

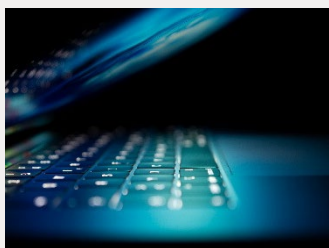
## CYBER READINESS & RESPONSE - BEREDSKAP FØR HENDELSEN INNTRER

Trusselbildet er i endring og antall dataangrep mot norske virksomheter øker. Eksterne aktører tar i bruk AI-baserte prosesser som automatiserer og skalerer selve angrepskjeden. Dataangrep gjennomføres raskere, mer målrettet og med mindre menneskelig innsats. Angrep foregår mer kontinuerlig og tilpasser seg forsvarstiltak underveis, med "uendelig" kapasitet på angripers side.

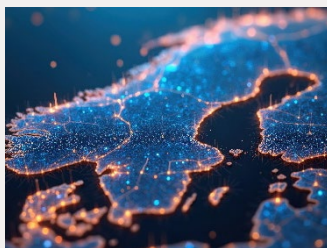
Selv virksomheter med sterke interne ressurser og godt utviklet risikobevisssthet, opplever at de første timene etter en hendelse preges av uklare ansvarsforhold, usikre varslingsfrister og forsinkede beslutninger fordi beredskapen ikke var konkretisert på forhånd.

Schjødt tilbyr nå **Cyber Readiness & Response**, et rammeverk som etablerer den juridiske og organisatoriske infrastrukturen for å reagere hurtig og riktig. Vi kartlegger virksomheten i lys av regelverket som gjelder for bransjen og sektoren, og sørger for at det er avklart hvem i organisasjonen som skal varsle myndigheter, forsikringsgiver, kunder og leverandører, og innen hvilke frister. Dette kombineres med en praktisk plan for selve håndteringen, slik at det er tydelig hvem som tar beslutninger om tiltak, hvilken verktøykasse som er tilgjengelig, og hvilke forebyggende aktiviteter, herunder intern og ekstern kommunikasjon, som skal iverksettes når hendelsen inntreffer.

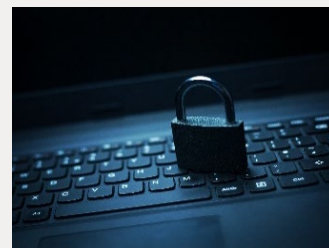
### Cyber Readiness & Response inneholder blant annet:



En samlet oversikt som viser alle varslings- og rapporteringsplikter som utløses ved en cyberhendelse.



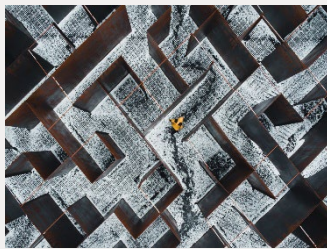
Gjennomgang av kunde- og leverandøravtaler, slik at avtalte varslingsfrister som er kortere enn de lovbestemte blir fanget opp i tide.



Gjennomgang av cyberforsikringen: hva utløser dekning, hvilke krav stilles til advokater og responsleverandører.



En operativ plan for de første timene og døgnene etter en hendelse: hvem leder, hvem beslutter, hva skal være gjort de første 72 timene.



Et forhåndsdefinert, tverrfaglig responsteam dere kan aktivere direkte dersom krisen utløses. Rask, effektiv og klar.



Klar avklaring av beslutningsstrukturen internt: når skal en lokal hendelse eskaleres til konsernnivå?

