

BEVISSTHET OG BEREDSKAP

Atea sikkerhetsrapport 2025



ATEA

DEL LO TH N N

- 
- 04** Om undersøkelsen
 - 06** Vi har ikke tid til å vente
 - 08** Viktigste funn
 - 09** Sikkerhetsbudsjettene står på stedet hvil
 - 11** Flertallet mangler IT-sikkerhetsressurser
 - 13** Tiltak og ansvar
 - 14** Beredskapsplan
 - 18** Er din bedrift et lett bytte for cyberangrep?
 - 22** AI og IT-sikkerhet: Nye muligheter, større risiko

- 25** Kvanteteknologi - “Harvest now, decrypt later”
 - 26** NIS2-direktivet
 - 29** Avslutning
- 

OM UNDERSØKELSEN

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

Intervjumetode:	Web og telefon
Utvalgskilde:	Næringslivsbasen
Intervjulengde:	7 minutter
Feltperiode:	17.01.25 - 08.02.25
Antall intervju:	516
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:	352
Daglig leder:	164
Offentlig sektor:	237
Privat sektor:	279
20-49 ansatte:	236
50-99 ansatte:	95
100-249 ansatte:	74
250 ansatte eller flere:	111

Feilmargin uttrykker påliteligheten av et tall. Kantar har på denne målingen intervjuet 516 bedrifter med over 20 ansatte. Utvalgsstørrelsen for denne gruppen er på 15 358. Feilmarginen i dette tilfellet er +/- 4 prosentpoeng med et konfidensintervall på 95 %.



VI HAR IKKE TID TIL Å VENTE

Thomas Tømmernes

Konserndirektør for IT-sikkerhet
Atea

Dette er tredje året vi kartlegger IT-sikkerheten i norske virksomheter. Vi har spurt daglige ledere og IT-ansvarlige over hele landet hvordan de vurderer egen beredskap, kompetanse og investeringsevne i møte med et stadig mer krevende trusselbilde.

Alle rapporter fra både myndighetsorganer, privat sektor og analyseselskaper peker på at trusselbildet er mer skremmende enn noen gang tidligere.

Kunstig intelligens, usikre verdikjeder og underleverandører, uro i verden og nye krav fra EU, som NIS2, og den kommende sikkerhetsloven, gjør at presset på IT-sikkerheten øker. Likevel sier nesten halvparten at de fortsatt bruker under fem prosent av IT-budsjettet på sikkerhet. Det er for lite. Det har vært mange hendelser i media de siste årene, der fellesnevneren for disse er at de fleste hendelsene kunne vært unngått med enkle og kostnadseffektive løsninger.

Men denne rapporten handler om mer enn tall og trender. Den er et verktøy for deg som har ansvar for virksomhetens digitale sikkerhet, og som vet at det



ikke finnes én enkel løsning – men at det finnes mange smarte, nødvendige og gjennomførbare tiltak som kan gjøre en forskjell.

Sikkerhet handler om å forstå virksomhetens motstandsdyktighet sett opp mot dagens trusselbilde. Start med å kartlegge hvor virksomheten står i dag. Bruk resultatene til å definere hvilken risiko virksomheten er villig til å akseptere, og bli enige i ledelsen om hvordan dere skal jobbe målrettet mot dette.

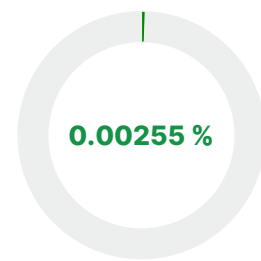
Du har kanskje sett emneknaggen #SammenSikrerViNorge. Den er ikke eid av noen – og derfor eid av oss alle. Den handler om felles ansvar, om å erkjenne at IT-sikkerhet er et samfunnsproblem og noe vi må prioritere, dele erfaringer om, og øve på. Sammen.

Så – bruk rapporten. Del den. Snakk om den. Still spørsmål i styret. Prioriter tiltakene. Og viktigst: Sørg for at sikkerhet er en naturlig og integrert del

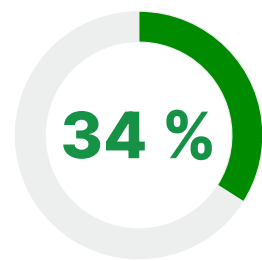
av virksomhetens daglige drift og utvikling. For det å ha god sikkerhet er ikke en utgift, men et konkurransefortrinn.

Trusselbildet venter ikke. Og det bør ikke vi heller.

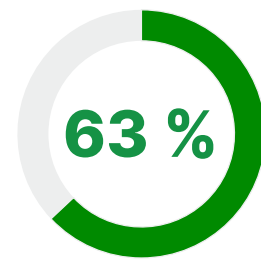
VIKTIGSTE FUNN



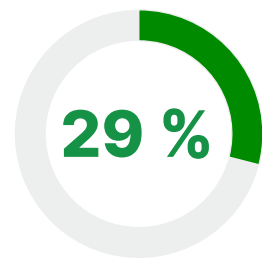
Majoriteten av virksomhetene setter av mindre enn 0.0025 % av sitt totale budsjett til IT-sikkerhet



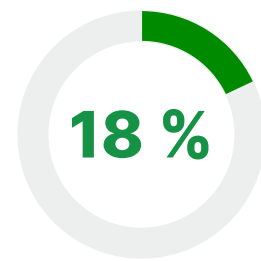
34 % mener kunstig intelligens utgjør en IT-sikkerhetsrisiko for virksomheten



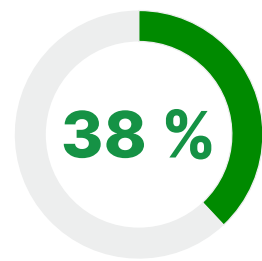
63 % oppgir at riktig bruk av sikkerhetsteknologi er det viktigste området innenfor IT-sikkerhet det kommende året



29 % vurderer risikoen som svært liten eller liten, for at virksomheten skal bli utsatt for et cyberangrep



For 18 % av virksomhetene vil en hendelse som fører til at man mister tilgang til IT-systemene sine, føre til umiddelbar driftstans



38 % av virksomhetene er ikke kjent med NIS2-direktivet

Som i tidligere undersøkelser, bruker de små virksomhetene langt mindre ressurser og fokus på IT-sikkerhet, enn de større virksomhetene:

- 18 % av de minste virksomhetene har egne ansatte hvor hoveddelen av arbeidsoppgavene omhandler IT-sikkerhet, mot 55 % for de største virksomhetene
- 61 % av de største virksomhetene skal øke investeringene i IT-sikkerheten de neste 12 månedene, mot kun 26 % av de minste virksomhetene.
- 19 % av de minste virksomhetene har gjort compliance-arbeid mot NIS2, ISO eller NSMs Grunnprinsipper eller lignende for å ivareta egen IT-sikkerhet, mot 68 % for de største virksomhetene
- 23 % av de minste virksomhetene anser kunstig intelligens som en IT-sikkerhetsrisiko, mot 61 % for de største virksomhetene
- 53 % av de minste virksomhetene kjenner ikke til NIS2-direktivet, mot kun 7 % av de største virksomhetene

Offentlige og private virksomheter

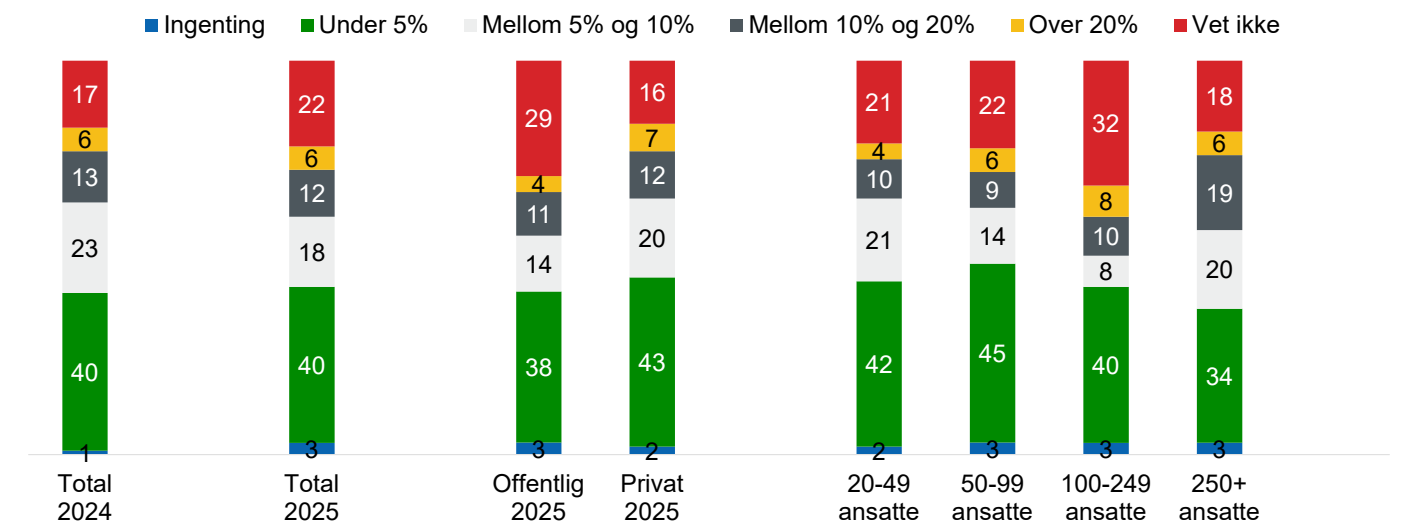
- Blant offentlige virksomheter oppgir kun 9 % at de har cyberforsikring, mens hele 37 % oppgir at de ikke vet. For private virksomheter oppgir 27 % at de har cyberforsikring, mens kun 18 % ikke vet
- 32 % av offentlige virksomheter er ikke kjent med NIS2-direktivet, mot 43 % av private virksomheter
- 35 % av offentlige virksomheter har egne ansatte hvor hoveddelen av arbeidsoppgavene omhandler IT-sikkerhet, mot 21 % av private virksomheter

