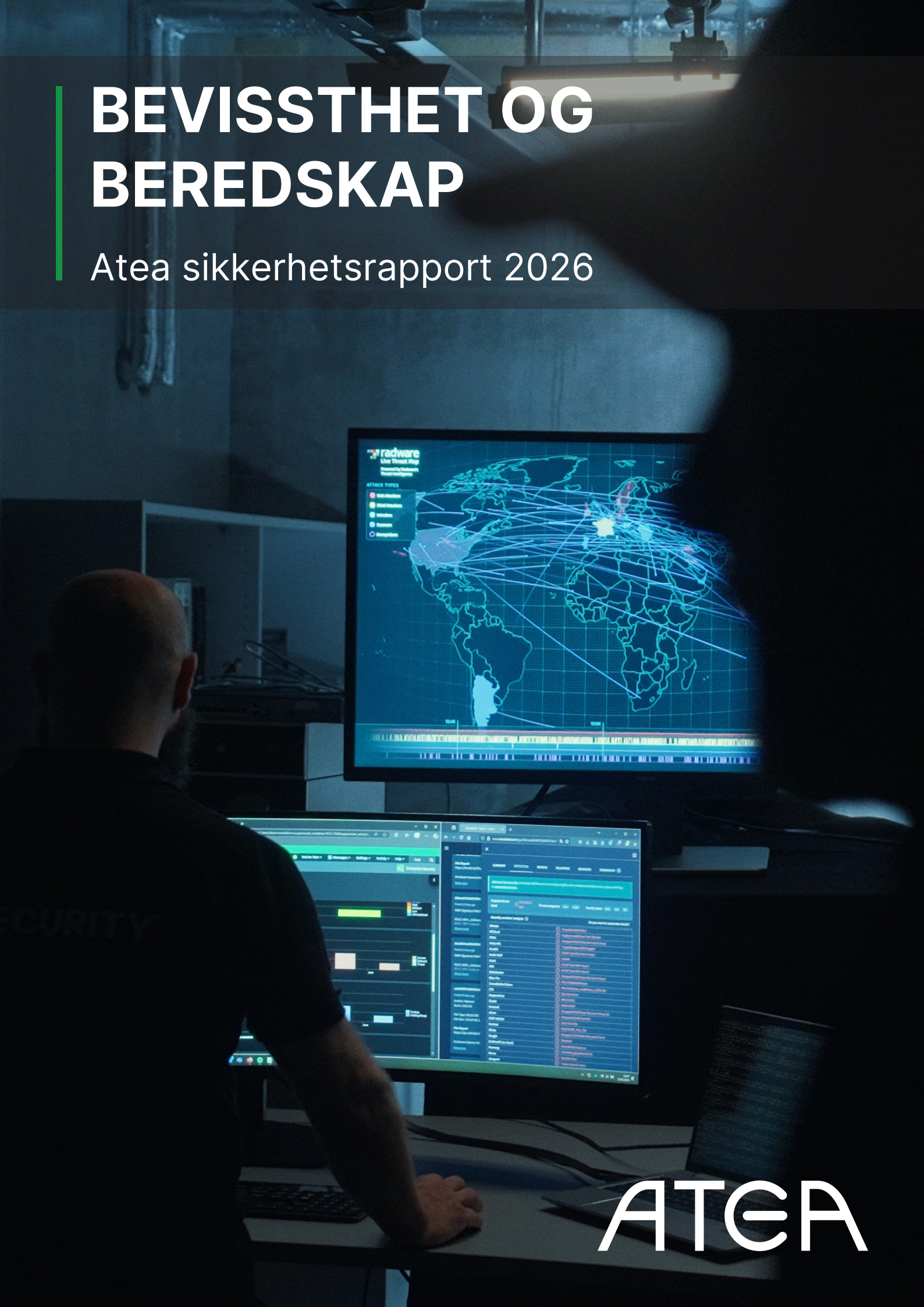
BEVISSTHET OG BEREDSKAP

Atea sikkerhetsrapport 2026



ATEA

INNHOLD

Om undersøkelsen

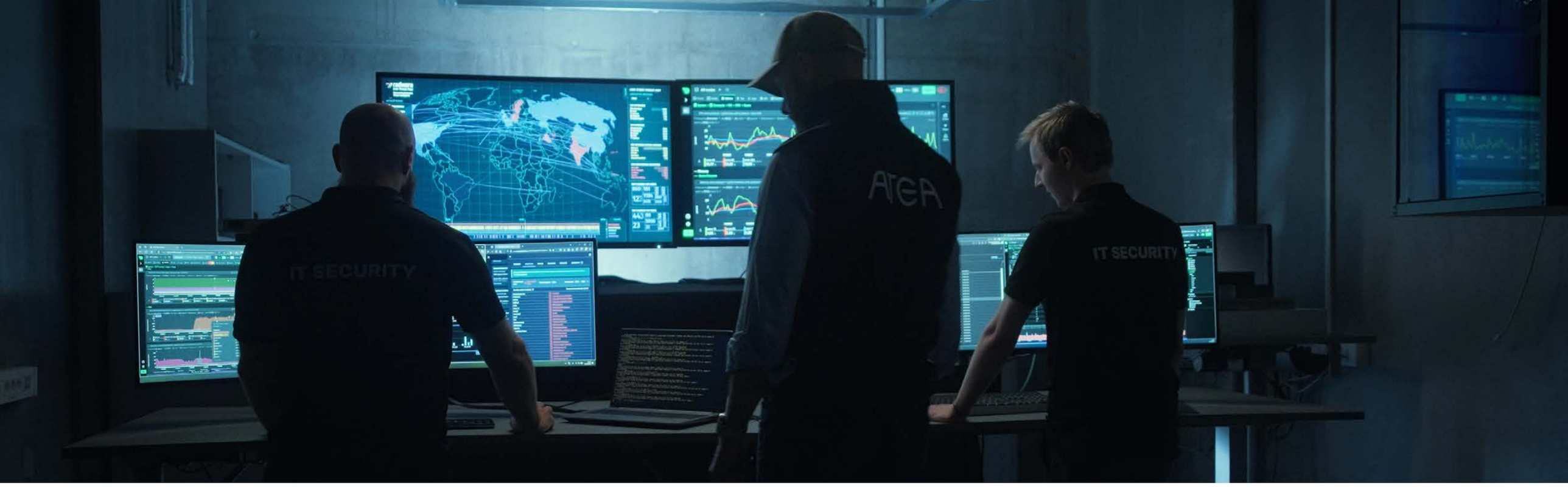
Denne undersøkelsen er gjennomført av Kantar på oppdrag fra Atea. Formålet er å kartlegge IT-sikkerheten i norske virksomheter. Dette er fjerde gang undersøkelsen gjennomføres. Samme metodikk benyttes hver gang for å følge utviklingen over tid.

Intervjumetode:	Web og telefon
Utvalgskilde:	Næringslivsbasen
Intervjulengde:	7 minutter
Feltperiode:	20.01.26 - 16.02.26
Antall intervju:	391
Målgruppe:	Daglig leder / ansvarlig for IT/IT-sikkerhet i norske virksomheter med 20 eller flere ansatte
Utvalg:	Virksomheter med 20 eller flere ansatte

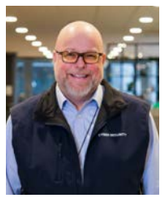
Det er omtrent 33 000 virksomheter i Norge med 20 eller flere ansatte.

Baser i undersøkelsen	**N=**
Ansvarlig for IT/IT-sikkerhet:	261
Daglig leder:	130
Offentlig sektor:	204
Privat sektor:	187
20-49 ansatte:	179
50-99 ansatte:	76
100-249 ansatte:	58
250 ansatte eller flere:	78

Feilmargin uttrykker påliteligheten av et tall. Kantar har på denne målingen intervjuet 391 bedrifter med 20 eller flere ansatte. Utvalgsstørrelsen for denne gruppen er på 14 968. Feilmarginen i dette tilfellet er +/-4.9 prosentpoeng med et konfidensintervall på 95 %.



Skjerpet trusselbilde krever sterkere samarbeid



Thomas Tømmernes
Konserndirektør for IT-sikkerhet
Atea

I årets undersøkelse stilte vi for første gang spørsmål om hvordan verdenssituasjonen påvirker det digitale trusselbildet. Nesten to av tre virksomheter svarer at den urolige situasjonen i verden påvirker risikoen de står overfor. Samtidig ser vi at større virksomheter i enda større grad opplever dette som en betydelig faktor.

Dette samsvarer også med vurderingene fra norske myndigheter. Både Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Etterretningstjenesten peker på et mer alvorlig og sammensatt trusselbilde. Der digitale angrep i økende grad brukes i konflikter mellom stater og mot kritisk infrastruktur.

I et slikt trussellandskap blir samarbeid stadig viktigere. Trusselbildet utvikler seg raskere enn det mange virksomheter kan håndtere alene. Undersøkelsen viser derfor også hvor viktig samarbeidet med eksterne IT-sikkerhetsmiljøer har blitt. Syv av ti virksomheter oppgir at de samarbeider med en ekstern leverandør for å ivareta IT-sikkerheten, og et stort flertall av private virksomheter sier at de vil støtte seg på sin IT-partner dersom de blir utsatt for en alvorlig cyberhendelse. IT-leverandører spiller dermed en viktig rolle i det digitale sikkerhetsarbeidet i Norge. Vi sitter tett på teknologien, følger utviklingen i trusselbildet og bidrar med kompetanse og erfaring som mange virksomheter ikke har internt.

