Norske bedrifter er underforsikret:

Cybertrusselen øker – styret kan få regningen

Til tross for stadig mer avanserte cyberangrep, står mange norske bedrifter uten forsikring. Når angrepet først skjer, kan styret bli sittende med ansvaret.

Tekst: Stine Grihamar og Oliver Orskaug

Phishing, deepfakes og usynlige hull i programvaren. Cyberangrep handler ikke lenger bare om enkle svindelforsøk – de er målrettede, sofistikerte og kan være nesten umulige å oppdage.

– Behovet for cybersikkerhet og dermed også forsikring er økende. Det vi ser, er at flere aktører tilbyr forsikring. Også en del norske selskaper tilbyr gode cyberforsikringsprodukter, sier Lars Albert Jøstensen, advokat og partner i CMS Kluge.

Jøstensen, som har vunnet kategorien lovende talent innen forsikringsrett i Advokatundersøkelsen både i 2023 og 2024, overtok ansvaret i forsikringsgruppen i CMS Kluge i vinter. Før det jobbet han med forsikringsrett i DLA Piper.

Flere burde vært forsikret

Han forteller at cyberforsikring er nyttig for alle virksomheter, men at det er først og fremst små og mellomstore selskaper som bør vurdere å ha en cyberforsikring.

Cyberforsikringer er utviklet for å beskytte bedrifter mot økonomiske tap som følge av cyberangrep, inkludert databrudd og ransomware-angrep.

– Forsikring er jo et veldig nyttig instrument for å redusere risikoeksponeringen til selskapet. Små og mellomstore selskaper mangler kapasiteten som større selskaper har til å beskytte seg. Mange av dem har heller ikke ressurser til å bygge opp egne team som kan håndtere det stadig mer komplekse risikobildet, sier han.

– *Hvor vanlig er cyberforsikring i Norge?*

– Det er blitt mer vanlig. Men det er fortsatt et produkt som ikke alle har, og det er sikkert flere som burde hatt det.

Han legger til at forsikring er ett av flere tiltak i møte med cyberrisiko.

– Det er viktig å huske på at selv med forsikring må virksomheten jobbe aktivt med cybersikkerhet, sier han.

Gratis sikkerhetsvurdering

For at bedrifter som er bakpå skal komme i gang med å identifisere eventuelle sikkerhetssårbarheter, har Finans Norge Forsikringsdrift lansert en gratis cybersikkerhetsvurdering.

Bedrifter får tilbakemelding om hvor robuste de er med tanke på dataangrep.

– Analysen er gratis og består av tre nivåer som passer spesielt godt for små og mellomstore bedrifter, sier kommunikasjonssjef Stine Neverdal i Finans Norge Forsikringsdrift.

Foto: Aon Norway

– Invester i forebyggende tiltak: Linn Jeanette Johansen, kommersiell leder i Aon Norway.

Nytt EU-regelverk: CMS Kluge-partner Lars Albert Jøstensen advarer om at styret kan bli gjort ansvarlig etter cyberangrep.

> **Det farligste man gjør som styre og ledelse er å skyve ting under teppet og tenke at cyberrisiko ikke angår ens egen bedrift**
>
> Lars Albert Jøstensen, CMS Kluge

Foto: Iván Kverme

– Sørg for god opplæring av de ansatte

Økokrim har sett mange eksempler på at kriminelle kommer inn i bedrifter via svakheter hos leverandørene.

Økokrim-sjef Pål Lønseth understreker at næringslivet selv har et ansvar for å beskytte seg mot digital svindel. God cybersikkerhet i egen virksomhet er viktig, men minst like avgjørende er det å sikre hele verdikjeden.

– Jeg har sett mange eksempler på at kriminelle kommer inn i virksomheten via svakheter hos leverandørene, sier han.

– Økende trend

I tillegg mener han det er viktig at bedriftene sørger for at de ansatte besitter kompetansen som trengs for å minske risikoen for å bli lurt.

– Sørg for å innarbeide rutiner og god opplæring av de ansatte, sier han.

Et økende problem er såkalt innsiderisko. Dette må også selskapene være klar over,understreker Lønseth.

– I utlandet er dette en økende trend. Finans Norge har utviklet en egen veileder på innsiderisiko for finansnæringen, og det norske politiet har etterforsket flere saker mot innsidere i finanssektoren. Etter hvert som selskapene blir bedre på cybersikkerhet, forsøker kriminelle i større grad å rekruttere personer på innsiden. Derfor må også HR-avdelinger tenke sikkerhet i rekrutteringsprosesser, sier Lønseth.

Kripos eller Økokrim

– Hva er rådet til bedrifter som allerede er rammet av cyberkriminalitet?

– Det kommer an på hvordan man blir rammet. Er det tjenestenektangrep ta kontakt med Kripos. Er det svindel mot virksomheten, må man anmelde til oss i Økokrim.

Foto: Thomas Brun/NTB kommunikasjon

Statuskontroll: Kommunikasjonssjef Stine Neverdal i Finans Norge Forsikringsdrift tilbyr gratis analyse av bedrifters cybersårbarhet og råd til sikkhetsgrep som bør tas.

Foto: Aon

Kjøpervennlig marked: Søren Stryger, meglersjef for cyberforsikringer i Europa, Midtøsten og Afrika i Aon.

Første nivå tar omtrent én time å gjennomføre og består av en kartlegging av 15 grunnleggende tekniske sikkerhetstiltak alle bedrifter bør få avklart om er på plass.