SIKKERHETS- BUDSJETTENE STÅR PÅ STEDET HVIL

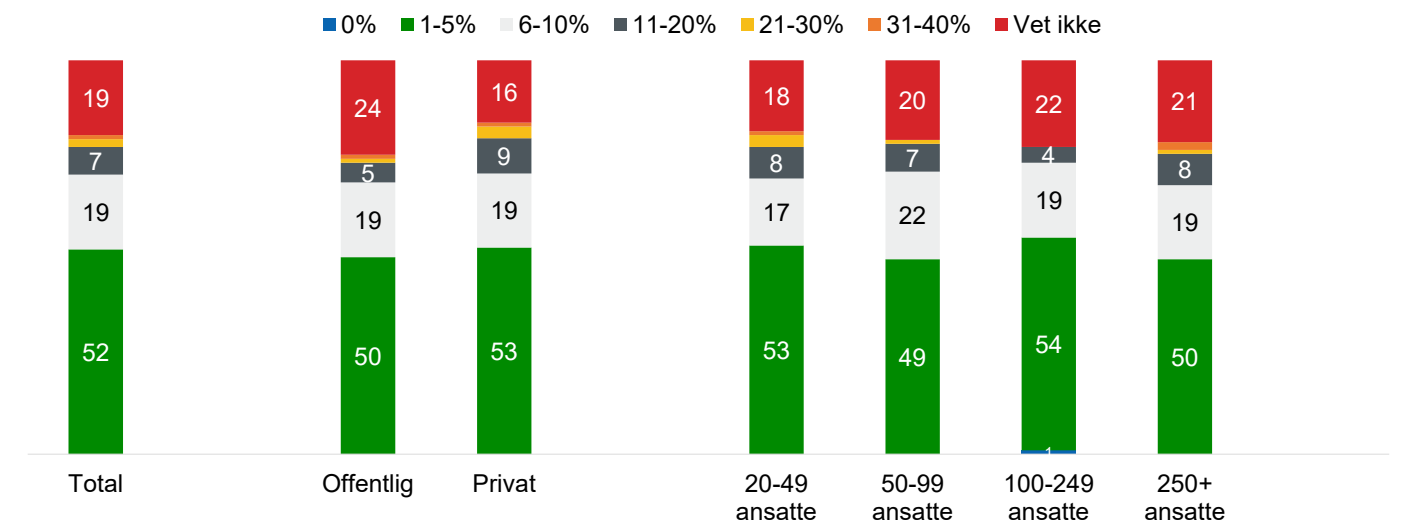
De økonomiske forutsetningene sier noe om norske virksomheters evne til å investere i sikkerhetstiltak. Det er i utgangspunktet et parameter som vil variere fra virksomhet til virksomhet. Vi har derfor spurt om hvor stor prosentandel av IT-budsjettet som går til IT-sikkerhet. 40 % av respondentene sier at mindre enn 5 % av IT-budsjettet går til IT-sikkerhet, som er på

samme nivå som i fjor. Det er heller ikke noen store forskjeller mellom privat og offentlig sektor på dette spørsmålet, men vi kan se at privat sektor totalt sett har en større investeringsvilje enn offentlig sektor.

Når vi legger til grunn at ca. halvparten av virksomhetene investerer mindre enn 5 % av budsjettet sitt på IT, er det



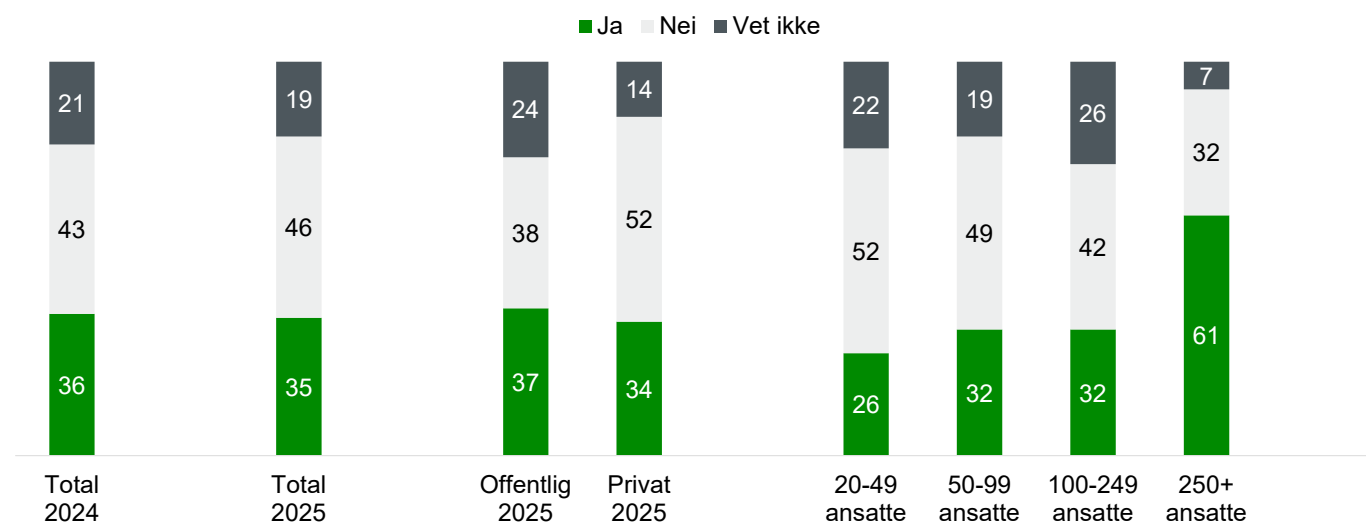
Budsjett IT-sikkerhet: Omtrent hvor stor del av virksomhetens IT-budsjett går til IT-sikkerhet?



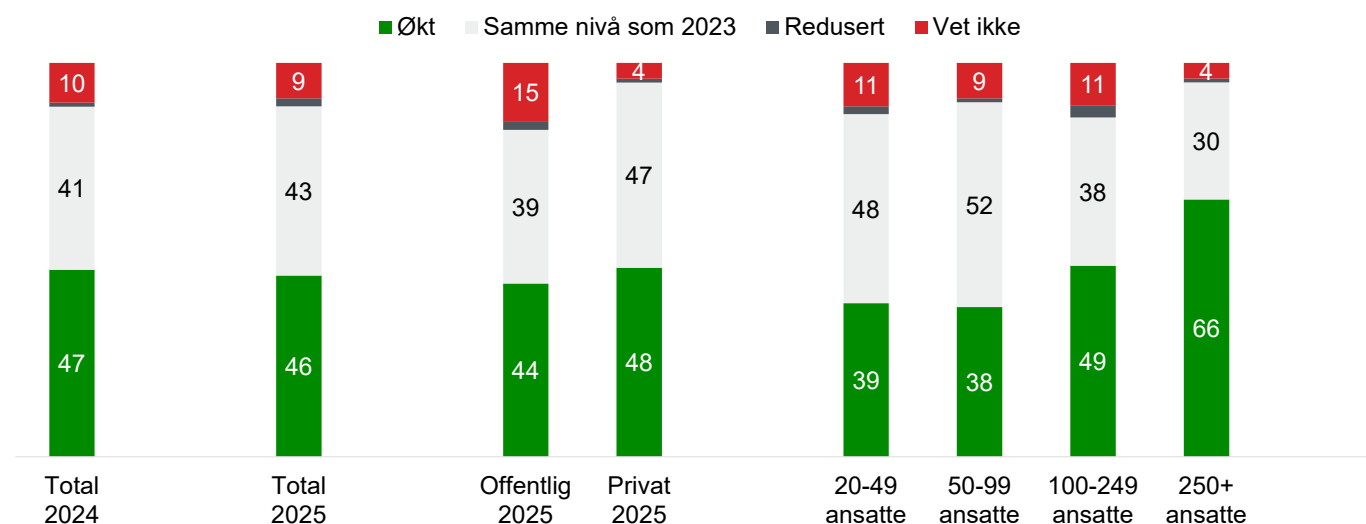
Budsjett IT: Omtrent hvor stor del av virksomhetens budsjett går til IT?

en ganske lav andel av det totale budsjettet som går til IT-sikkerhet. Faktisk, kan vi ut fra dataene argumentere for at majoriteten av virksomhetene setter av mindre enn 0,0025 % av sitt totale budsjett til IT-sikkerhet. Tallene viser at det ikke har skjedd store endringer fra i fjor, noe vi mener er med på å sette begrensninger for norske virksomheters evne til å ruste seg mot et økende trusselbilde.

Resultatene viser at nærmere halvparten av virksomhetene mener å ha økt investeringene på IT-sikkerhet i 2024. Dette er på samme nivå sammenlignet med året før. 1 av 3 virksomheter forventer å øke budsjettene på IT-sikkerhet ytterligere de neste 12 mnd. Det er de største virksomhetene som sier at de vil øke investeringene mest i IT-sikkerhet det neste året.



Investeringer i IT-sikkerhet de neste 12 månedene: Skal virksomheten øke investeringene innen IT-sikkerheten de neste 12 månedene, sammenlignet med de forrige 12 månedene?

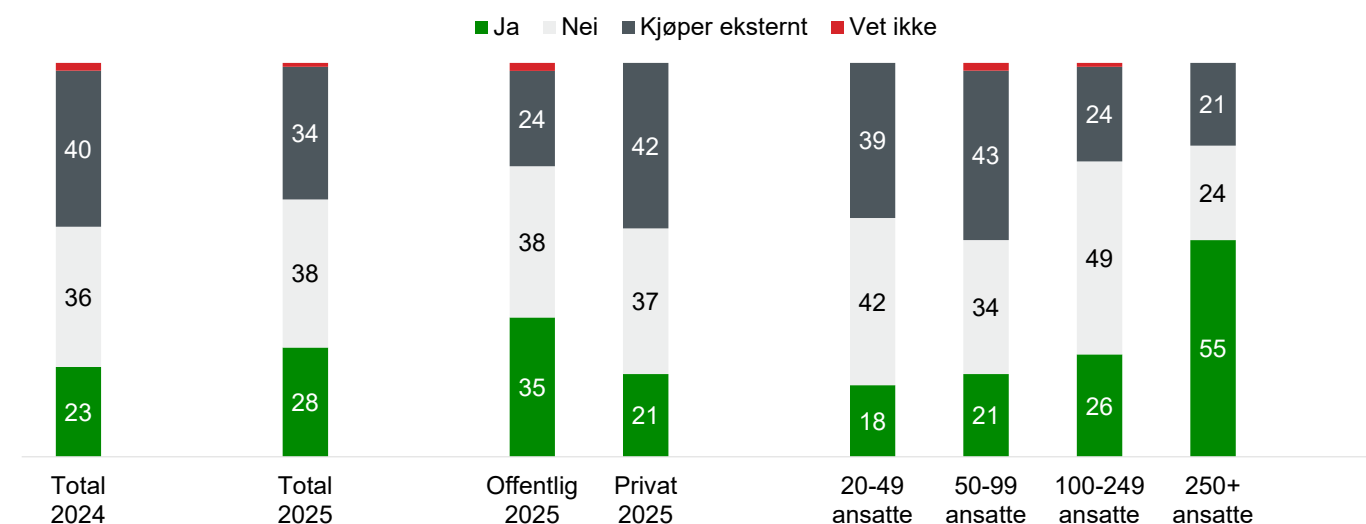


Investeringer i IT-sikkerhet i 2024 sammenlignet med 2023: Ble virksomhetens investeringer innen IT-sikkerhet økt eller redusert i 2024, sammenlignet med 2023?