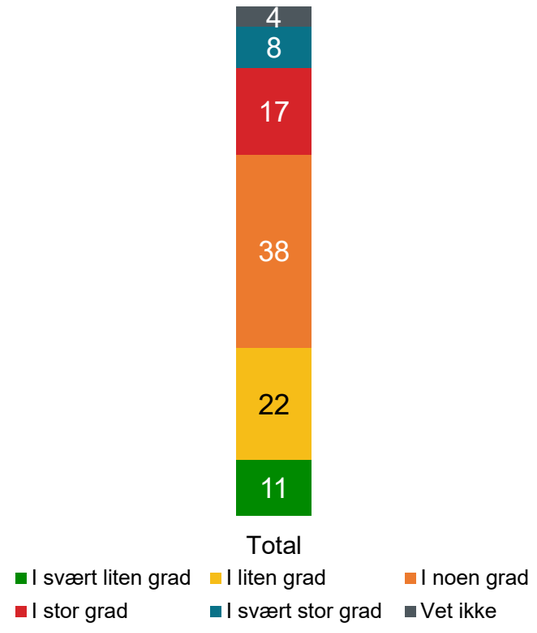
Men vi jobber ikke i et vakuum. For meg peker dette også på noe større. Digital sikkerhet skapes ikke av bare oss i de private sikkerhetsbransjene eller myndighetene. Den utvikles i et samspill mellom virksomheter, leverandører, myndigheter og fagmiljøer. Når dette samspillet fungerer godt, styrkes også den digitale motstandskraften i samfunnet.

Dette er fjerde året vi tar temperaturen på IT-sikkerheten i norske virksomheter. Bak tallene i rapporten ligger erfaringer, vurderinger og prioriteringer fra virksomheter over hele landet. Samlet gir de et bilde av hvordan norske virksomheter arbeider med digital sikkerhet i dag, og hvor innsatsen bør rettes videre.

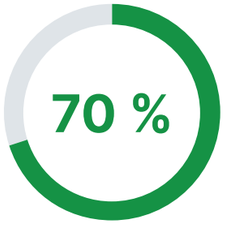
Bruk funnene i rapporten som et utgangspunkt for diskusjon og prioriteringer i egen virksomhet. Løft temaet i ledergruppen og i styret, og vurder hvilke tiltak som er viktigst å starte med. Digital sikkerhet må være en del av den daglige driften og utviklingen av virksomheten.

Virksomheter som arbeider systematisk med sikkerhet styrker både tillit og konkurransekraft.

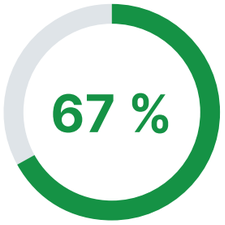
Hvordan verdenssituasjonen påvirker det digitale trusselbildet: *I hvilken grad opplever du at en mer urolig verdenssituasjon (krig, geopolitisk spenning og økt internasjonal konflikt) påvirker det digitale trusselbildet for din virksomhet?*



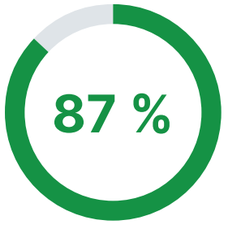
Viktigste funn



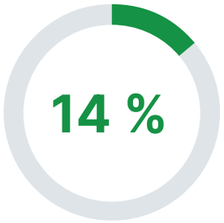
70 % har samarbeid og støtte fra ekstern leverandør for å ivareta egen IT-sikkerhet.



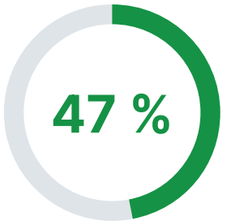
67 % har en beredskapsplan.



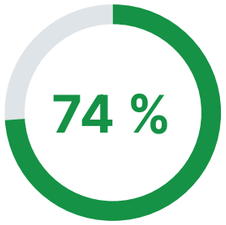
87 % av private virksomheter lener seg på sin IT-partner ved en cyberhendelse.



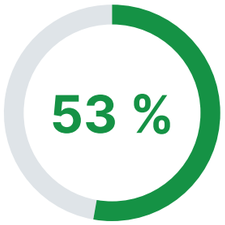
Bare 14 % erkjenner kvanteteknologi som en sikkerhetsrisiko.



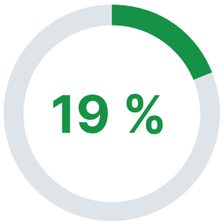
47 % anser kunstig intelligens som en IT-sikkerhetsrisiko for virksomheten.



74 % frykter ansattes bruk av uautoriserte AI-tjenester.



53 % er fortsatt ikke kjent med NIS2-direktivet.



Bare 19 % av private virksomheter opplever at myndighetene har bidratt til å styrke virksomhetens IT-sikkerhet, mot 34 % av de offentlige.

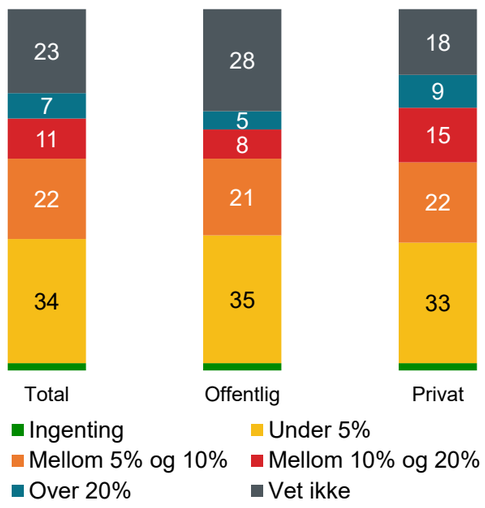
Investeringer og tiltak som former norsk IT-sikkerhet

Ane Svensli
Prosjektleder for IT-sikkerhet
Atea

Som tidligere år starter vi rapporten med å se på økonomi, budsjett og investeringer i IT-sikkerhet hos norske virksomheter. Årets tall viser fortsatt en del usikkerhet i mange virksomheter, hvor 23 % ikke vet hvor stor del av IT-budsjetter som går til sikkerhetstiltak. Usikkerheten er størst i offentlig sektor (28 %), mens private virksomheter ligger på tilsvarende nivå som i 2025 (18 %).

Samtidig ser vi en markant styrking av sikkerhetsinvesteringene i virksomheter med 50 eller flere ansatte, hvor en langt større andel enn i 2025 i år oppgir å bruke 5 % eller mer av budsjettet på IT-sikkerhet.

Budsjett IT-sikkerhet: *Omtrent hvor stor andel av virksomhetens IT-budsjett går til IT-sikkerhet?*



Investeringer i IT-sikkerhet de neste 12 månedene

Tallene viser at stadig flere virksomheter planlegger å øke investeringene i IT-sikkerhet i 2026. Samtidig varierer ambisjonene betydelig mellom både bransjer og virksomhetsstørrelser. Totalt oppgir 39 % at de vil øke budsjettene, mens 37 % ikke planlegger økninger, og 24 % fortsatt er usikre. Som tidligere er det særlig de største virksomhetene, med

Investeringer i IT-sikkerhet i 2026: *Skal virksomheten øke investeringen på IT-sikkerheten i 2026?*

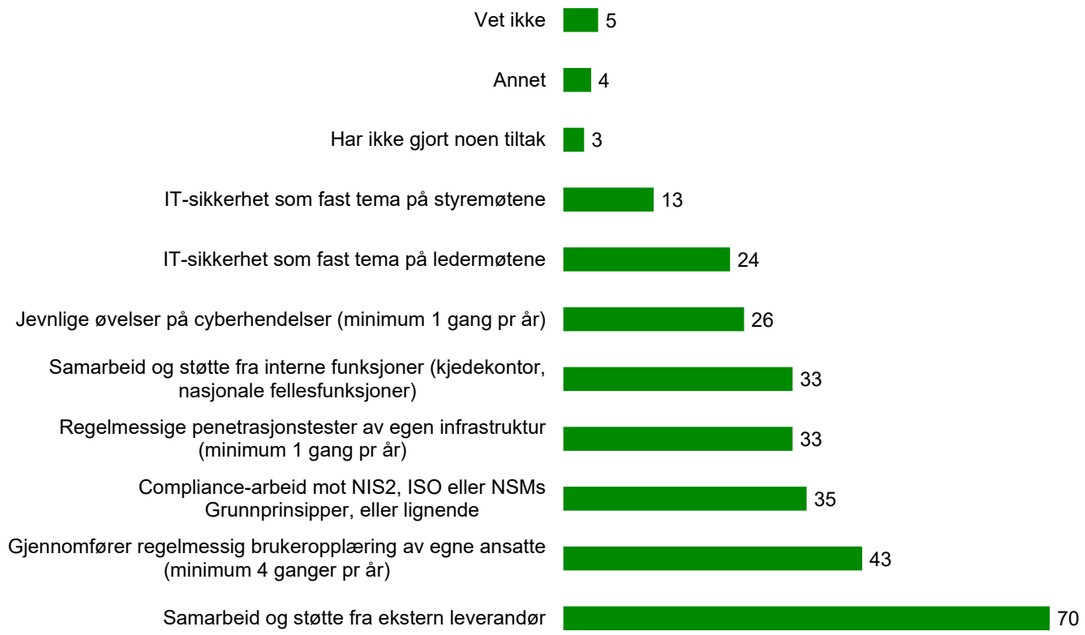
250 ansatte eller flere, som står for den tydeligste veksten, men også små og mellomstore bedrifter viser større investeringsvilje enn før.

