HAR DU KRAV PÅ Å FÅ VITE DET NÅR KONTRAKTSPARTEN DIN BLIR HACKET?

Vellykkede cyberoperasjoner mot norske virksomheter er tredoblet på et halvt år, samtidig som agentisk kunstig intelligens flytter deler av angrepet til maskinhastighet. For personopplysninger og enkelte regulerte tjenester finnes lovbestemte varslingsregler. For din proprietære og konfidensielle informasjon er det ofte kontrakten som avgjør om du får vite det.

Nasjonal sikkerhetsmyndighet (NSM) hevet 27. oktober 2026 det nasjonale cyberrisikonivået til høyt og publiserte vurderingen åpent for første gang. NSM har det siste halve året sett en tredobling av vellykkede cyberoperasjoner mot norske virksomheter, og peker på språkmodeller og agentiske KI-systemer i cyberoperasjoner som en alvorlig risiko. Microsoft opplyste 21. oktober 2026 at en statstilknyttet aktør siden september har brukt det agentiske KI-rammeverket ARTEX til å automatisere angrep mot hundrevis av virksomheter innen blant annet energi, industri, finans, programvare og juridiske tjenester, og at det i flere tilfeller gikk under tre timer fra første målretting til angriperen hadde privilegert tilgang til virksomhetens skymiljø. Veien inn var en kompromittert tjenesteleverandør.

Dette er bakteppet for at Schjødt nå lanserer Cyber Readiness & Response, et juridisk og organisatorisk beredskapsrammeverk som gjør virksomheten i stand til å håndtere alvorlig hendelser.

Én side av beredskapen er mer oversett enn de andre, og det er den dette nyhetsbrevet handler om.

Personopplysninger har et varslingsregime. Hva med forretningshemmelighetene?

Lovgivningen har detaljerte varslingsregler på enkelte områder. Personvernforordningen krever at den behandlingsansvarlige melder et brudd på personopplysningssikkerheten til Datatilsynet senest innen 72 timer etter å ha fått kjennskap til det, mens databehandleren skal varsle den behandlingsansvarlige uten ugrunnet opphold. Digitalsikkerhetsloven krever at tilbydere av samfunnsviktige tjenester varsler tilsynsmyndigheten, med kopi til NSM, innen 24 timer etter at de fikk kjennskap til en hendelse som virker betydelig inn på tjenesteleveransen. For finanssektoren kommer særregler etter DORA i tillegg.

I energi, shipping og infrastruktur ligger noe av virksomhetens mest verdifulle informasjon ofte utenfor selskapets egne systemer. Fartøysdesign, prosess- og systemtegninger, reservoar- og produksjonsdata, tekniske spesifikasjoner, pris- og kontraktsinformasjon, kildekode, sårbarhetsrapporter og driftsdata deles med verft, utstyrsleverandører, kunder, rådgivere, klasseselskaper og programvareleverandører. Tilsvarende gjelder i andre bransjer for blant annet transaksjonsmateriale, strategier, anbud og finansielle modeller. Når sikkerheten svikter hos en av disse, finnes det utenfor særregulerte tilfeller ingen generell lovfestet varslingsplikt som sikrer at du får vite det.

Forretningshemmelighetsloven gjør kontraktsreguleringen enda viktigere. Vernet forutsetter at innehaveren har truffet rimelige tiltak for å holde informasjonen hemmelig. Forarbeidene peker uttrykkelig på kontraktsfestede konfidensialitetsforpliktelser overfor oppdragstakere og eksterne samarbeidspartnere som et relevant tiltak. Mangelfull kontraktsregulering kan derfor få betydning ikke bare for hva som skjer etter et brudd, men også for om opplysningene har det rettslige vernet som en forretningshemmelighet.

Forbud mot å dele er ikke det samme som plikt til å varsle

De fleste kontrakter sier mye om at informasjonen skal holdes hemmelig, og lite om hva som skal skje den dagen hemmeligholdet svikter. De alminnelige leveringsbetingelsene i nordisk industri, NL 17 og Orgalim S 2022, forbyr videreformidling av tegninger og dokumenter, men pålegger ingen plikt til å si fra når de likevel kommer på avveie. De fleste konfidensialitetsavtaler sier det samme. Der varsling er nevnt, er det ofte som en plikt til å "notify promptly", uten terskel, frist eller innhold.

Det største hullet ligger ofte i virksomhetens egne standardvilkår. Mange selskaper i energi, shipping, infrastruktur og industri opererer med innkjøpsbetingelser, leverandørvilkår, rammeavtaler og konfidensialitetsavtaler som har vært videreført og justert gjennom mange år. De kan være detaljerte om hvem som får motta konfidensiell informasjon, men helt tause om hva leverandøren skal gjøre dersom uvedkommende får tilgang til den ved en sikkerhetshendelse. En oppdatert intern cyberpolicy hjelper lite dersom kontrakten mot den som faktisk sitter på informasjonen, ikke er oppdatert.

