Cyber beredskabsplan

Under cyberangreb – 5 vigtigste steps i dit beredskab

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.
4. Ring med det samme til Tryg for at få hjælp til at afværge angrebet og håndtere konsekvenserne.
5. Anmeld angrebet til politiet. Du skal også anmelde sikkerhedsbruddet til Datatilsynet, hvis der er sket tab af persondata.

Tjekliste, når du reetablerer 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 der sket og hvad er ramt? 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.
- ✓ **Hvad var læringen?**
  Lav en plan, som sikrer, at lignende cyberangreb opdages med det samme, og at jeres systemer og procedurer forbedres.

Kontaktoplysninger

Ring til Tryg døgnet rundt
44 20 61 40

Ring **114** eller anmeld på
politi.dk/hacking

Anmeld angrebet til Datatilsynet på
datatilsynet.dk/sikkerhedsbrud

Indsatsleder i tilfælde af cyberangreb

Jobtitel _____

Navn _____

Telefon _____

Ansvarlig for kontakten til eksterne it-eksperter

Jobtitel _____

Navn _____

Telefon _____

Tryg | Klausdalsbrovej 601 | 2750 Ballerup
Tryg Forsikring A/S | CVR-nr. 24260666

FAK 20303 (03.22)