At en så stor andel fortsatt svarer «nei» eller «vet ikke», tyder samtidig på at mange virksomheter mangler tydelige prioriteringer og planer for sikkerhetsarbeidet i året som kommer.

Tiltak for å ivareta IT-sikkerhet

For å få innblikk i modenhet og prioriteringer i norske virksomheter, spør vi hvilke tiltak

Tiltak for å ivareta egen IT-sikkerhet: *Hvilke tiltak har virksomheten gjort for å ivareta egen IT-sikkerhet?*



virksomhetene gjør for å ivareta IT-sikkerheten. Årets undersøkelse viser at flertallet av virksomhetene som er spurt tar i bruk eksterne ressurser for å styrke IT-sikkerheten. Dette er et nytt svaralternativ og får hele 70 %, noe som betyr at syv av ti virksomheter har oppgitt dette. Dette er et høyt tall, og understreker hvor viktig tilgang på kompetanse og kapasitet utenfra er.

Vi ser samtidig en positiv utvikling innenfor interne tiltak. Brukeropplæring øker tydelig, fra 34 % i 2025 til 43 % i år. Det er også en mindre økning i gjennomføring av penetrasjonstester (fra 29 % i 2025 til 33 % i år) og at IT-sikkerhet tas opp som tema i styrerommet (fra 9 % til 13 %). Compliance-arbeid og øvelser ligger på omtrent samme nivå som i fjor.

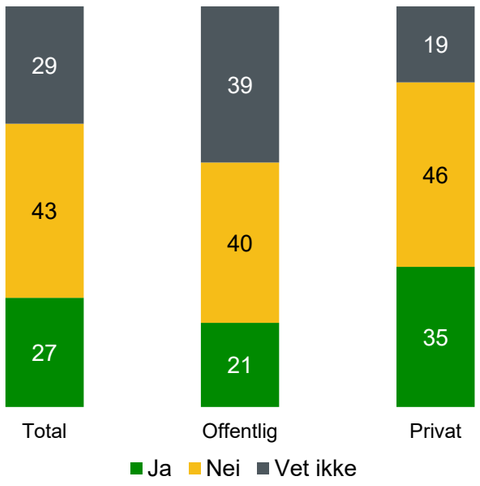
På hvilke tiltak de gjennomfører kan vi se tydelige forskjeller mellom små og store virksomheter. Mens de største virksomhetene i større grad gjennomfører flere ulike sikkerhetstiltak, er aktiviteten mer begrenset blant de mindre. Dette gjenspeiles tydelig i at alle virksomheter med mer enn 100 ansatte rapporterer at de har gjort minst ett tiltak, mens andelen som oppgir «ingen tiltak» faller fra 14 % i 2025 til kun 3 % i år. Vi ser videre at disse 3 % er utelukkende virksomheter med under 100 ansatte.

Oppsummert viser funnene at samarbeid med eksterne leverandører er det klart viktigste tiltaket for norske virksomheter, foran både brukeropplæring og compliance-arbeid.

Økende interesse for cyberforsikring

Siden vi startet med denne undersøkelsen i 2023, har spørsmålet om cyberforsikring fått relativt like svar, frem til i år. Tallene fra årets undersøkelse viser en tydelig og positiv utvikling. Andelen virksomheter som har tegnet cyberforsikring har økt fra 19 % i 2025 til 27 % i 2026. Dette tolker vi som et signal om at stadig flere tar innover seg de økonomiske konsekvensene som cyberangrep kan innebære og ønsker en mer helhetlig risikostyring.

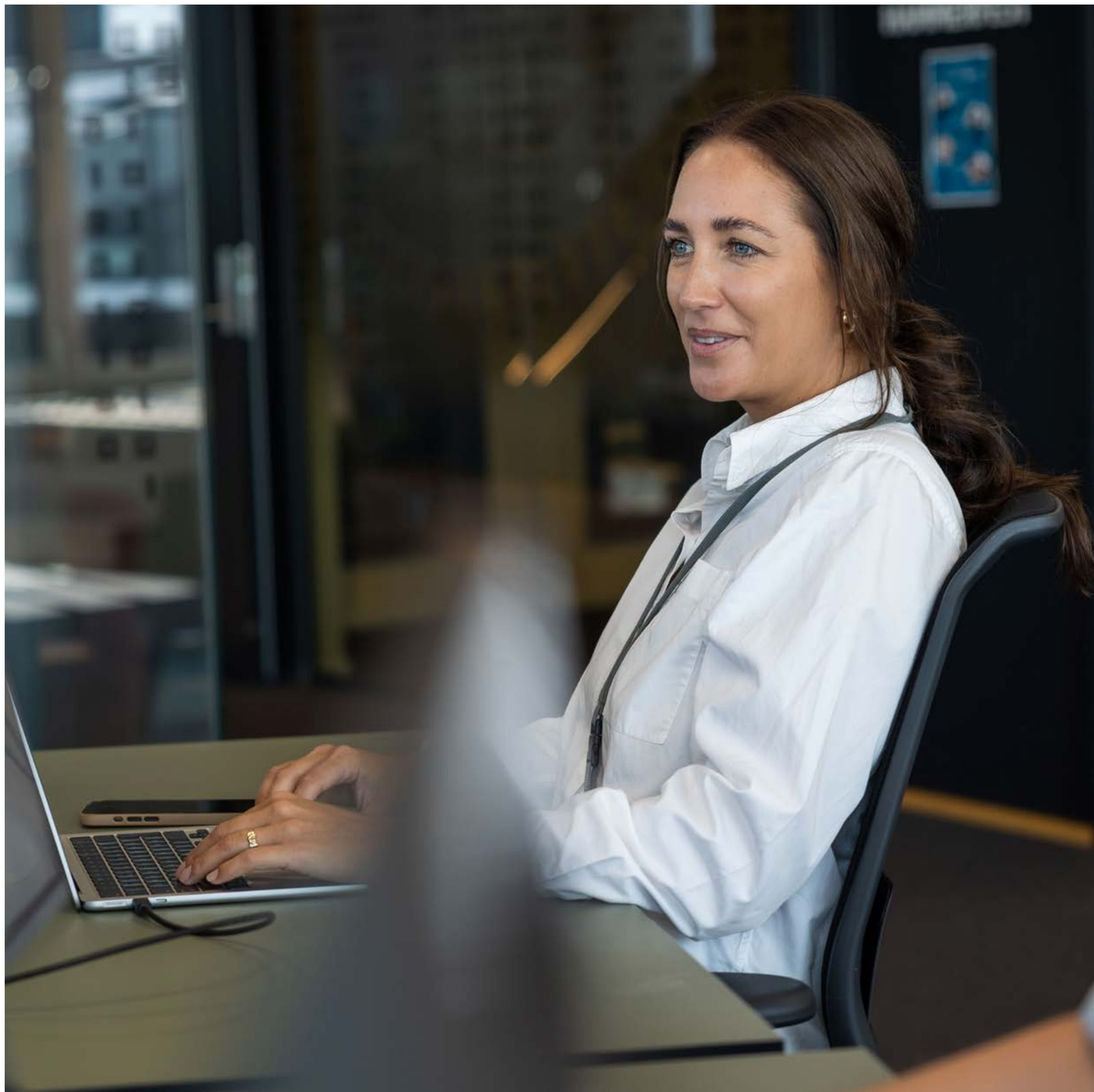
Cyberforsikring: *Har virksomheten cyberforsikring?*



Den største veksten ser vi innenfor bransjen «industri», som har økt fra 28 % i 2025 til 41 % i 2026. Det er også en tydelig forskjell mellom det offentlige og private. I det offentlige oppgir 21 % (9 % i 2025) at de har cyberforsikring, mens i det private er det 35 % (27 % i 2025).

Andelen som svarer «vet ikke» holder seg relativt stabil, noe som kan tyde på at ansvaret for cyberberedskap og forsikring fortsatt kan være fragmentert i enkelte virksomheter.

Den økende interessen for cyberforsikring viser tydelig at norske virksomheter i større grad velger å kombinere tekniske og organisatoriske sikkerhetstiltak med økonomiske virkemidler. Forsikringen blir ikke bare sett på som «nice to have», men som en strategisk del av totalberedskapen. Den representerer dermed ikke bare en økonomisk trygghet, men også et konkurransefortrinn ved at den fungerer som et bevis på at virksomheten tar sikkerhet på alvor.