FLERTALLET MANGLER IT-SIKKERHETS-RESSURSER

Årets undersøkelse viser at kun 28 % av de spurte virksomhetene har ansatte hvor hoveddelen av arbeidsoppgavene er IT-sikkerhet. Dette er en liten økning fra fjorårets rapport.

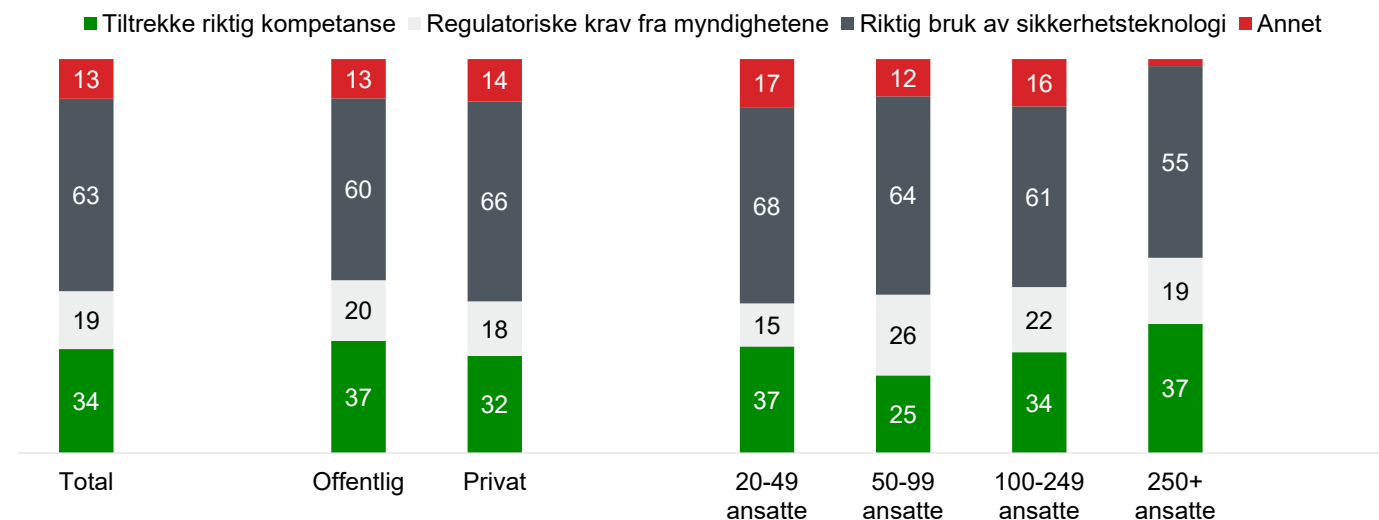
34 % av virksomhetene oppgir at de kjøper IT-sikkerhetskompetanse eksternt. Det er flere i det private næringslivet (42 %) som kjøper kompetanse eksternt enn virksomheter i offentlig sektor (24 %). Offentlige ansetter i større grad egne folk med ansvar for IT-sikkerhet enn det private virksomheter gjør. Likevel er det fortsatt 38 % av de spurte virksomhetene som ikke har egne ansatte hvor hoveddelen av arbeidsoppgavene omhandler IT-sikkerhet.



Egne ansatte som jobber med IT-sikkerhet i virksomheten: Har virksomheten egne ansatte hvor hoveddelen av arbeidsoppgavene omhandler IT-sikkerhet?

Det kan være flere grunner til at mange virksomheter ikke har egne ansatte dedikert til IT-sikkerhet. En viktig faktor er kostnadene forbundet med å ansette spesialister på området. For mindre virksomheter, og kanskje spesielt for private virksomheter med mer fleksible budsjetter, kan det være mer kostnadseffektivt å kjøpe inn denne kompetansen fra

noen eksterne og kun ved behov. På den annen side, kan en årsak til at det offentlige ansetter egne eksperter selv, være at de ofte har strengere reguleringer og krav til IT-sikkerhet (som for eksempel Sikkerhetsloven, Helseregisterloven, osv.), noe som kan gjøre det mer hensiktsmessig å ansette egne spesialister.

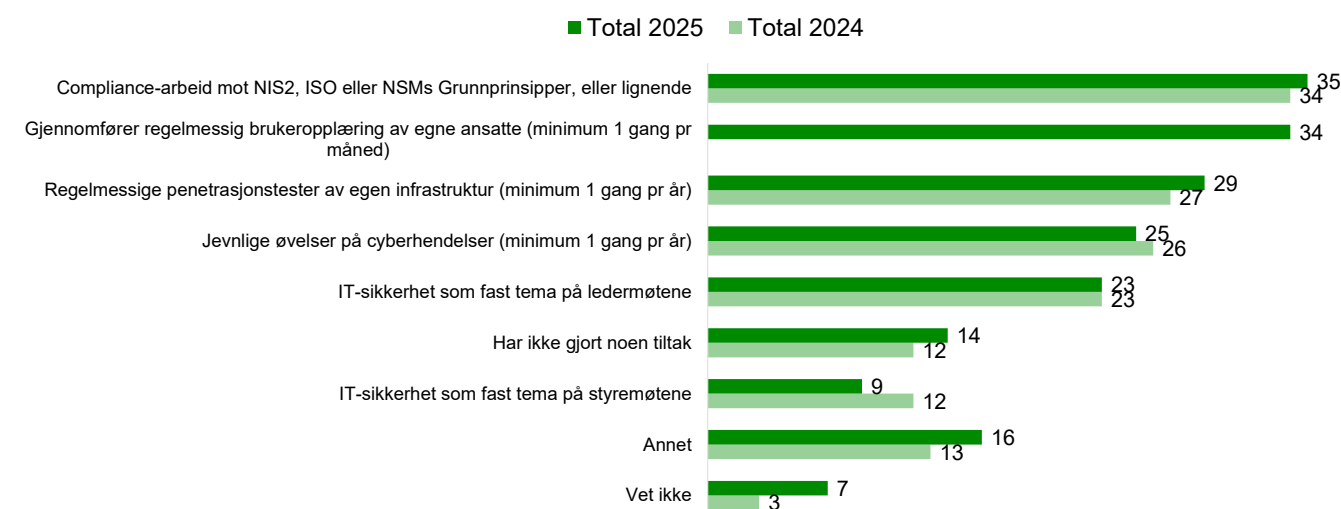


Viktigste områder innenfor IT-sikkerhet det kommende året: Hvilke områder innenfor IT-sikkerhet er viktigst for dere det kommende året?

I årets undersøkelse spurte vi også hvilke områder innenfor IT-sikkerhet som er viktigst for respondentene det kommende året. 34 % oppgir «tiltrekke riktig kompetanse», mens 19 % mener «regulatoriske krav», og hele 63 % oppgir «riktig sikkerhetsteknologi».

Vi står i en kompetansekrise. Mange virksomheter har manglende bevissthet rundt helt grunnleggende IT-sikkerhetstiltak. Kompetanse er avgjørende for å senke risiko og håndtere mulige sikkerhetsbrudd. Har din virksomhet kapasitet og kompetanse på IT-sikkerhet?

TILTAK OG ANSVAR



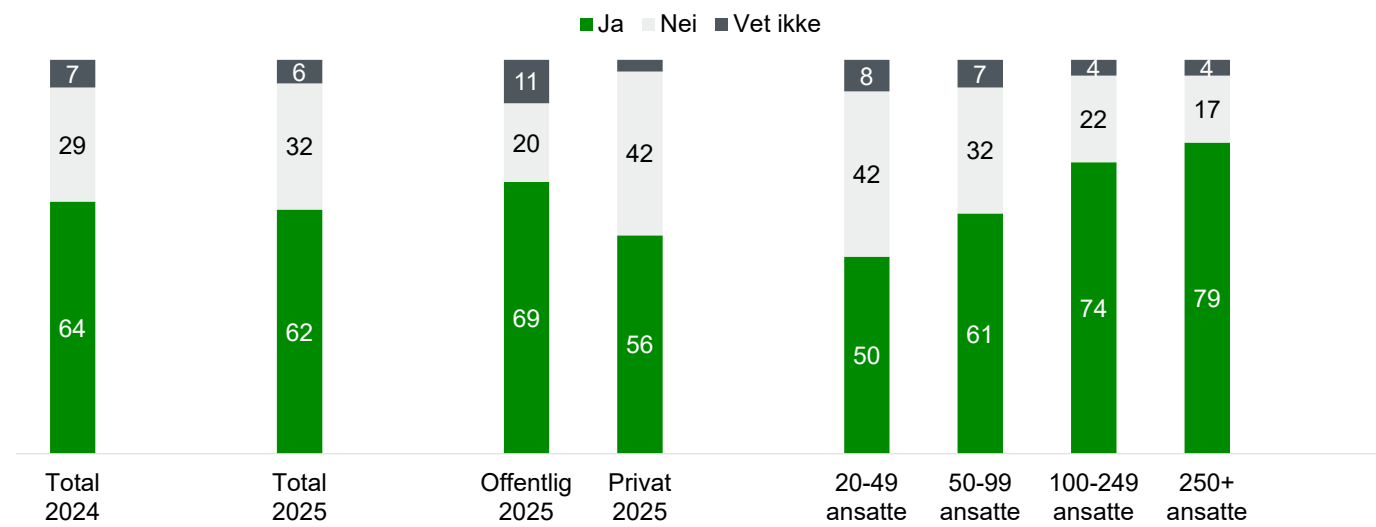
Tiltak for å ivareta egen IT-sikkerhet: Hvilke tiltak har virksomheten gjort for å ivareta egen IT-sikkerhet?