Disse tiltakene kan, hvis de gjennomføres, forhindre opptil 80 prosent av dataangrep som bedrifter typisk rammes av.

– Det er viktig å være føre var, da skadene etter slike angrep kan bli omfattende, sier Neverdal.

Ønsker bedrifter en utvidet cybersikkerhetsvurdering etter første nivå, kan gå til nivå to. Da vil 20 sikkerhetstiltak bli kartlagt, blant annet knyttet til risiko, prosesser og organisering i organisasjonen. Vurderingene retter et spesielt søkelys mot ledelsen. Gjennomgangen tar tre til fire timer.

– Etter hvert gjennomførte nivå, får man en detaljert rapport med anbefalinger om hvordan bedriften kan styrke sin cybersikkerhet, sier Neverdal.

Dersom bedriften ønsker en mer omfattende vurdering, kreves mer teknisk kompetanse og to–tre halvdagsmøter til selve gjennomgangen.

Da blir man presentert for 118 tiltak som Nasjonal Sikkerhetsmyndighet mener bedrifter bør ha på plass, skal man være best mulig rustet mot cyberangrep. Alle resultatene fra undersøkelsen lagres trygt hos DNV, så ikke uvedkommende får tilgang til bedriftens eventuelle svakheter.

– Farlig å skyve ting under teppet

CMS Kluge-partner Jøstensen forteller at det har dukket opp tilfeller av styreansvarsproblematikk i kjølvannet av cyberangrep, der det blir hevdet at sikkerheten ikke har vært god nok.

– Dette skjer særlig i tilfeller hvor man ikke får dekket tap hos tredjeparter, og styret forsøkes holdt ansvarlig, sier han og fortsetter:

– Ansvarliggjøringen er blitt mer aktuell blant annet gjennom innføringen av NIS 2-direktivet i EU. Regelverket stiller tydelige krav til styrets og ledelsens ansvar for forsvarlig cybersikkerhet – selv om det foreløpig ikke er implementert i Norge.

– Det vil si at styreansvarsforsikring er blitt enda viktigere?

– Ja, men man bør ha styreansvarsforsikring uavhengig av denne trenden, rett og slett fordi det er et betydelig ansvar å sitte i et styre, sier han.

– Det farligste man gjør som styre og ledelse er å skyve ting under teppet og tenke at cyberrisiko ikke angår ens egen bedrift.

Phishing og deepfakes

En av de vanligste angrepsformene er å utnytte svakheter i programvarer, såkalt software vulnerability, forklarer Jøstensen. Dette kan skje dersom bedriften for eksempel ikke har lastet ned programvareoppdateringer, eller gjennom

utnyttelse av ukjente svakheter i systemet, såkalt «nulldagssårbarhet».

– I tillegg brukes phishing, der ansatte mottar en skadelig epost som enten har som formål å lokke epostmottagere til å dele personopplysningene sine, eller å plante skadelig programvare gjennom et vedlegg eller en lenke, sier han.

I starten av krigen mellom Russland og Ukraina gikk angrepene ned en periode, antagelig fordi mange av de sentrale aktørene bak angrepene mot Norge befant seg i disse landene. I den seneste tiden har kunstig intelligens bidratt til å endre trusselbildet.

– Det har gjort phishing og målrettede angrep vanskeligere å oppdage, fordi verktøy som oversettelser og deepfakes er blitt mer avanserte, sier han.

10–15 prosent har forsikring

Ifølge forsikringsmegleren Aon er fortsatt mange bedrifter underforsikret.

– Alle bedrifter, uavhengig av størrelse, bør vurdere cyberforsikring. Trusselen er ikke begrenset til store selskaper; små og mellomstore bedrifter er også utsatt. Aon anslår at kun 10-15 prosent av mellomstore bedrifter har en cyberforsikring, sier Søren Stryger, meglersjef for cyberforsikringer i Europa, Midtøsten og Afrika i Aon.

Han sier markedet for disse forsikringene har utviklet seg de seneste årene.

– Prisene har stabilisert seg etter noen turbulente år, og det er nå et kjøpervennlig marked for de som har investert i sikkerhet og risikoplaner, sier han.

Også Aon understreker at forsikringen ikke dekker alt.

– Bedrifter må derfor også investere i forebyggende tiltak for å minimere risikoen, sier Linn Jeanette Johansen, kommersiell leder i Aon Norway.

Hun utdyper at norske forsikringsselskaper tilbyr løsninger, men det kan være begrensninger på erstatningssum og hva som dekkes.

– For å få en cyberforsikring som dekker faktiske behov, kan det være nødvendig å se til forsikringsmarkeder utenfor Norge, som for eksempel Lloyd's of London eller andre internasjonale aktører, sier hun.

If, Tryg, Gjensidige, Frende og Fremtind er noen av de norske forsikringsselskapene som tilbyr cyberforsikring, mens AIG, Beazley, QBE, Allianz, Chubb, Axa XL, Zurich og HDI er blant de internasjonale.

– Færre cyberhendelser enn fryktet

I det daglige jobber Jøstensen i CMS Kluge hovedsakelig med dekningsspørsmål innen ulike forsikringstyper. Han har også erfaring med hendelseshåndtering og bistår forsikringstagere i forbindelse med cyberangrep.

– Hvor ofte må du bistå forsikringstagere?

– Det har vært en del cyberhendelser opp gjennom årene, men ikke så mange som man kunne fryktet. Det kan tyde på at mange norske virksomheter, i hvert fall de som har tegnet forsikring, er relativt bevisste på risikoen og jobber forebyggende. ■