Dagens beredskap- og trusselsituasjon

Kristin Vegsund Brennan
Business Owner, IRT Norge
Atea

Årets undersøkelse viser at norske virksomheter har opplevd en 8 % økning i hendelser som har krevd håndtering fra IT-avdelingen. Det er samtidig en liten nedgang i angrep som stoppes av sikkerhetssystemer, enn i året før, i både offentlig og privat sektor. Til tross for dette vurderer norske virksomheter risikoen for å bli utsatt for et cyberangrep som uendret fra fjoråret. Hvorav bare 21 % svarer at de ser på cyberangrep som en stor eller svært stor risiko mot deres virksomhet. Dette tyder på at flere norske virksomheter mangler kunnskap og forståelse om trusselbildet de står ovenfor i dag, men også hvilke konsekvenser et eventuelt angrep kan medføre. Når det verste har skjedd, oppdager flere virksomheter at omfanget og konsekvensene av et angrep har vært mer alvorlige enn de hadde forutsett, ifølge Ateas Incident Response Team (IRT).

Om Atea IRT

Atea IRT bistår kunder med håndtering av hendelser. Det kan være alt fra kompliserte og langvarige hendelser, som for eksempel løsepengevirusangrep (ransomware), til mindre hendelser som for eksempel phishing-forsøk og brukeridentitet på avveie. De forteller at kriminelle aktører med finansielle motiver er svært aktive, og at de utnytter at mange norske virksomheter ikke har styrket grunnmuren godt nok. Atea Incident Response Team (IRT) består av høyt sertifiserte og erfarne sikkerhetskonsulenter med bred faglig kompetanse. IRT inngår i Nasjonal Sikkerhetsmyndighets godkjennelsesordning for hendelseshåndtering.

Atea IRT så at disse angrepsmetodene dominerte i 2025

1. **AiTM angrep:** Er en avansert form for phishing hvor trusselaktører infiltrerer og plasserer seg mellom brukeren og en legitim tjeneste for å fange opp innloggingsinformasjon og sesjonsdata
   - Selv ikke to-faktor autentisering beskytter mot AiTM angrep
   - Atea har sett en tydelig økning i slike angrep det siste året
2. **Info-stealer:** Er en skadelig programvare designet for å stjele passord og sensitiv informasjon lagret i brukerens nettleser
   - Har utviklet seg i kompleksitet og spredning det siste året.
   - Medfører konsekvenser for den ansatte personlig og for virksomheten
   - Uten de rette sikkerhetsmekanismene kan en trusselaktør ta seg videre inn i virksomhetens systemer

Nasjonal Sikkerhetsmyndighet (NSM) beskriver dagens sikkerhetspolitiske situasjon som alvorlig, preget av stor usikkerhet og vedvarende spenninger. Etterretningstrusselen vurderes også som økende, ifølge Politiets sikkerhetstjeneste (PST), spesielt mot kritisk infrastruktur. Hvor ondsinnede aktører kartlegger sårbarheter og innhenter informasjon fra digitale systemer. Samtidig påpekes det manglende beredskap hos norske virksomheter, med alt fra risikoanalyse- og forståelse til beredskapsplaner.

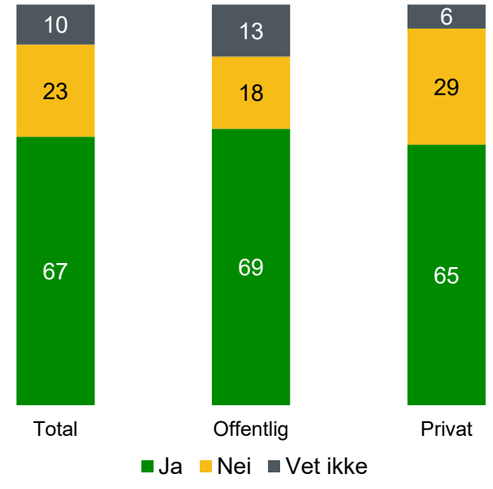
Flere virksomheter fokuserer på beredskap

I dagens sikkerhetspolitiske situasjon er det desto viktigere at norske virksomheter har en plan for hvordan de skal håndtere et angrep. På spørsmål om virksomheten har en beredskapsplan hvis man skulle bli utsatt for en alvorlig IT-sikkerhetshendelse, svarer 67 % at de har en beredskapsplan. 23 % svarer at de ikke har en beredskapsplan, og 10 % vet ikke. Det er flere som har en beredskapsplan enn i året før, spesielt hos de større virksomhetene. NSM påpeker likevel vesentlige mangler i sikkerhetsstyring hos flere norske virksomheter, spesielt i forhold til beredskapsdokumentasjon.

Beredskap må fungere i praksis, ikke bare på papiret

Det er ikke godt nok å bare *ha* en beredskapsplan. Ateas hendelseshåndterere opplever at flere beredskapsplaner er overfladiske, og derfor er

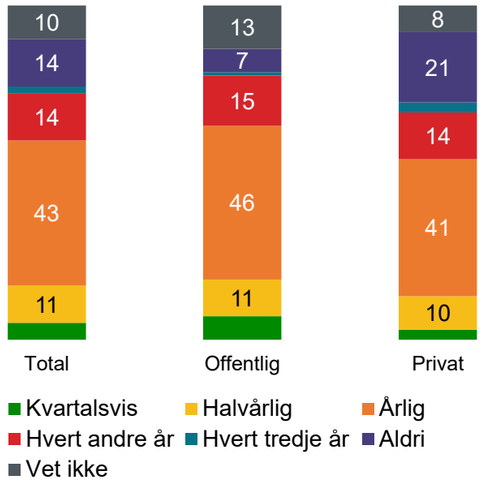
Beredskapsplan: *Har virksomheten en beredskapsplan for å håndtere IT-sikkerhetshendelser?*



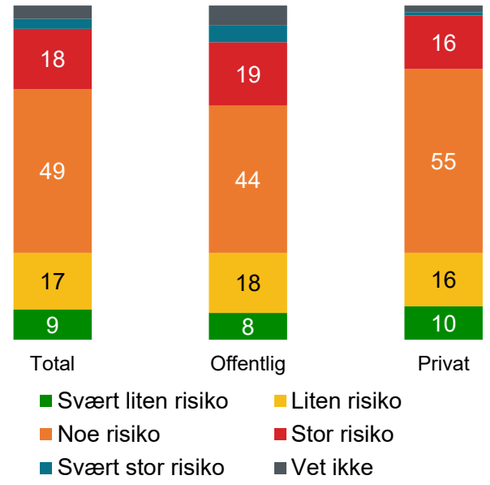
det de færreste som faktisk klarer å benytte seg av den når uhellet er ute. En god beredskapsplan må være anvendelig i kriser. Under en alvorlig hendelse skal det aldri være tvil om hvem som er ansvarlig for hvilke arbeidsoppgaver, eller hvordan virksomheten kommuniseres internt og eksternt, og hvordan det skal prioriteres i en eventuell gjenopprettingsprosess. Derfor må en beredskapsplan definere alt dette tydelig.

Hvor godt beredskapsplanen *faktisk* fungerer, avgjøres til syvende og sist gjennom håndtering av

Øving på beredskapsplan: *Hvor ofte vil du si at det øves på beredskapsplanen?*



Risiko for cyberangrep: *Hvordan vurderer du risikoen for at virksomheten skal bli utsatt for et cyberangrep?*



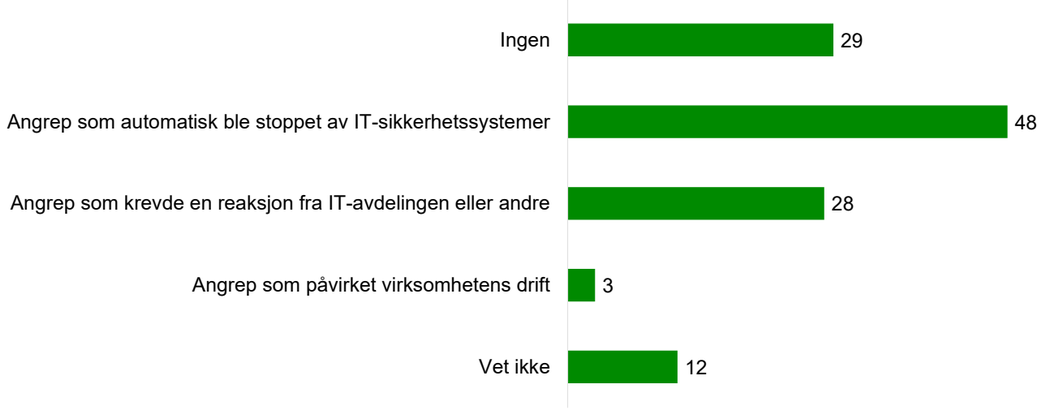
en reell hendelse, eller gjennom beredskapsøvelser. Av de som svarer at de har en beredskapsplan øver i underkant av 60 % årlig eller oftere, hvor de i stor grad involverer ledelsen. Atea IRT har også sett en positiv økning i forespørsler rundt og fokus på beredskapsøvelser hos både offentlige og private virksomheter det siste året.