Det kan være mange tiltak virksomheter gjør for å ivareta egen IT-sikkerhet. Vi har spurt norske virksomheter om de har gjennomført tiltak som vi mener er blant de viktigste. Det er «Compliance-arbeidet» med NIS2-kravene som nevnes oftest, tett fulgt av regelmessig brukeropplæring av egne ansatte. Det er urovekkende

mange som svarer at de ikke gjør noen av disse tiltakene. Det er grunn til å tro at flere virksomheter legger dette ansvaret over på en tredjepart, og dermed har outsourcet ansvaret sitt. Vi mener dette er spesielt urovekkende, og viser kanskje en manglende forståelse for eget ansvar når det kommer til sikkerhet.



BEREDSKAPSPLAN



Beredskapsplan: Har virksomheten en beredskapsplan dersom dere skulle bli utsatt for en IT-sikkerhetshendelse?

På spørsmål om virksomheten har en beredskapsplan dersom man skulle bli utsatt for en IT-sikkerhetshendelse, ser vi at svarene er relativt like som i fjor. 62 % oppgir at de har en beredskapsplan, 32 % har ikke beredskapsplan og 6 % vet ikke.

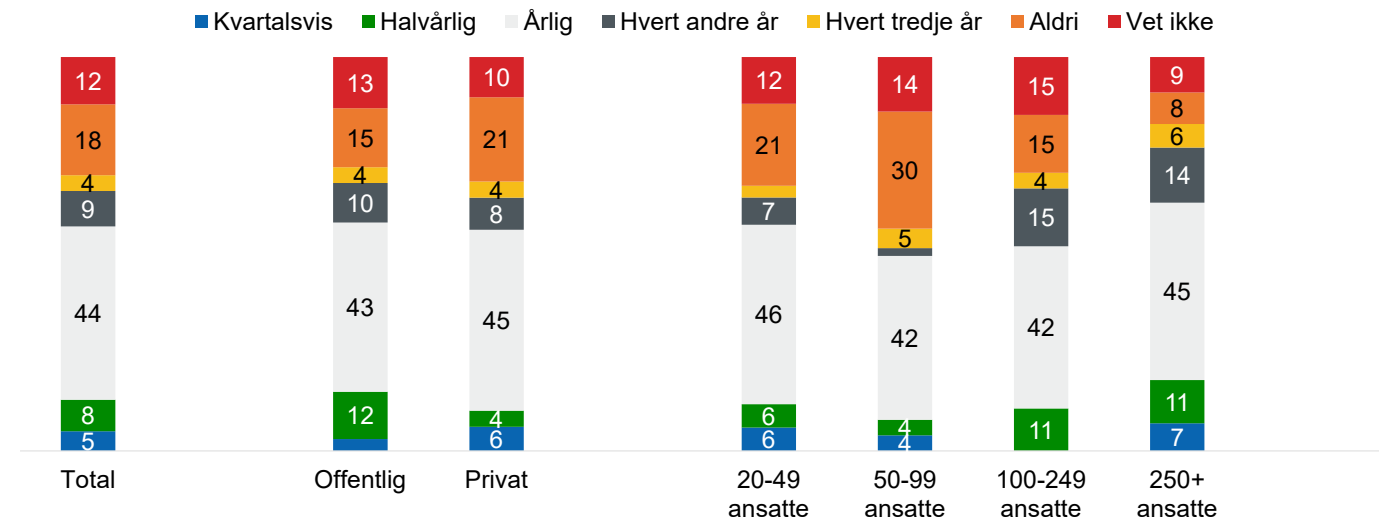
Erfaringene til hendelseshåndtererne i Atea Incident Response Team (Atea IRT) er at virksomheter i Norge har beredskapsplaner i mange forskjellige former og med ulikt detaljnivå. Det viktigste med en beredskapsplan er at den er forankret og forstått i organisasjonen, og at den blir testet og øvd på.

Det finnes også eksempler på at beredskapsplaner ikke blir brukt under skarpe hendelser. Planene finnes på papir, men er ikke oppdaterte og lever ikke som en del av virksomhetens beredskapsevne. Dette kan skyldes at planen ble laget av en tidligere IT-sjef eller direktør, og at den nå bare eksisterer som et dokument uten reell verdi.

Oppsummert: Det er viktig at organisasjonen leser, forstår og er kjent med innholdet i beredskapsplanen for at den skal være nyttig.

Vi kjenner til virksomheter som har stått i en hendelse hvor de har hatt svært detaljerte og omfattende beredskapsplaner, men hvor organisasjonen ikke er kjent med dem. Dette kan føre til kaos siden menneskene i organisasjonen ikke er kjent med eller forstår sine roller og rollebeskrivelsene i praksis er utydelige. Det er bedre å ha en enkel og godt forstått plan enn en kompleks plan som ingen kjenner til.

57 % av virksomhetene som oppgir at de har en beredskapsplan sier at de øver på beredskapsplanen årlig eller oftere. Årlige treninger forutsetter at øvelsen er god og konstruktiv, og at funn og forbedringspunkter gjøres noe med. Det er viktig å være påskrudd og ha en ambisjon om å bli god på bruk av beredskapsplanen. Hvis man ikke trener oftere enn årlig, kan det være vanskelig å forbedre planverket.



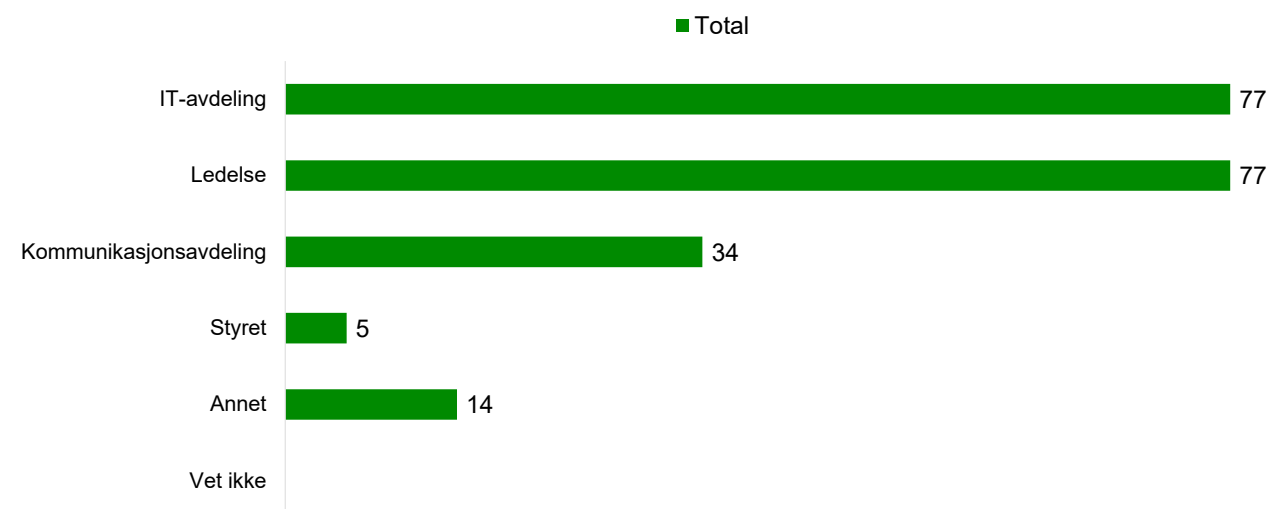
Øving på beredskapsplan: Hvor ofte vil du si at det øves på beredskapsplanen?

FEM SIKKERHETSRÅD

- 1 Forstå trusselbildet:** IT-sikkerhet handler ikke bare om teknologi, men også om mennesker og prosesser. Hold deg oppdatert på aktuelle trusler og hvordan de kan påvirke din virksomhet.
- 2 Styrk grunnsikkerheten:** Sikre at virksomheten har grunnleggende sikkerhetstiltak på plass, som flerfaktoraутентisering (MFA), jevnlig oppdateringer og sikkerhetskopiering av data.
- 3 Bygg en sikkerhetskultur:** De fleste sikkerhetsbrudd skyldes menneskelige feil. Tren ansatte regelmessig i sikkerhetsbevissthet og sørg for at de vet hvordan de skal håndtere mistenkelige henvendelser.
- 4 Ha en beredskapsplan:** Når et angrep skjer, teller hvert sekund. Sørg for at virksomheten har en tydelig plan for hvordan hendelser skal håndteres, inkludert varsling, isolering og gjenoppretting.
- 5 Still krav til leverandører:** IT-sikkerhet stopper ikke ved egen dør. Sørg for at alle leverandører og samarbeidspartnere følger strenge sikkerhetskrav, slik at verdikjeden din ikke blir en sårbarhet.

Øvelser

Det er viktig at planverket lever og utvikles, også når nye ansatte kommer inn i virksomheten og folk slutter. Beredskapsgruppen bør gjennomføre øvelser for å sikre at folk er i stand til å utføre sine roller.



Organisatoriske lagdeler på øvelsen: Hvilke organisatoriske lagdeler er med på øvelsen?

I årets undersøkelse oppgir flesteparten av virksomhetene (77 %) at ledelse og IT-avdeling er med på øvelsen(e). 34 % oppgir at kommunikasjonsavdelingen deltar og kun 5 % oppgir styret.

