Appendiks 10. Akut checkliste ved cyberhændelser

Tabellen til højre viser et eksempel på en akut checkliste ved en cyberhændelse.

Checklisten er illustrativ:

- ✓ Alle sikkerhedshændelser er forskellige
- ✓ Der findes ikke én checkliste, der dækker alle situationer
- ✓ Det er vigtigt at kunne være fleksibel i reaktionen

Det vigtigste arbejde sker *før,* virksomheden bliver ramt, bl.a. ved etablering af en *incident response* plan, sikring af backup og evt. indgåelse af aftale med en ekstern sikkerhedspartner, der kan hjælpe.

Efter en kritisk hændelse kommer ofte en lang proces med at sikre, at angrebet er ordentligt elimineret, systemer er genetableret (ofte fra backup), og alle sårbarheder er udbedret.

På bl.a. https://sikkerdigital.dk/virksomhed/naar-skaden-er-sket findes overordnet hjælp til nogle af de mest almindelige typer hændelser.

#	Akut checkliste	Eksempler
1	**Undgå panik og bevar roen**	› Betal ikke de kriminelle
2	**Få overblik over problemet**	› Bed om en root cause analyse
3	**Begræns den akutte skade**	› Isoler hændelsen hvis muligt › Afbryd forbindelsen til internettet › Afbryd forbindelsen til netværket › Sluk ikke for computerne › Skift password › Kontakt banken (ved økonomisk svindel)
4	**Brug Incident Response planen**	› Processen for hændelseshåndtering ligger typisk hos systemejerne
5	**Få kvalificeret ekstern hjælp**	› Fra bl.a. sikkerhedseksperter, jurister og leverandører
6	**Prioritér indsatsen**	› Hvad er der sket og hvad er ramt? › Hvad er konsekvensen for forretningen? › Implementer en plan for forretnings kontinuitet › Er der kompromitteret persondata? › Fokus: Er der (stadig) en backup, der virker?
7	**Kommunikér klart og løbende**	› Intern underretning til ledelse og medarbejdere › Ekstern kommunikation til samarbejdspartnere og presse
8	**Foretag nødvendige anmeldelser**	› Politianmeldelse › Anmeldelse til Datatilsynet (ved tab af persondata) › Anmeldelse til andre myndigheder (særlig i kritiske sektorer)
9	**Husk dokumentation af forløbet**	› Minutlog og revisionsspor mm.
10	**Sørg for bevissikring**	› Få kvalificeret ekstern hjælp til bevissikring › Pas på ikke at ødelægge beviser › Kopi af inficerede maskiner til efterforskning › Sikring af logfiler
11	**Følg op på udbedringsplan**	› Etablering af overvågning og evt. sikkerhedskontroller, så yderligere forsøg på kompromittering opdages