Det som er bekymringsverdig er at nesten 24 % svarer at de aldri øver, eller at de er usikre på om de øver på beredskap i det hele tatt. Dette tyder på at alt for mange norske virksomheter fortsatt mangler rutiner for å håndtere en alvorlig IT-sikkerhetshendelse om det skulle oppstå.

Styrket motstandskraft gjennom kunnskap og øvelse

Atea IRTs budskap er tydelig: God beredskap er grunnleggende. Norske virksomheter må styrke kunnskap og forståelse om trusselbildet og de potensielle konsekvensene et angrep kan medføre, slik at de kan gjøre gode prioriteringer i sitt beredskapsarbeid. De må ha fokus på å styrke grunnmuren og få kontroll på egen angrepsflate. Og helt til slutt, norske virksomheter må øve på kritiske hendelser slik at de kan møte dagens og morgendagens trusler med trygghet og handlekraft.

Cyberangrep i 2025: *Hvilke typer cyberangrep har virksomheten vært utsatt for i 2025?*



Samarbeid og støtte i møte med dagens cybertrusler

Audun Risberg
BDM Cyber Security
Atea Group

Funnene i årets undersøkelse viser at samarbeid og støtte fortsatt spiller en avgjørende rolle for hvordan norske virksomheter vurderer egen evne til å håndtere alvorlige cyberhendelser. Samtidig avdekkes det tydelige forskjeller mellom virksomhetsstørrelser og graden av modenhet innen IT-sikkerhet.

Mange tror de klarer seg uten IT

Til tross for økt oppmerksomhet og fokus rundt vår digitale sårbarhet, svarer fortsatt 11 % av virksomhetene at de mener de vil kunne klare seg ett år eller mer uten IT-systemer. Dette er et oppsiktsvekkende funn i en tid der digitalisering er dypt integrert i de fleste forretningsprosesser.

Gruppen som i hevder dette, kjennetegnes ellers i undersøkelsen av lavere investeringer i IT-sikkerhet, manglende cyberforsikring og ingen plan om økt sikkerhetsinvestering i 2026.

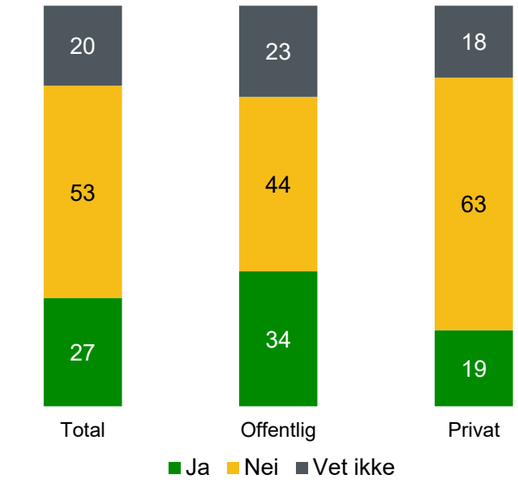
Denne kombinasjonen kan indikere både en undervurdering av reell risiko og en optimisme knyttet til egen risiko og uavhengighet. Dette peker på et behov for økt informasjon, veiledning og støtte, særlig rettet mot sektorer som tradisjonelt ikke har opplevd risikoen av cyberhendelser som relevant.

Myndighetenes rolle

Totalt sett ser vi en jevn økning i andelen virksomheter som opplever at myndighetene bidrar til å styrke deres IT-sikkerhet. Totalt er denne andelen opp 4 % fra året før, og samlet sett er bildet relativt stabilt både for offentlige og private virksomheter.

Ser vi nærmere på virksomhetenes størrelse, viser det seg imidlertid tydelige forskjeller. De største virksomhetene, med 250 ansatte eller flere, opplever i langt mindre grad enn i fjor at myndighetene har bidratt til å styrke deres IT-sikkerhet. I årets undersøkelse svarer kun 35 % av disse virksomhetene bekreftende, mot hele 51 % i

Støtte fra myndighetene: *Opplever du at myndighetene har bidratt til å styrke virksomhetens IT-sikkerhet?*



2025. Dette kan indikere at større virksomheter i økende grad forventer mer konkrete tiltak, tydeligere reguleringer eller mer operativ støtte enn det som tilbys i dag.

Virksomheter med 20 - 249 ansatte rapporterer derimot økt grad av støtte fra myndighetene. Dette kan tyde på at informasjonstiltak, veiledere og regelverksarbeid i større grad treffer små og mellomstore virksomheter, som tradisjonelt har hatt mindre interne ressurser til å følge med på utviklingen innen IT-sikkerhet og regulatoriske krav.

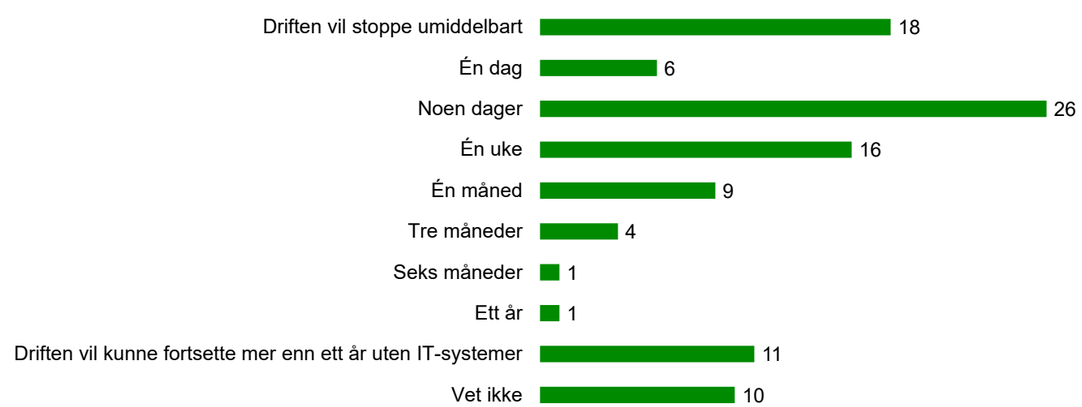
Hvem kontakter du ved et alvorlig cyberangrep?

Et positivt trekk i årets funn er at flere virksomheter oppgir at de vil kontakte offentlige instanser som Politiet, NSM og Datatilsynet ved et alvorlig cyberangrep. Dette indikerer økt bevissthet rundt rapporteringsplikt, ansvar og behovet for koordinert håndtering av alvorlige hendelser. Samtidig kan denne utviklingen også tolkes som et uttrykk for økt tillit til offentlige aktører og deres rolle i krisehåndtering. Dette er et viktig fundament for effektiv nasjonal beredskap, der informasjonsdeling og rask respons er avgjørende for å begrense skadeomfanget.

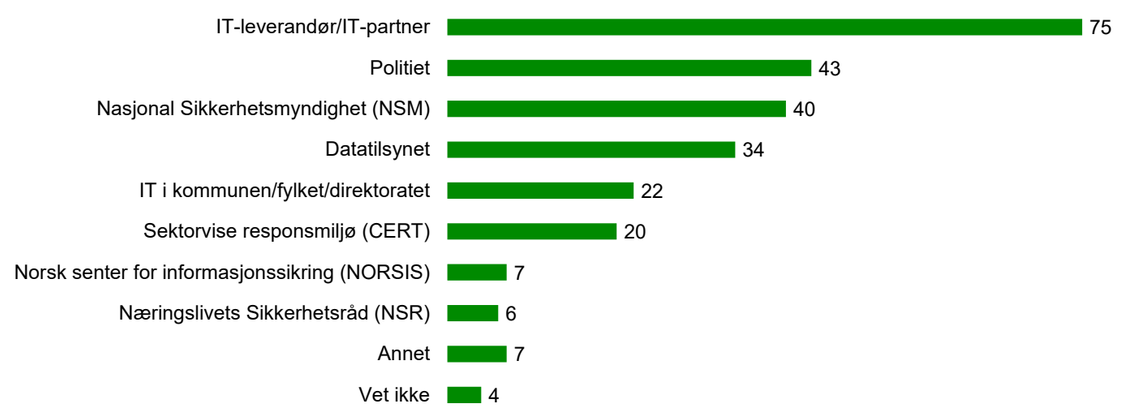
Private virksomheter lener seg på sin IT-partner

For private virksomheter er det imidlertid liten tvil om hvem de i størst grad vil lene seg på ved et alvorlig cyberangrep. Hele 87 % oppgir at de vil støtte seg på sin IT-partner i en slik situasjon. Dette understreker den sentrale rollen eksterne leverandører og samarbeidspartnere har i de private virksomheters faktiske beredskap. Funnene bekrefter at samarbeid og støtte fra eksterne leverandører ikke bare er et supplement, men ofte en forutsetning for effektiv håndtering av cyberhendelser.