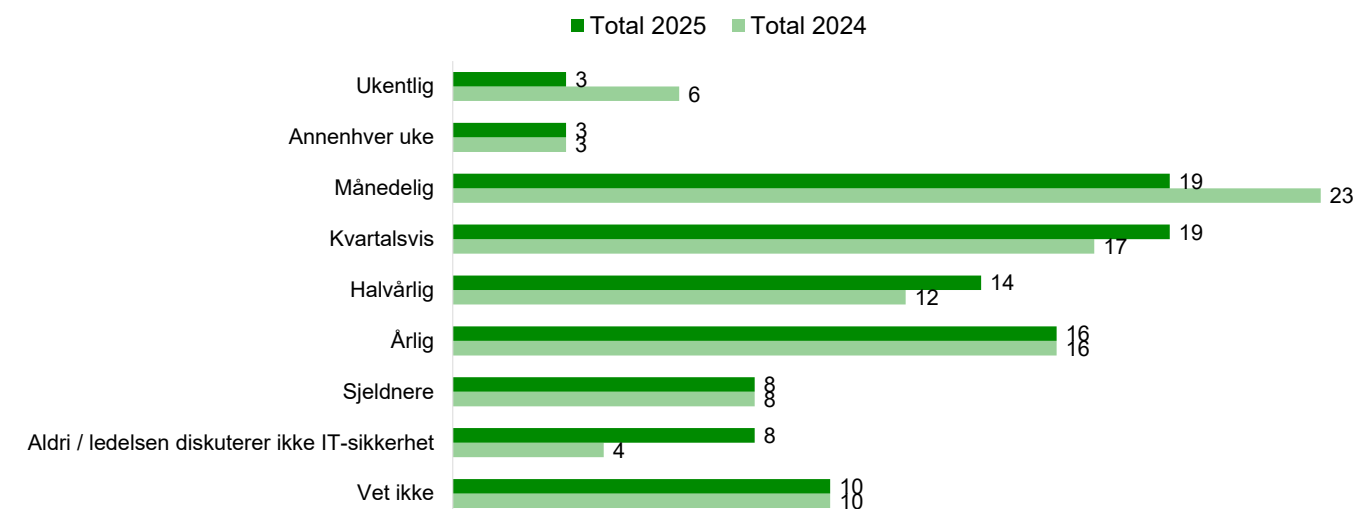
Våre erfaringer tilsier at ledelsen og beredskapsledelsen er viktige deltakere, da deres involvering er avgjørende for å sikre effektiv kommunikasjon og koordinering under øvelsen. Kommunikasjonsavdelingen spiller en åpenbar rolle i både intern og ekstern kommunikasjon, selv om det kan variere avhengig av organisasjonens struktur. I noen tilfeller kan dedikert personell eller kommunikasjonsdirektøren være ansvarlig for ekstern kommunikasjon.

IT-avdelingen er en viktig deltaker i øvelsen, da de ofte har en bedre forståelse av digitale angrep og deres konsekvenser. Derfor er det viktig at IT-avdelingen terper på detaljene og praktiske aspekter ved å håndtere slike angrep. Øvelsen gir IT-avdelingen muligheten til å forbedre sin forståelse og ferdigheter, samtidig som de samarbeider med andre, inkludert tredjeparter, for å sikre en helhetlig tilnærming til krisehåndtering.

19 % av norske virksomheter oppgir at de diskuterer IT-sikkerheten internt månedlig eller kvartalsvis i ledelsen.

Det er viktig at disse diskusjonene skjer regelmessig for å sikre at ledelsen har et godt innblikk i risikomatriksen og tar høyde for risikoen i sitt arbeid. Selv om det ikke er avgjørende om diskusjonene skjer ukentlig, månedlig eller kvartalsvis, er det viktig at arbeidet understøtter forståelsen av digitale trusler og risikoer som virksomheten står overfor.

“Beredskapsøvelser og diskusjoner rundt IT-sikkerhet kan bidra til en bedre forståelse og dermed hyppigere diskusjoner om emnet.”



Diskusjon om IT-sikkerhet i ledelsen: Hvor ofte diskuterer ledelsen IT-sikkerheten til virksomheten?



ER DIN BEDRIFT ET LETT BYTTE FOR CYBERANGREP?

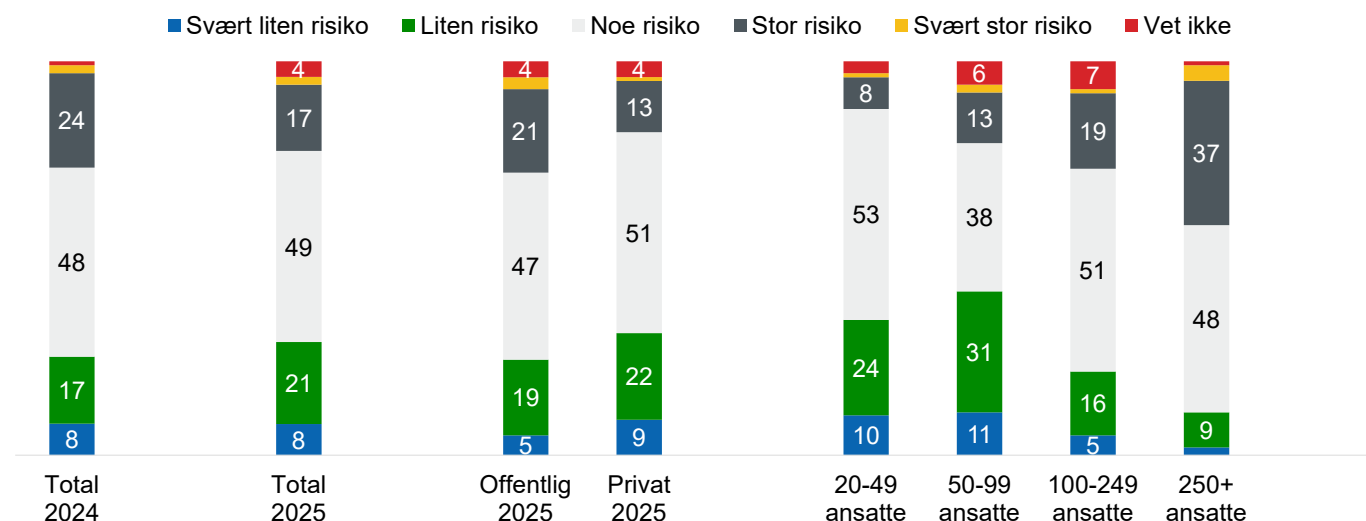
Vi kan dele opp de fleste angrep mot norske bedrifter i to kategorier:

- Målrettede:** Her har angriperen på forhånd sett seg ut hvem de skal angripe og gjør gjerne undersøkelser rundt firmaet. De har ofte et mål som er større enn bare økonomisk vinning, selv om det også kan være målet.
- Opportunistiske:** Her angripes målet stort sett kun fordi det er mulig og enkelt. Du er rett og slett den lavest hengende frukten.

bedrift, som ofte ikke har dedikert IT-sikkerhetsfolk, å ha kontroll på eget trusselbilde.

Det er vanskelig å anslå hvor stor sjanse det er for at man skal bli utsatt for et cyberangrep, men man bør alltid planlegge som om man kommer til å bli utsatt for det. De opportunistiske angrepene kan treffe hvem som helst.

God IT-sikkerhet krever at man har systemer som løser problemer for deg. Det kan være de tradisjonelle



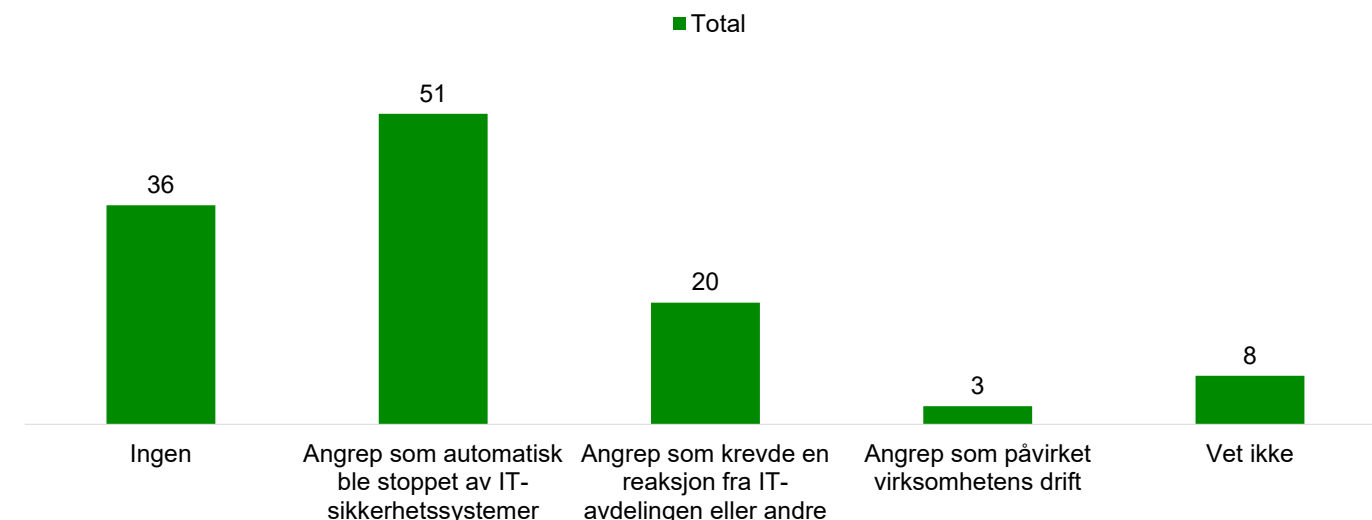
Risiko for cyberangrep: Hvordan vurderer du risikoen for at virksomheten skal bli utsatt for et cyberangrep?

Det er kanskje enkelt å tenke at hvis man er en liten virksomhet, så vil ikke angriperne bry seg med å angripe en. Og tenker man bare på målrettede angrep, så er nok det sant. Vår erfaring er likevel at de fleste cyberangrep er opportunistiske. Det gjør at små virksomheter ofte er like utsatt for angrep som de store, men uten de samme ressursene for sikkerhetsarbeid som de store.

