Beredskabsplan ved cyberangreb

Hvad skal du gøre ved et cyberangreb?

1. Træk netværkstikket ud og sluk for virksomhedens wi-fi.

2. Sørg for at oplyse relevante medarbejdere og eksterne nøglepersoner om cyberangrebet.

3. Betal ikke løsepenge og gå heller ikke i dialog med de IT-kriminelle.

Hvem skal du kontakte ved et cyberangreb?

Indsatsleder i tilfælde af cyberangreb

Jobtitel _____

Navn _____

Telefon _____

Ansvarlig for kontakten til eksterne IT-eksperter

Jobtitel _____

Navn _____

Telefon _____

Tjekliste, når du skal reetablere data- og IT-systemer

Nu starter dit samarbejde med eksterne IT-eksperter. Følg listen her, så du får det hele med:

- ✓ **Få overblik**
  Hvad er omfanget af skaderne? Har I fortsat backup? Prioriter indsatsen herefter
- ✓ **Tag stilling til reetablering**
  Skal jeres IT-systemer op at køre igen på det eksisterende udstyr, på andet udstyr eller i et virtuelt miljø?
- ✓ **Lav en foreløbig tidsplan**
  Afstem med dine samarbejdspartnere, hvornår systemerne forventes at være tilbage i drift igen. Orienter ledelsen og medarbejderne – og husk, at planen er foreløbig. Lav den om, hvis nødvendigt.
- ✓ **Test inden genstart**
  Vær sikker på, at systemet er klar til drift, at data er intakt og at netværksforbindelsen fungerer, efter systemet er reetableret.
- ✓ **Kommuniker løbende**
  Når systemet fungerer igen, skal ledelsen og medarbejderne orienteres.

Gode råd ved et cyberangreb

1. Har du en cyberforskring, så ring med det samme til Tryg for at få hjælp til at afværge angrebet og håndtere konsekvenserne på telefon 44 20 61 40.
2. Man kan ringe gratis til Cyberhotlinen for digital sikkerhed for vejledning under og efter et cyberangreb på 33 37 00 37.
3. Anmeld angrebet til politiet på 114. I skal huske at melde et evt. tab af persondata til Datatilsynet