Drift uten IT-systemer: *Se for deg at virksomheten blir utsatt for et cyberangrep og mister tilgang til alle IT-systemer. Hvor lenge klarer da virksomheten å holde driften i gang?*



Hvem kontaktes ved et alvorlig cyberangrep: *Dersom virksomheten skulle oppleve et alvorlig cyberangrep - hvilke av følgende aktører/instanser ville dere kontaktet for å få hjelp?*

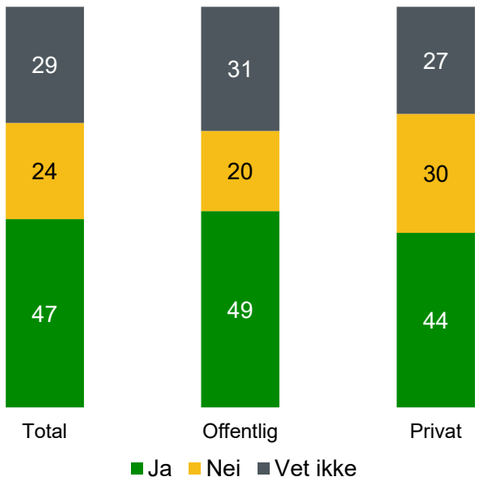


AI som ny risikofaktor

Trond Mehus
Stratetigsk løsningsrådgiver
Atea

I årets sikkerhetsundersøkelse ser vi en markant økning i bekymringen for AI som sikkerhetsrisiko. Andelen virksomheter som mener AI kan utgjøre en trussel har økt fra 34 % i 2025 til 47 % i 2026, en økning på 13 %. Denne utviklingen henger tett sammen med at flere virksomheter tar i bruk AI-tjenester, både eksterne og internt utviklede løsninger.

Kunstig intelligens som IT-sikkerhetsrisiko: *Utgjør kunstig intelligens en IT-sikkerhetsrisiko for virksomheten?*



Kunstig intelligens (AI) får stadig større gjennomslag, både gjennom økt bruk av AI-agenter og mer tilgjengelige tjenester for ansatte. IT-rapporten CIO Analytics 2025 fra Atea, viser at 45 % av IT-beslutningstakere i Nord-Europa planla å øke bruken av AI i 2025, og over halvparten av disse ønsker å videreutvikle bruken fremover. Den samme trenden gjelder både offentlig og privat sektor i Norge.

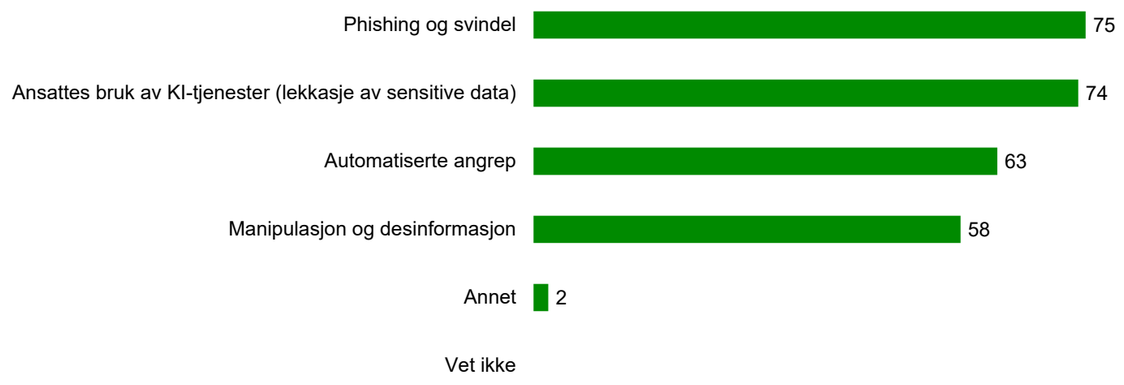
Større virksomheter (250+ ansatte) uttrykker høyest bekymring, noe som kan knyttes til strengere regulatoriske krav som NIS2, EUs AI Act, Sikkerhetsloven og forretningshemmelighetsloven.

Frykter svindel og «skygge AI»

Et betydelig funn er at 74 % frykter ansattes bruk av uautoriserte AI-tjenester. Skygge-AI og verktøy som ikke er godkjent av virksomheten kan føre til alvorlige sikkerhetsbrudd. For eksempel når ansatte uforvarende laster opp sensitiv informasjon i tredjepartsløsninger.

Phishing og svindel topper listen over bekymringer. Det skyldes at AI gjør det enklere å produsere troverdig falskt innhold, og trusselaktører får bedre grunnlag for målrettede og persontilpassede angrep. Samtidig er det fortsatt mange som ikke vet om AI utgjør en sikkerhetsrisiko. I offentlig sektor gjelder dette 31 % (ned fra 37 %), og i privat sektor 27 % (ned fra 35 %). Dette kan tyde på at risikovurderinger ikke er gjennomført eller at virksomhetene ennå ikke har tatt AI i full bruk. Blant de største virksomhetene er usikkerheten langt mindre. Kun 9 % svarer «vet ikke», noe som indikerer høyere modenhet og mer systematiske risikovurderinger.

Mest fryktede IT-sikkerhetsriskoer fra kunstig intelligens: *Hvilke IT-sikkerhetsrisikoer frykter dere mest fra kunstig intelligens?*



Kvantesikkerhet er fortsatt lavt på agendaen

Kato Kristiansen
IT-sikkerhetssjef
Atea

Et tydelig funn er at usikkerheten rundt kvanteteknologi fortsatt er stor. Over halvparten av respondentene svarer «vet ikke» på om teknologien utgjør en sikkerhetsrisiko for virksomheten. Samtidig ser vi at større virksomheter i større grad vurderer kvanteteknologi som en mulig risiko. Det kan tyde på at kunnskapen om teknologien og dens sikkerhetsimplikasjoner foreløpig er mest utviklet i større organisasjoner med mer modne sikkerhetsmiljøer.

Resultatene kan tyde på at kvantesikkerhet foreløpig ikke står høyt på agendaen i mange virksomheter, selv om temaet i økende grad diskuteres i fagmiljøer og hos sikkerhetsmyndigheter. Vi skrev i fjorårets rapport litt om gjennombruddene man har oppnådd i forskningen på kvantedatamaskiner. Fremskrittene fortsetter, og hver dag kommer vi litt nærmere den dagen hvor kvantedatamaskiner blir kraftige nok til å knekke dagens krypteringsnøkler. Dette vil kunne få store konsekvenser for sikker kommunikasjon verden over.. Dette skjæringspunktet omtales også som «Q-Day».

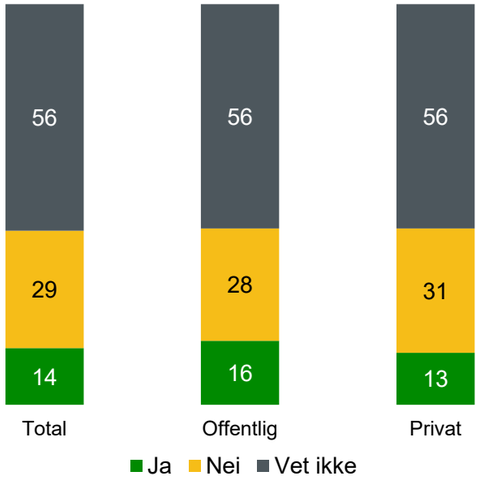
Men det er egentlig ikke avgjørende å vite nøyaktig når «Q-Day» inntreffer, fordi det er hvordan vi benytter tiden frem til det skjer som avgjør hvordan vi påvirkes og hvor store konsekvensene blir.

God planlegging og kontrollert migrering er nøkkelen her - og det kan være en prosess som går over flere år. Et lengre tidsperspektiv gjør det også mulig å oppgradere maskin- og programvare som en del av systemenes planlagte livssyklus. Det kan redusere både risiko og behovet for kostbare investeringer og utskiftninger midt i et livsløp.

Etter hvert har begrepet «harvest now, decrypt later» blitt godt kjent. Altså hvordan forskjellige aktører lytter til og lagrer kryptert datakommunikasjon. Selv om dagens kryptering gjør det nærmest umulig å dekryptere den innhentede kommunikasjonen, så lagrer man ganske enkelt disse dataene i påvente av kvantedatamaskiner som knekker krypteringen relativt raskt, og dermed gir nevnte aktører tilgang til å lese dataene i klartekst. I tilfeller der det stilles krav om at data skal være beskyttet i mange år fremover, og man fortsatt ikke har tatt i bruk nye kryptografiske standarder, vil beskyttelsen i praksis allerede være utilstrekkelig.

Nasjonale sikkerhetsmyndigheter er tydelige i sine kryptografiske anbefalinger: Virksomheter bør kartlegge hvor kryptografi brukes i egen organisasjon og arbeide for kryptografisk smidighet, slik at algoritmer kan byttes ut dersom det oppdages sårbarheter. Samtidig bør det utarbeides en plan for migrering til kvanteresistent kryptografi, og arbeidet bør starte så tidlig som mulig.

Kvanteteknologi som IT-sikkerhetsrisiko: *Utgjør kvanteteknologi en IT-sikkerhetsrisiko for virksomheten?*



Norske virksomheter fortsatt i startfasen av NIS2-arbeidet

Jarle Nordby Johnsen
Sikkerhetsrådgiver
Atea

Tallene fra undersøkelsen viser minimale endringer fra 2025, og virksomhetene rapporterer fortsatt at det er begrenset hvor påvirket de blir av NIS2. Dette kan tyde på at mange fortsatt ikke opplever direktivet som noe akutt. Til tross for at det er forventet å bli implementert i norsk lovverk i løpet av 2026-2027. Det er også fortsatt en overraskende stor andel (53 %) som svarer at de ikke er kjent med direktivet, eller ikke vet om de blir påvirket.