## OVERSIKT OVER ALT I CYBER READINESS & RESPONSE:

|                                                  |                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Kartlegge gruppestruktur og jurisdiksjon</b>  | Kartlegge hvilke konsernselskaper, virksomhetsområder og land som kan bli berørt av en hendelse, og hvilke regler og myndigheter som gjelder for hver av dem.                                                                                                                                           |
| <b>GDPR &amp; personvern</b>                     | Kartlegge hvem som er behandlingsansvarlig, databehandler osv. for ulike kunder og land, og hvilke tilsynsmyndigheter som kan bli involvert ved en grenseoverskridende hendelse.                                                                                                                        |
| <b>Varslingsplikt til myndighetene</b>           | Gå gjennom kunde-, leverandør- og databehandleravtaler for å finne avtalte frister og plikter ved sikkerhetshendelser, særlig der disse er strengere enn lovkravene.                                                                                                                                    |
| <b>Beredskap for børsnoterte selskaper</b>       | Lage en prosess for å vurdere om en hendelse er innsideinformasjon. Samt kartlegge hvem som skal vurderer dette, hvem som beslutter utsatt offentliggjøring, og hvordan børsmelding kan sendes om vanlige systemer er nede.                                                                             |
| <b>Styring og beslutninger ved hendelse</b>      | Klargjøre hvem som leder responsen og hva som skal avgjøres av ledelsen, juridisk avdeling, konsernledelsen og styret, inkludert eskalering og bruk av eksterne rådgivere.                                                                                                                              |
| <b>Cyberforsikring og skadebegrensning</b>       | <p>Gjennomgå forsikringsvilkårene: hva som dekkes, varslingskrav, samtykke før kostnader pådras, egenandeler og dokumentasjonskrav.</p> <p>Lage en plan for når juridiske og forsikringsmessige vurderinger ikke er like, for eksempel om kundevarsel bør gis selv om det ikke er juridisk påkrevd.</p> |
| <b>Forhåndsgodkjente rådgivere</b>               | Avklare forsikringens krav til advokater og andre rådgivere, og søke om at Schjødt godkjennes som fast rådgiver. Klargjøre eventuelle begrensninger i pris og omfang.                                                                                                                                   |
| <b>Struktur for håndtering over landegrenser</b> | Etablere en overordnet struktur der Schjødt kan koordinere arbeidet med egne team i Norden/UK og lokale advokater andre steder, og avklare hvordan varsler og kommunikasjon koordineres på tvers av land.                                                                                               |
| <b>Eksternt responsteam</b>                      | På forhånd identifisere tekniske-, forensiske- og kommunikasjonsrådgivere i tillegg til lokale advokater, og sjekke om disse er godkjent av forsikringsselskapet.                                                                                                                                       |
| <b>Praktisk handlingsplan ved hendelse</b>       | En konkret plan for de første timene og dagene: hvem skal involveres, hvilke beslutninger må tas, og hvordan de ulike sporene skal koordineres, med klare trinn for første time, første døgn og de første 72 timene.                                                                                    |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bevissikring og undersøkelse</b>     | Rutiner for bevissikring, forensisk undersøkelse og dokumentasjon, samt hvordan rådgivere engasjeres for å bevare fortrolighet.                                                                                                                                                                                                                                                                |
| <b>Politi, utpressing og sanksjoner</b> | Avklare når politi eller andre myndigheter bør involveres, og lage en egen prosess for ransomware/utpressing, inkludert sanksjonsregler og eventuell bruk av forhandlere.                                                                                                                                                                                                                      |
| <b>Krisekommunikasjon</b>               | <p>Legge en plan for kommunikasjon med kunder, ansatte, leverandører og media. Avklare hvem som skal ha ansvar for kommunikasjonen, og hvordan sikre at budskap ikke skaper problemer i andre land.</p> <p>I tillegg sørge for reserveløsninger dersom e-post og andre systemer er kompromittert, og at viktige kontaktlister og dokumenter er tilgjengelige uavhengig av disse systemene.</p> |
| <b>Maler for varsler</b>                | Forhåndsutarbeidede utkast til varsler til myndigheter, kunder, forsikringsselskap, styret og eventuelt børsmelding.                                                                                                                                                                                                                                                                           |
| <b>Rapportering til styret</b>          | Rutiner for løpende rapportering og dokumentasjon av beslutninger, viktig for senere myndighetssaker, forsikring og eventuelt ansvar.                                                                                                                                                                                                                                                          |
| <b>Krav mot tredjeparter</b>            | Kartlegge kritiske leverandører og sørge for at bevis håndteres på en slik måte at senere krav ikke svekkes.                                                                                                                                                                                                                                                                                   |
| <b>Øvelse</b>                           | Teste opplegget med en realistisk øvelse som inkluderer frister, kundesvevender, forsikring, flere land og media - ikke bare IT.                                                                                                                                                                                                                                                               |
| <b>Løpende oppdatering</b>              | Avklare når materialet skal oppdateres (oppkjøp, nye land, nye leverandører m.m.), som grunnlag for en løpende avtale med periodiske gjennomganger og øvelser.                                                                                                                                                                                                                                 |