De nyeste standardkontraktene har begynt å ta tak i det. NF 25 og NTK 25 fikk i desember 2025 en artikkel 35 om digital sikkerhet, med en gjensidig plikt til å varsle den andre parts kontaktpunkt uten ugrunnet opphold om sikkerhetshendelser som er egnet til å ramme den andre part. Frist, innhold og samarbeid er overlatt til et vedlegg som partene selv må fylle. SHIP25 fra oktober 2025 går lengst. Verftet skal varsle rederiet senest innen tolv timer, også om hendelser hos underleverandører, og gi en første vurdering av alvor og konsekvenser. Men plikten er knyttet til fartøyet og verftets leveranse, ikke til rederiets konfidensielle informasjon som sådan, og verftets ansvar for brudd på klausulen er begrenset til 0,25 prosent av kontraktsprisen.

For svært mange avtaler er svaret på spørsmålet i overskriften derfor fortsatt nei.

Hvorfor det haster

Microsofts ARTEX-sak viser hva det nye tempoet betyr i praksis. I flere av angrepene gikk det under tre timer fra første målretting til privilegert tilgang. NSMs grunnprinsipper for IKT-sikkerhet, som tiltakspakken av 27. oktober bygger på, anbefaler at virksomheter undersøker om leverandøren har rutiner for hendelseshåndtering og sikkerhetsrapportering. Hvem leverandøren skal rapportere til, og hvor raskt, må virksomheten selv sikre i kontrakten.

For enkelte virksomheter løper samtidig egne lovbestemte frister. Etter digitalsikkerhetsloven skal tilbydere av samfunnsviktige tjenester varsle innen 24 timer etter at de selv fikk kjennskap til hendelsen, og NSM understreker at fristen er absolutt også når hendelsen skjer hos en samarbeidspartner eller underleverandør. I tillegg kan kontrakter, forsikring og børsregelverk utløse egne varslings- og handlingsbehov. Når angrepet utvikler seg på timer, er en kontrakt som lar leverandøren vente med å varsle til egen undersøkelse er ferdig, ikke god nok.

Vår vurdering

Etter vår vurdering bør varsling om sikkerhetshendelser behandles som en ordinær del av kontraktsreguleringen mellom partene, på linje med varsling om forsinkelse og mangler. Klausulen bør inn i konfidensialitetsavtalen, standardvilkårene og de viktigste leverandør- og samarbeidsavtalene, og den bør regulere minst seks forhold. Hva som utløser plikten, der terskelen bør omfatte faktisk eller begrunnet mistanke om uautorisert tilgang, uten krav om bevis for at informasjonen er brukt eller hentet ut. En konkret maksimalfrist i timer, satt etter informasjonens betydning og virksomhetens egne varslingsplikter. Markedet spenner fra tolv timer, der SHIP25 nå ligger, til 72 timer, der kjøperens egne frister til tilsynene er styrende, og for særlig verdifull informasjon bør utgangspunktet ligge i den nedre delen av spennet. At første varsel skal gis på det grunnlaget som foreligger, og ikke vente på at undersøkelsen er ferdig. At leverandøren skal begrense skaden og bevare logger og andre relevante bevis. At plikten føres videre til underleverandører, rådgivere og leverandører av sky- og KI-tjenester. Og at ansvaret for rimelige kostnader til undersøkelse, varsling og tapsbegrensning reguleres uttrykkelig.

Klausulen bør være gjensidig. De fleste virksomheter er både kjøper og leverandør, og den plikten man krever av egne leverandører, vil man møte fra egne kunder. En cyberklausul er dessuten bare så effektiv som kontraktskjeden bak den. En utmerket klausul mot hovedleverandøren hjelper lite dersom hovedleverandøren ikke har de samme rettighetene mot den underleverandøren der hendelsen faktisk

skjer. Det er også grunnen til at klausulen hører sammen med virksomhetens egen beredskap. En kontraktsfestet frist er bare verdt noe dersom organisasjonen selv er i stand til å reagere innen den.

Hva bør virksomheter gjøre nå?

Styret og ledelsen bør be om svar på fire spørsmål.

- Hvilken proprietær og konkurransesensitiv informasjon har vi delt med leverandører, kunder og samarbeidspartnere?
- Hvilke av disse har en kontraktsfestet plikt til å varsle oss ved et sikkerhetsbrudd, og innen hvilken frist?
- Er våre egne standardvilkår, konfidensialitetsavtaler og viktigste leverandør- og samarbeidsavtaler oppdatert for cyberhendelser, og er varslingsplikten ført videre gjennom kontraktskjeden?
- Er vår egen organisasjon i stand til å oppfylle de varslingsfristene kunder, tilsyn og forsikringsselskap stiller til oss?

Schjødt har utarbeidet en standardklausul for varsling om sikkerhetshendelser som tilpasses den enkelte virksomhet og bransje, og bistår med gjennomgang av konfidensialitetsavtaler, standardvilkår og leverandøravtaler. Gjennomgangen inngår i Schjødt Cyber Readiness & Response, der vi også etablerer varslingsmatrise, juridisk responsplan og forhåndsavtalt responsteam, og er tilgjengelige hele døgnet når hendelsen inntreffer. Ta kontakt med Torkel Hope, Camilla Bråfelt, Stian S. Tennfjord eller din faste kontaktperson i Schjødt.

Spørsmålet styret bør stille i dag, er enkelt. Hvis en leverandør, kunde eller rådgiver med tilgang til vår mest verdifulle informasjon blir kompromittert i kveld, får vi vite det i tide, og vet vi hva vi skal gjøre i morgen tidlig?