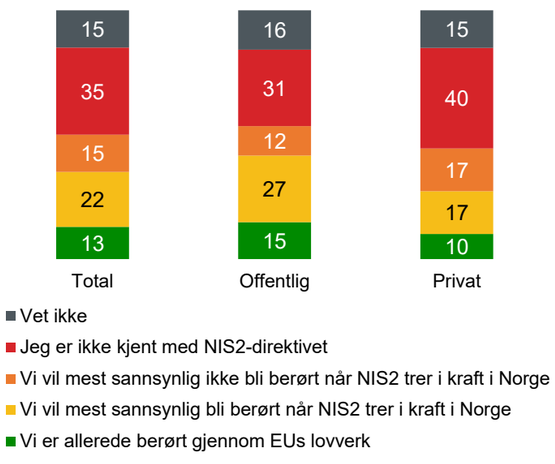
En mulig forklaring på dette kan være at Norge ikke implementerte NIS1-kravene før i oktober 2025, gjennom den nye Digitalsikkerhetsloven. Ettersom NIS1 ble innført i EU i 2016, kan dette ha bidratt til at mange virksomheter oppfatter at de fortsatt «har god tid» og ikke har tatt stilling til dette enda. Om vi ser på omfanget av kravene i NIS2, og hvem som blir omfattet, kunne man kanskje forvente at norske myndigheter hadde vært tydeligere. Slik at virksomhetene får tid til å etablere nødvendige tiltak.

Flere i offentlig sektor jobber med å innfri kravene

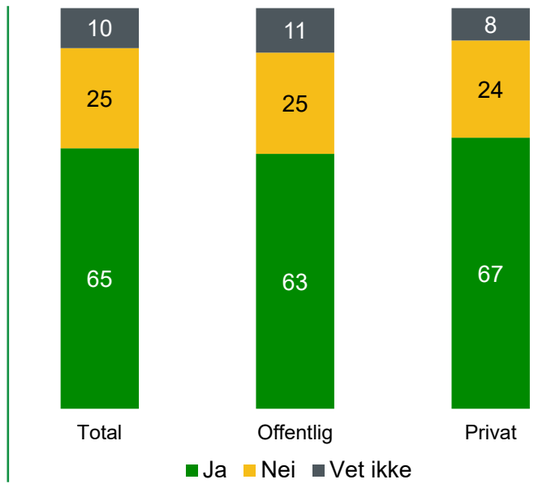
Av virksomhetene som er, eller vil bli berørt av lovverket, ser vi en viss positiv utvikling fra 2025 til 2026 når det gjelder arbeid med å innfri kravene. Offentlig sektor øker arbeidet sitt fra 51% til 63 %, og er nå på nivå med privat sektor. Dette kan tyde på at offentlig sektor har fått større klarhet i hvilke krav som kommer, og har startet med et systematisk arbeid for å nærme seg disse.

Selv om flere virksomheter i offentlig sektor arbeider med å oppfylle kravene, er økningen samlet sett på tvers av sektorer overraskende liten. Det kan tyde på at mange virksomheter fortsatt befinner seg tidlig i gjennomføringsfasen.

Hvordan NIS2-direktivet påvirker virksomheten: *Hvordan påvirker NIS2-direktivet virksomheten?*



Innfri kravene i NIS2: *Jobber virksomheten målrettet med å innfri kravene i NIS2?*

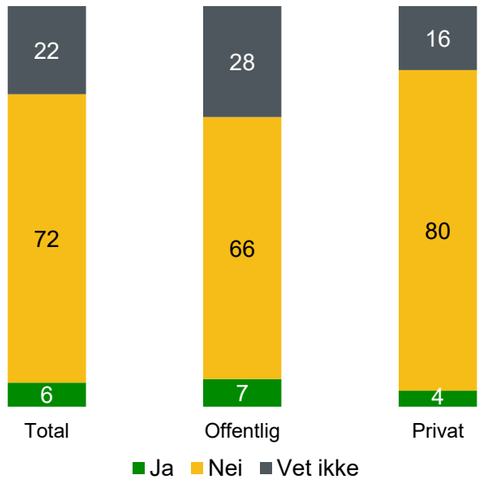


Flere av kravene i NIS2 er organisatoriske og krever både ressurser, kompetanse og tid for å innføre. En sentral utfordring er at kravene i større grad retter seg mot virksomhetens ledelse, og ikke bare mot IT-avdelingen. Tiltakene kan derfor ikke løses raskt eller isolert gjennom innkjøp av nytt utstyr eller enkle tekniske oppgraderinger. Dette kan være en av forklaringene på at fremdriften i arbeidet ikke øker så raskt som man kanskje kunne forventet.

Få får NIS2-krav fra kunder

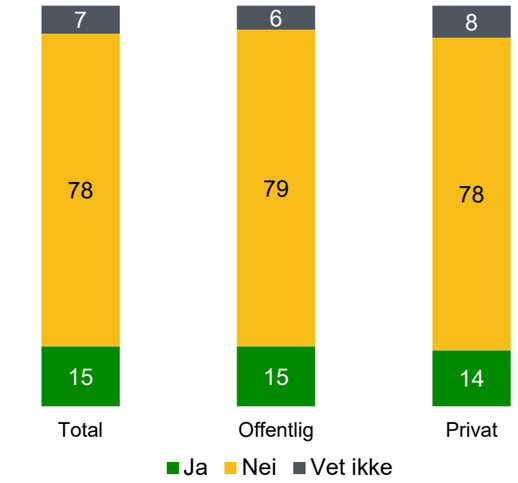
Det er fortsatt få virksomheter som har fått krav fra kunder om NIS2-samsvar, og tallene viser kun en svak økning siden 2025. Dette tyder på at det norske markedet foreløpig ikke opplever den samme kundedrevne effekten av NIS2 som man ser i andre EU-land. Dette er delvis naturlig, ettersom regelverket allerede er innført i EU, og kunder der forventer at leverandører etterlever kravene for å sikre eget samsvar.

Krav fra kunder som en konsekvens av NIS2-direktivet: *Har virksomheten mottatt noen krav fra kunder som en konsekvens av NIS2-direktivet?*



I det norske markedet arbeider mange virksomheter fortsatt med å oppfylle kravene i NIS1 og digitalsikkerhetsloven. Selv om dette regelverket stiller visse krav til kontroll over underleverandører, er kravene mer eksplisitte i NIS2. Det er derfor rimelig å forvente at kundekrav knyttet til det nye regelverket vil utvikle seg gradvis, etter hvert som virksomhetene får bedre kjennskap til regelverket og større selskaper avklarer egne krav til leverandørkjeden.

Krav fra kunder som en konsekvens av NIS2-direktivet: *Har virksomheten mottatt noen krav fra kunder som en konsekvens av NIS2-direktivet?*



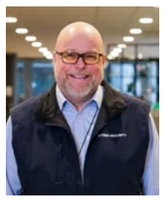
Grafen viser svar fra virksomheter som tidligere har oppgitt at de enten allerede er berørt av NIS2 eller vet at de vil bli det. Det gjør funnene interessante ettersom dette er aktører vi kanskje forventer ligger lengre fremme, og som tidligere ville kjent et press fra egne kunder.

Tallene viser en svak økning over hele linjen, men er fortsatt lave. Offentlige virksomheter skiller seg ut da de øker fra 1 % til 15 %, og vi ser også en økning i industri og varehandel. Dette viser at virksomheter med klar NIS2-eksponering nå i større grad opplever krav oppover i verdikjeden, men kun i visse bransjer.

Det lave nivået totalt sett kan tyde på at kundekravene fortsatt i liten grad har begynt å gjøre seg gjeldende. Selv blant virksomheter som er eller blir berørt av regelverket. En mulig forklaring er at mange aktører, også i EU, fortsatt befinner seg i en tidlig fase av implementeringen og har hovedfokus på tiltak som må gjennomføres internt i egen virksomhet. Arbeidet med å stille systematiske krav videre i leverandørkjeden kan derfor komme senere.

En annen utfordring kan være manglende oversikt over hvilke krav som faktisk bør stilles. I mange virksomheter ligger ansvaret for sikkerhet og leverandøroppfølging i ulike deler av organisasjonen, for eksempel innen leverandørstyring eller økonomi. Det kan gjøre det mer krevende å etablere tydelige og konsistente sikkerhetskrav i leverandørkjeden.

