvikler sig af forskellige årsager hurtigt. Det vi kan gøre noget ved er, hvordan vi forbereder os og hvor vi øger vores forebyggende indsatser. Phishingkampagnen kan være med til at skærpe opmærksomheden. Erfaringen fra andre kommuner siger, at ca. 40 % klikker på et link, som beskrevet i ovenstående øvelse.

Der kan med fordel iværksættes en særlig større informationskampagne af informativ og varslende karakter en måned forud for øvelsen, så der skabes en bevidsthed omkring cybersikkerhed, og man ved der vil komme en øvelse. Efter en evaluering kan øvelsen gennemføres uden varsling. Det er vigtigt, at der er åbenhed og god og konstruktiv dialog, hvis man som medarbejder har klikket på linket i øvelsen.

Det er vigtigt, at man med øvelsen og når ud til alle, og at der er opmærksomhed på, at medarbejderne bruger forskellige platforme.

Afbud:
Kim Tommy Jensen (Vej- og ejendomschef)
Helle Steffensen
Ole Andersen
Anni Hovmann Nielsen
Vibbe Vogel Hansen

Bilag: