Det skal du gøre ved et cyberangreb

Før
- Lav en risikovurdering af jeres virksomhed og jeres data
- Har I det ønskede sikkerhedsniveau? Lav en GAP-analyse og opdag evt. sikkerhedsmangler
- Lav en beredskabsplan med navne, kontaktinformationer og actions
- Sørg for, at medarbejderne har det rette kompetenceniveau
- Lav øvelser og test, at beredskabsplanen fungerer
- Tag backup, test backup og hav en offline-kopi af data
- Opdater altid al jeres software
- Supplér evt. sikkerhedsværnet med Prevention-, Detection- og Response-løsninger
- Tjek indgående og især udgående trafik for mistænkelig adfærd
- Log alle hændelser og sørg for, at alle logs bliver opsamlet
- Sæt alarmering op, så I bliver underrettet ved tegn på angreb

Under
- Find beredskabsplanen frem og følg den
- Skab et overblik over omfanget. Hvem, hvad og hvor mange er ramt?
- Analysér hændelsen ved brug af logs og sikkerhedsløsninger
- Prioritér indsatsen
- Isolér og begræns skaden. Tag evt. kompromitterede enheder af netværket
- Reinstallér evt. inficerede computer (brug backup'en)

Efter
- Dokumentér angrebet, og hvad I har gjort for at bekæmpe det og stoppe spredning
- Automatisér de handlinger, der udgør modsvaret til angrebet Ex begræns skaden
- Følg aldrig cyberkriminelles anvisninger til ex at betale løsesum
- Meld angrebet til politiet
- Evaluer, hvad I bør gøre anderledes fremadrettet

Har du brug for hjælp?
Kontakt TDC Erhverv 70 70 90 90 eller vores sikkerhedseksperter på: raadgivning@tdcsikkerhed.dk

TDC A/S, CVR 14 77 39 08, Communication/MC 9328.1720