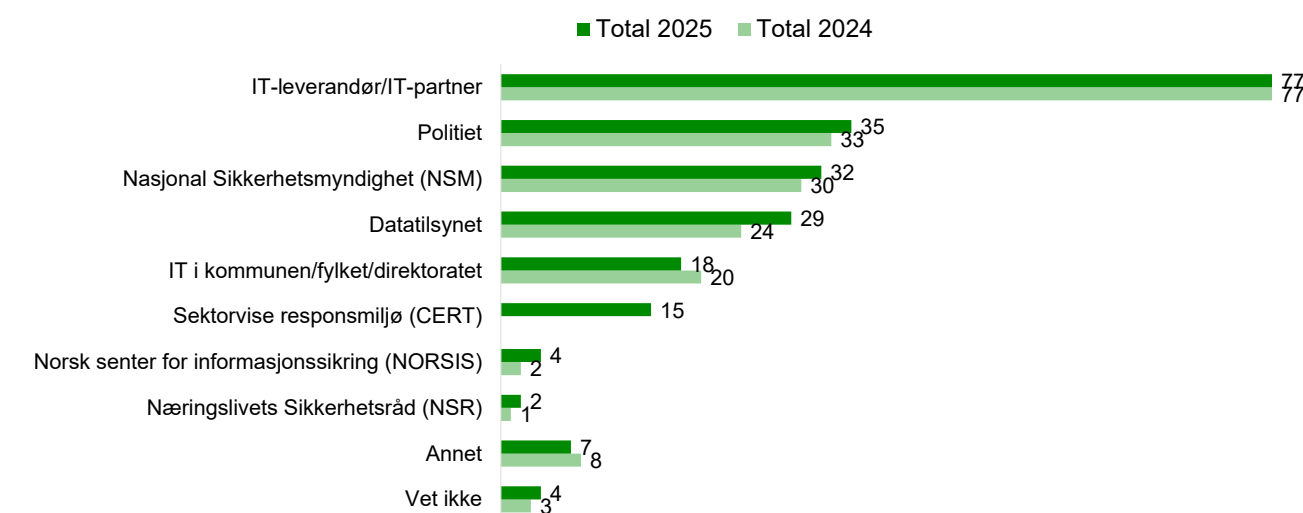
Når små bedrifter anser risikoen for å bli utsatt for dataangrep som generelt lavere enn større, tror vi det handler om at man stort sett tenker på de målrettede angrepene. I tillegg kan det være vanskelig for en mindre

endepunktssikringene våre, brannmurer som blokkerer inntrengere eller mer avanserte maskinlæringstjenester som blokkerer kontoen vår om vi plutselig endrer bruksmønsteret vårt.

Vi tror at de fleste bedrifter opplever at systemene våre beskytter oss. Av og til kanskje så godt at vi ikke engang merker det. Når bare 20 % av bedrifter har opplevd angrep som fører til aksjon fra IT-avdelingen, skyldes nok det at de automatiske systemene etter hvert fungerer veldig godt, og gjør mye av jobben for oss. At 3 % svarer at de har opplevd hendelser som faktisk



Cyberangrep opplevd i 2024: Hvilke typer cyberangrep har virksomheten opplevd i 2024?



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

påvirker driften stemmer godt med våre erfaringer. Tallet er forholdsvis lavt, men denne typen hendelser er ofte store, så konsekvensene dersom det skjer blir også store.

Når noen har brutt seg inn hos deg vil alle ringe politiet først. Med IT-innbrudd er det helt tydelig at det er vanskeligere å vite hvor man skal henvende seg. Det er i alle fall helt tydelig at IT-leverandører som Atea har et stort ansvar når denne typen hendelser skjer. Dette er et ansvar vi kjenner på, og som gjør at vi som selskap tar sikkerhet på alvor, og har et spesialtrent team klare til å rykke ut for å hjelpe til med håndtering av cyberangrep – Atea Incident Response Team.

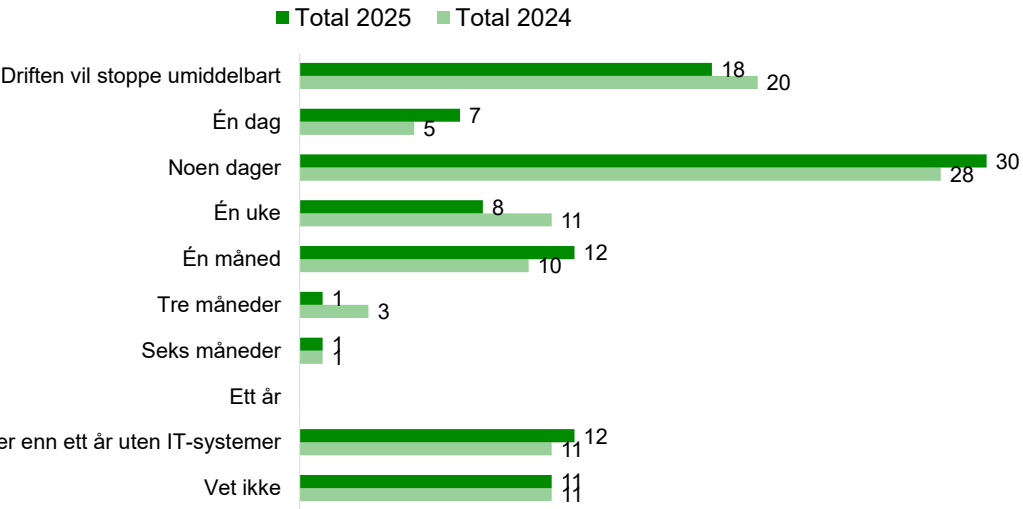
At vi etter hvert i Norge har fått på plass flere gode sektorvise responsmiljøer (CERTer) er gledelig. Dette er

miljøer som kan være til uvurderlig hjelp for bedriftene og organisasjonene som sogner til dem. Likevel vil de fleste bedrifter i Norge ikke ha en CERT å snu seg til. Vi er igjen avhengige av at de private IT-leverandørene tar ansvar både når det gjelder preventiv og reaktiv sikkerhet.

At IT etter hvert er integrert i alle prosesser vi bruker på jobb, og uansett om du er en butikk, en fabrikk eller et sykehjem så er du avhengig av IT. For 18 % av bedriftene vil en hendelse som fører til at man mister tilgang til IT-systemene sine føre til umiddelbar driftsstans. Når Ateas Incident Response Team rykker ut og bistår i store hendelser, for eksempel løsepengevirus, ser vi ofte at den store kostnaden ved hendelsen ikke er konsulenter eller ny hardware. Det er tapte inntekter fordi man ikke får gjort jobben sin og levert produktene sine.

ATEA INCIDENT RESPONSE TEAM

Atea Incident Response Team (IRT) består av høyt sertifiserte og erfarne sikkerhetskonsulenter med bred faglig kompetanse. IRT inngår i Nasjonal Sikkerhetsmyndighets godkjennelsesordning for hendelseshåndtering. Vi er en av fire godkjente virksomheter i Norge. Mistenker du at din virksomhet er utsatt for et dataangrep? Ring 03060 og be om IRT.



Drift uten IT-systemer: Se for deg at virksomheten opplever et IT-sikkerhetsbrudd som gjør at dere mister tilgang til alle IT-systemer. Hvor lenge klarer da virksomheten å holde driften i gang?

I de fleste tilfeller klarer man å lage manuelle løsninger som gjør at enkelte oppgaver kan bli løst, men mesteparten av oppgavene er helt avhengig av IT-systemene. Varer nedetiden mer enn noen dager sier over halvparten av bedriftene i undersøkelsen

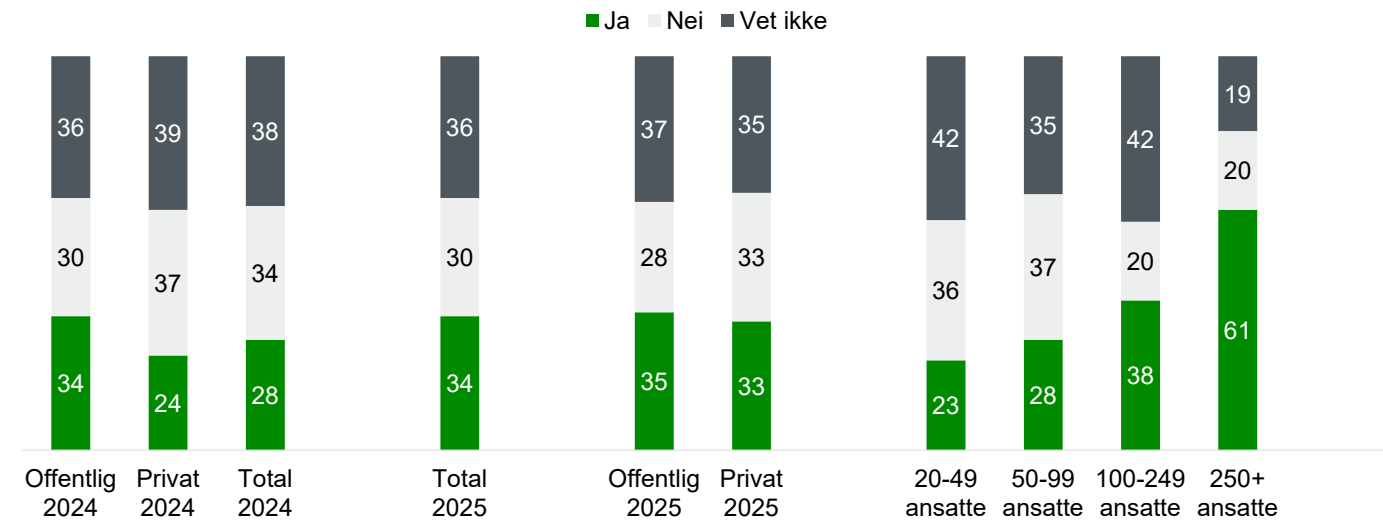
vår at de ikke klarer å holde virksomheten i gang. Ved løsepengevirus tar gjenoppbyggingsjobben ofte uker. Da er det viktig å ha beredskapsplaner slik at man vet hva man skal gjøre, for å sørge for at man raskest mulig er tilbake i drift igjen.



AI OG IT-SIKKERHET: NYE MULIGHETER, STØRRE RISIKO

Kunstig intelligens (AI) har raskt blitt en sentral teknologi i norske bedrifter. Samtidig reiser utviklingen betydelige spørsmål og bekymringer knyttet til IT-sikkerhet. Basert på funnene i denne undersøkelsen blant norske bedrifter, kan vi identifisere flere viktige innsikter:

- **Automatiserte angrep:** AI-teknologi effektiviserer cyberangrep, noe som fører til økt risiko for alvorlige sikkerhetsbrudd.
- **Misbruk av AI blant ansatte:** Uforsiktig bruk av AI-verktøy av ansatte kan føre til utilsiktet lekkasje av sensitiv informasjon.



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

De største bekymringene

- **Phishing og svindel:** AI øker risikoen ved at phishing-angrep blir mer sofistikerte og troverdige. Dette kompliserer identifiseringen av falske e-poster og lenker.
- **Lekkasje av sensitive data:** Risikoen for at sensitiv informasjon kommer på avveie øker gjennom hacking eller feil bruk av AI-verktøy, spesielt åpne AI-tjenester.
- **Manipulasjon og desinformasjon:** AI kan brukes til å påvirke offentligheten negativt, med fare for svekket tillit til institusjoner.
- **Sosial manipulering:** AI kan effektivisere og skalere sosial manipulering gjennom mer troverdige angrep som spear phishing.