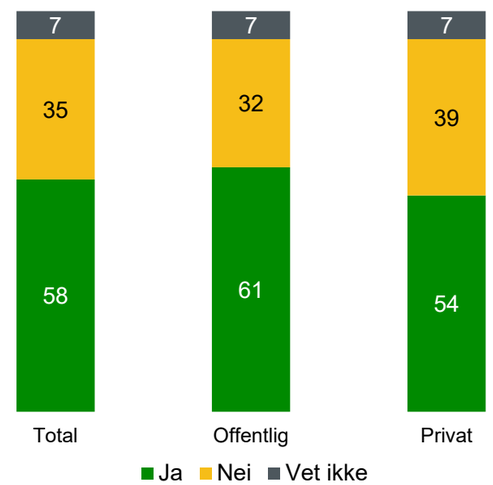
Nedgang i kjennskapen til NSMs grunnprinsipper



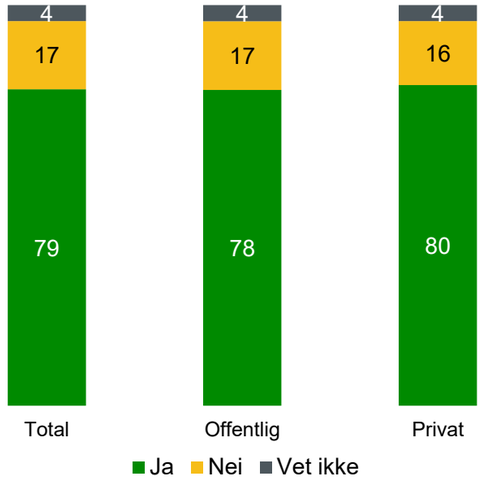
Thomas Tømmernes
Konserndirektør for IT-sikkerhet
Atea

Nasjonal sikkerhetsmyndighet (NSM) har de siste tiårene bygd tillit og relasjoner med sikkerhetsmiljøer i hele landet, inkludert oss i Atea. De har vært den naturlige koblingsboksen mellom myndigheter og næringsliv. Med ett ben i det regulatoriske, og ett ben i det operative. NSMs grunnprinsipper lansert i august 2017 og senere oppdatert, har fungert som en rettesnor for både virksomheter og oss som jobber kommersielt med å levere sikre tjenester og løsninger i det norske markedet. Det er bare å ta av seg hatten for et strålende stykke arbeid som virkelig har vært med på å styrke Norges digitale motstandskraft mot trusselbilde.

Kjennskap til NSM sine grunnprinsipper for IKT-sikkerhet: *Kjenner du til Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper forIKT-sikkerhet?*



Implementering av NSM sine grunnprinsipper for IKT-sikkerhet: *Har dere implementert Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet i deres drift?*



Færre kjenner til grunnprinsippene

For første gang siden Atea startet arbeidet med sikkerhetsrapporten ser vi en nedgang i andelen virksomheter som oppgir at de kjenner til NSMs grunnprinsipper for IKT-sikkerhet. Det gir grunn til bekymring. Vi kan ikke slå fast årsakene, men utviklingen reiser flere spørsmål. Har omfordeling av oppgaver og ansvar skapt mindre tydelig eierskap til rammeverket? Når roller og ansvar endres i det nasjonale sikkerhetsarbeidet, kan det også påvirke hvor godt slike anbefalinger når ut til virksomhetene.

Samtidig har antallet rammeverk, standarder og anbefalinger de siste årene innen digital sikkerhet økt betydelig. Mange virksomheter må forholde seg til flere styringsmodeller og krav samtidig, både fra myndigheter, leverandører og egne styringssystemer. I et slikt landskap kan oppmerksomheten rundt grunnprinsippene bli mindre enn tidligere.

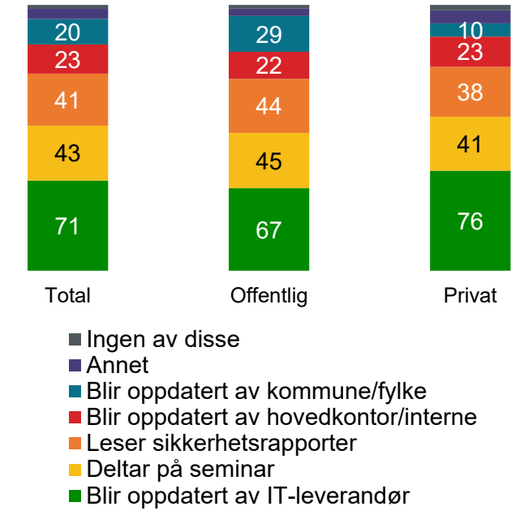
Samtidig ser vi en økning i andelen private virksomheter som oppgir at de har implementert grunnprinsippene i driften, fra 68 til 80 prosent.

Det er verdt å merke seg at dette spørsmålet kun er besvart av virksomheter som kjenner til grunnprinsippene. Likevel peker utviklingen på at prinsippene oppleves som nyttige og relevante i praktisk sikkerhetsarbeid. For mange aktører i privat sektor fungerer de som et viktig utgangspunkt for arbeidet med digital sikkerhet, og de løftes ofte fram i seminarer og faglige møteplasser der sikkerhetsarbeid diskuteres.

IT-leverandør er en viktig kunnskapskilde

Det er derfor svært gledelig å se at mange av virksomhetene i undersøkelsen viser til IT-leverandører, sikkerhetsrapporter og fagseminarer som viktige kilder til ny kunnskap og oppdatert kompetanse innen IT-sikkerhet.
IT-sikkerhet utvikles i et samspill mellom myndigheter, næringsliv og fagmiljøer. IT-leverandører spiller en særlig viktig rolle i dette økosystemet, noe også resultatene peker på. De sitter tett på teknologien, følger utviklingen i trusselbildet og jobber daglig med å implementere sikkerhetsløsninger i praksis hos virksomheter over hele landet. Dermed blir de også en viktig kanal for å spre kunnskap, erfaringer og beste praksis.

Oppdatert på IT-sikkerhet: *Hva gjør du for å bli oppdatert på IT-sikkerhet?*

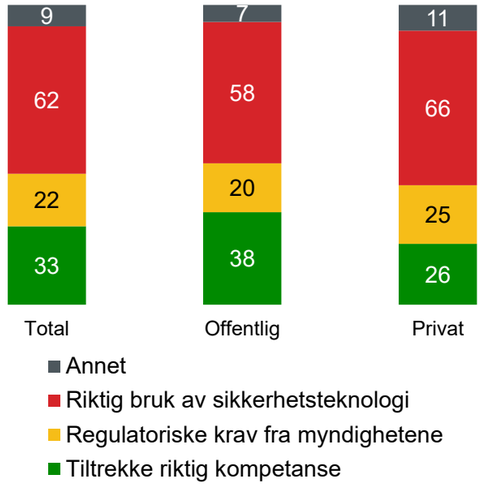


For oss som arbeider med dette hver dag, er det motiverende å se at slike møteplasser og kunnskapskilder fortsatt har høy verdi. Det gir energi til å fortsette arbeidet med å bidra til økt kompetanse, bedre samarbeid og et mer robust digitalt Norge.

AI endrer spillereglene for IT-sikkerhet

Årets rapport viser at man fortsatt har et høyt fokus på riktig bruk av sikkerhetsteknologi. Med økende adopsjon av AI-teknologi er dette kanskje viktigere enn noen gang.

Viktigste områder innenfor IT-sikkerhet det kommende året: *Hvilke områder innenfor IT-sikkerhet er viktigst for dere det kommende året?*



AI-drevne angrep vokser i hastighet og raffinement som gjør at mennesker ikke henger med, og man må ta i bruk AI som forsvar i større grad. Bruk av AI på sikkerhetssiden gir en proaktivitet som kan forutse, forstyrre og blokkere cybertrusler før de gjør skade. Samtidig som det er et paradoks at AI både er trussel og løsning.

Teknologileverandørene lanserer sine AI-drevne sikkerhetsløsninger i høyt tempo. Gartner mener at sikkerhetsprodukter basert på deteksjon og respons alene ikke vil være tilstrekkelig, og at de sikkerhetsløsningene som mangler forebyggende evner vil miste relevans. Videre anslår de at forebyggende sikkerhetsløsninger vil utgjøre halvparten av sikkerhetsbudsjettene innen 2030. *(Kilde: Gartner, September 2025)*

Når sikkerhetsprodusentene nå tilbyr nye kapabiliteter og funksjoner med sine AI-drevne løsninger, krever det at kundene har kompetanse til å vurdere hva som er de rette løsningene for dem. Mange har konkludert med at tiden er inne for ytterligere tjenesteutsetting på sikkerhetssiden. Det er nok derfor ikke tilfeldig at markedet for «security-as-a-service» vinner terreng og vokser raskere enn de tradisjonelle sikkerhetssegmentene. En annen faktor som sannsynligvis spiller inn, er innføringen av regulative krav som NIS2, hvor tjenesteutsetting gjør veien til å bli «compliant» enklere og raskere for mange.

Når AI-bølgene flommer over både brukere og infrastruktur, er det avgjørende at man har en helhetlig sikkerhetsstrategi, som er omsatt i gode rammeverk for «governance» og «policies». Tilnærminger hvor man forsøker å etablere rammeverk etter at systemer har gått i produksjon, er i beste fall en tålmodighetsprøve, for ikke å nevne økt risiko for nedetid og tapt omsetning.

Kato Kristiansen
IT-sikkerhetssjef
Atea

Atea er Norges største IT-selskap

Med rundt 1 800 ansatte fordelt på 23 kontorer rundt om i hele Norge står vi i Atea klare for å bistå virksomheten din. Våre rådgivere har solid teknologiforståelse og høy kompetanse, og vi støtter alt av teknologi.

Vil du vite mer?

Ta kontakt med:

sikkerhet@atea.no

www.atea.no/it-sikkerhet/

ATEA