Virksomheters syn på AI som sikkerhetsrisiko

- En betydelig andel (34 %) av virksomhetene anser AI som en reell IT-sikkerhetsrisiko, mens en nesten like stor andel andel (36 %) fortsatt er usikre.
- Spesielt bedrifter med høyere omsetning (over 750 mill.) er mer bevisste på risikoen (64 % mener AI er en sikkerhetsrisiko).
- Både det offentlige (35 %) og private aktører (33 %) viser økende bekymring og relativt lik forståelse av AI-risiko.
- Privat sektor har økt fra 24 % i 2024 til 33 % i 2025.

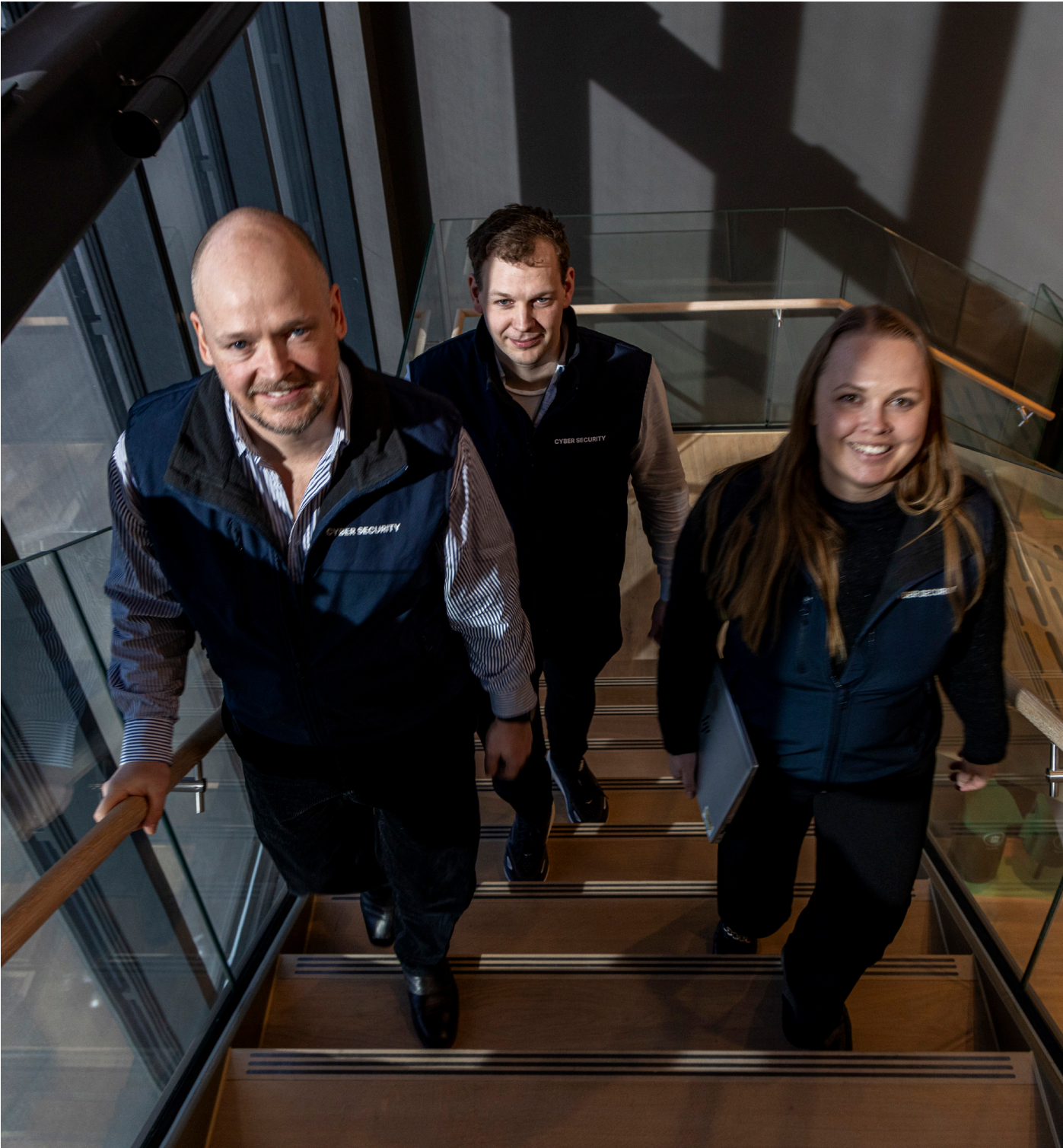
Hva betyr dette for norske bedrifter?

Den økende anerkjennelsen av AI som en alvorlig sikkerhetsrisiko viser at bedriftene må ta proaktive tiltak for å sikre seg mot nye former for cybertrusler. Dette inkluderer å:

- Investere i kontinuerlig opplæring og bevisstgjøring av ansatte om risikoer knyttet til AI. Opplæring kan bidra til at ansatte bruker AI-verktøy trygt, reduserer risikoen for lekkasje av sensitive data, og bidrar samtidig til bedre utnyttelse av AI-teknologi – en klar vinn-vinn-situasjon.

- Ha en tydelig AI-policy – hva er lov å bruke og hvordan skal det brukes?
- Utvikle sikkerhetsstrategier og løsninger som er tilpasset truslene fra AI-drevet cyberkriminalitet.

Den teknologiske utviklingen av AI tilbyr store muligheter, men introduserer også avanserte sikkerhetsutfordringer. For å møte denne dobbeltrollen er det avgjørende at virksomhetene erkjenner alvorret og aktivt utvikler sikkerhetskompetanse og forebyggende strategier. Fremtidens sikkerhet bør være dynamisk, med AI som både overvåkes og brukes effektivt for å styrke selskapenes forsvar.



8 EKSEMPLER PÅ KRIMINELLES BRUK AV AI

Vi har samlet en oversikt over eksempler på hvordan kriminelle bruker kunstig intelligens (AI):

- 1 Sofistikerte phishing-angrep:** Kriminelle bruker AI til å generere svært overbevisende falske e-poster og nettsider som etterligner legitime organisasjoner. Dette øker sannsynligheten for at mottakere blir lurt til å gi fra seg sensitiv informasjon.
- 2 Utvikling av skadevare:** Med AI kan angripere automatisere utviklingen av skadevare som er i stand til å tilpasse seg ulike miljøer, unngå deteksjon og utnytte sårbarheter mer effektivt.
- 3 Deepfake-teknologi:** AI brukes til å lage falske videoer og lydopptak som er nesten umulige å skille fra ekte. Dette kan brukes i direktørsvindel, der angripere utgir seg for å være en leder for å lure ansatte til å overføre penger eller gi tilgang til sensitiv informasjon.
- 4 Automatisert sosial manipulering:** Gjennom analyse av store datamengder kan AI identifisere individuelle mål og skreddersy angrep basert på personens atferd og preferanser, noe som øker sjansene for suksess.
- 5 Forgjøelse av sikkerhetssystemer:** Kriminelle kan bruke AI til å teste og identifisere svakheter i eksisterende sikkerhetssystemer, og deretter utvikle metoder for å omgå disse.
- 6 Generering av ulovlig innhold:** AI brukes til å produsere falske bilder, videoer eller lydopptak, kjent som deepfakes, som kan brukes til utpressing eller desinformasjon.
- 7 Automatisering av kriminelle prosesser:** Gjennom AI kan kriminelle effektivisere og skalere sine operasjoner, for eksempel ved å automatisere phishing-angrep eller utvikle avansert skadevare.
- 8 Forbedring av eksisterende metoder:** AI bidrar til å gjøre tradisjonelle angrep mer sofistikerte og vanskeligere å oppdage, som ved å forbedre sosial manipulering eller skjule ondskapen programvare.

KVANTETEKNOLOGI - “HARVEST NOW, DECRPYT LATER”

Selv om man har forsket på og forsøkt å utvikle fungerende kvantedatamaskiner i flere tiår, så er det først de siste årene at utviklingen virkelig har satt fart. Den teknologiske utviklingen gjør at forskerne nå bryter barrierer som tidligere har fremstått nærmest umulige å overkomme. For eksempel har Microsoft Research nylig annonsert at de har nådd en ny milepæl med «Harvest now, decrypt later» Majorana 1. Inntil nylig har det vært vanlig å omtale tidsperspektivet for når man tror verden har kvantedatamaskiner som vil utgjøre en fundamental forskjell som “flere tiår”. Microsoft sier nå at de ikke lenger teller tiår, men år.

En av de mest omtalte sikkerhetsutfordringene som kommer med introduksjonen av kvantedatamaskiner gjelder kryptografi. Dagens mest populære kryptografiske algoritmer har holdt stand i flere tiår og har vært avgjørende for å beskytte digital kommunikasjon og samhandling verden over. Flere av de asymmetriske algoritmene (RSA, ECC) som anses som bærebjelker i dagens digitale samfunn er ansett som sårbare i en verden med kvantedatamaskiner. Der hvor dagens superdatamaskiner ville bruke millioner av år på å knekke disse algoritmene, beskriver «Shor’s algorithm» en mulighet for at en kvantedatamaskin bare trenger minutter eller timer på samme oppgave.

For å møte disse utfordringene har NIST (National

Institute of Standards and Technology) invitert til et program som har som mål å utvikle nye algoritmer som ikke like enkelt lar seg knekke av en kvantedatamaskin. Det handler om «Post-Quantum-Cryptography» (PQC) og det ble i fjor sommer kåret vinnere blant bidragene, dvs. man har valgt ut de algoritmene som fremstår mest motstandsdyktig (Post-Quantum Cryptography | CSRC).

Det vil naturligvis ta årevis før den enkelte teknologiprodusent har integrert støtte for disse algoritmene i sine produkter, men uavhengig av dette er tiden allerede nå moden for at den enkelte organisasjon starter det viktige arbeidet for å være best mulig forberedt, ved:

- Å starte en kartlegging av hvordan man benytter krypto i egen organisasjon vil man kunne utarbeide en prioritert migreringsplan (eksempelvis det enkelte systems kritikalitet og/eller sensitivitet på data).
- Å etablere et prinsipp om at alt fremtidig innkjøp av hardware og software må ha støtte for PQC.
- At alle applikasjoner bør etterleve å være krypto-agile (med det menes at applikasjoner ikke må omskrives for å støtte nye kryptografiske algoritmer).

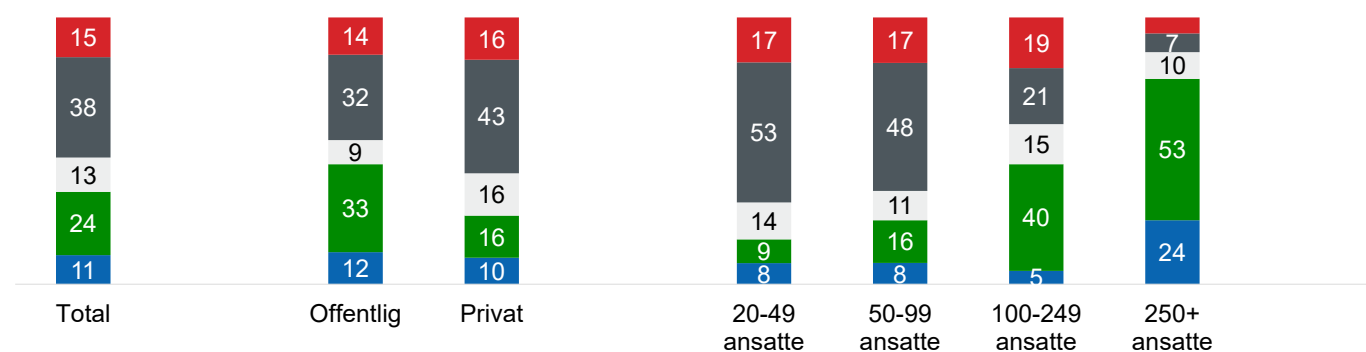
NIS2-DIREKTIVET

Resultatene viser, som forventet, at et fåtall mener at de allerede er berørt av lovverket. Det er stort sett selskaper, som er en del av større konsern med hovedkontor eller avdelinger i EU-land, som er direkte berørt og må etterleve kravene. Videre kan noen leverandører

eller tror at de vil bli berørt av regelverket når det trer i kraft. Dette kan tyde på en manglende forståelse av direktivets rekkevidde. Selv om en virksomhet ikke er direkte påvirket, kan den fortsatt være en del av verdikjeder og dermed omfattes av direktivet - indirekte.

■ Vet ikke
■ Vi vil mest sannsynlig ikke bli berørt når NIS2 trer i kraft i Norge
■ Vi er allerede berørt gjennom EUs lovverk

■ Jeg er ikke kjent med NIS2-direktivet
■ Vi vil mest sannsynlig bli berørt når NIS2 trer i kraft i Norge



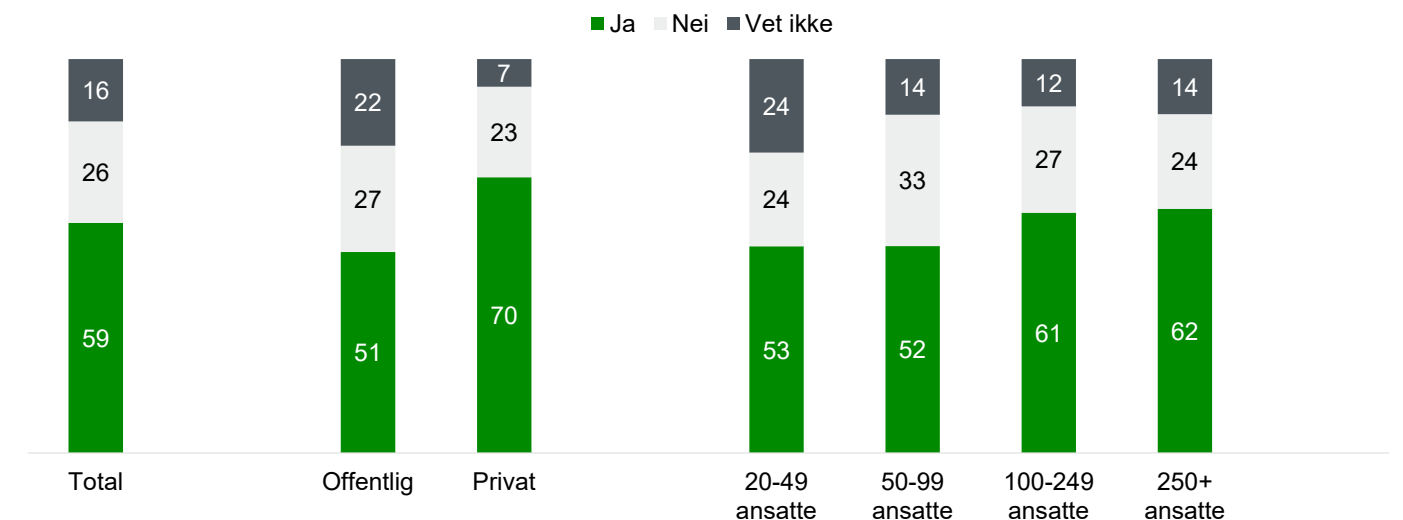
NIS2-direktivet og virksomheten: Hvordan påvirker NIS2-direktivet virksomheten?

av tjenester eller produkter med leveranser til EU-baserte selskaper som er direkte underlagt direktivet, være pålagt å følge tilsvarende krav for å opprettholde samarbeidet.

At nesten 40 % av private virksomheter ikke er kjent med NIS2-direktivet kan tyde på flere ting:

- Til tross for flere års kjennskap til direktivet i EU, har det vært mangel på målrettet kommunikasjon i Norge.
- Mange tror kanskje at dette ikke vil påvirke deres virksomhet da de ikke anser seg som en del av kritisk infrastruktur, og derfor har de ikke satt seg inn i det kommende lovverket.
- Siden direktivet foreløpig kun er et direktiv og ennå ikke har blitt implementert som lov, velger mange å avvende nasjonale krav før de prioriterer dette.
- Det er et begrenset fokus på sikkerhet i små og mellomstore bedrifter, og disse virksomhetene mangler ofte dedikerte ressurser for cybersikkerhet.

Resultatene indikerer at større virksomheter i høyere grad er kjent med direktivet og den største andelen av disse er i offentlig sektor. Imidlertid viser undersøkelsen at over 65 % av virksomhetene totalt ikke er kjent med



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

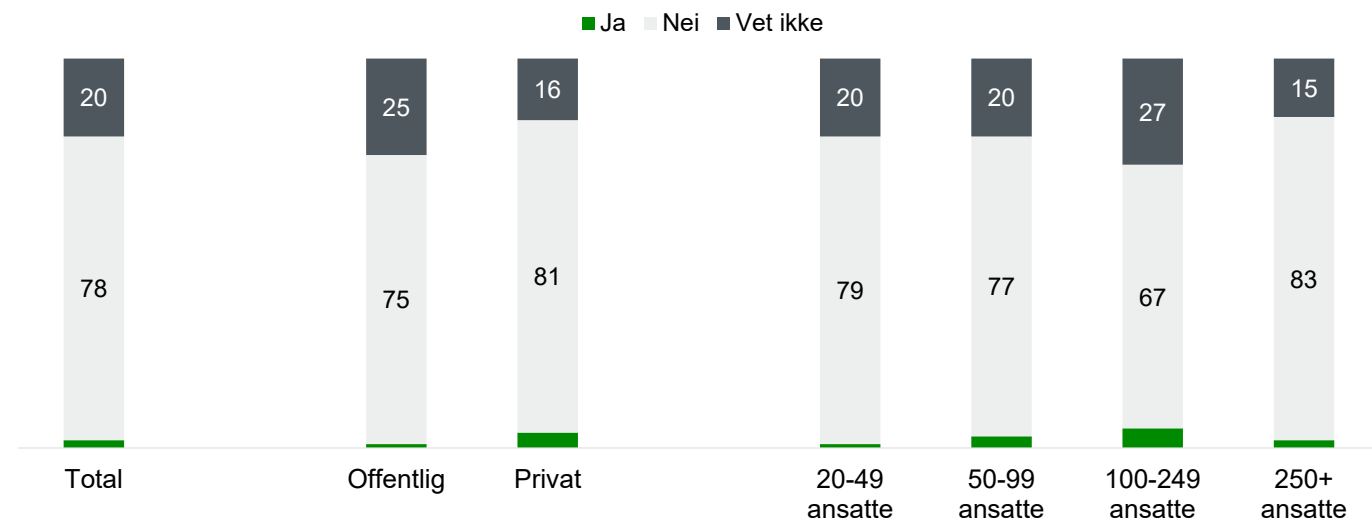
Mange respondenter oppgir at de har en aktiv tilnærming til NIS2, og at virksomhetene arbeider målrettet for å oppfylle kravene. Virksomhetene vil være bedre forberedt hvis de har en proaktiv holdning og har et forhold til egen modenhet (gapet mellom ønsket nivå og kravene). For virksomheter som ennå ikke har påbegynt arbeidet, må det forventes en tidkrevende og betydelig innsats med å etablere nødvendige prosesser for å møte lovkravet.

Det er verdt å merke seg at 49 % av offentlige virksomheter svarer nei eller vet ikke på spørsmålet om virksomheten jobber målrettet mot å innfri kravene i NIS2. Det er krav til at virksomhetens øverste ledelse har ansvar for forebyggende sikkerhetsarbeid. Kan det være at offentlige virksomheter i dag ikke jobber aktivt mot å tilfredsstille dette kravet? NIS2-kravene blir en del av norsk lov, og manglende samsvar kan medføre økonomiske sanksjoner. Hovedfokus bør likevel være den grunnleggende hensikten bak direktivet:

«NIS2-direktivet er en hjørnesten i EUs innsats for å sikre et høyt felles nivå av cybersikkerhet i alle medlemsland»

Ved å gi spesifikke føringer for god cybersikkerhet, sikre et samarbeid mellom medlemsland og definere spesifikke krav, er formålet å øke den generelle sikkerheten i EU/EØS. Dette målet bør være interessant for alle virksomheter uavhengig om man er underlagt direktivet eller ikke.

I undersøkelsen kommer det frem at det foreløpig er få norske bedrifter som får krav fra egne kunder angående NIS2. NIS2 skulle vært på plass i alle EU-land i oktober i fjor, men de nasjonale regelverksendringene er ikke på plass i alle land enda. For eksempel så kommer Sverige, som mange norske bedrifter samarbeider med, til å innføre ny lov tidligst sommeren 2025.



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

Uansett, det forventes at disse tallene vil øke i perioden som kommer. Ettersom artikkel 21 i direktivet stiller krav til sikkerhet i leverandørkjeden, bør norske virksomheter tidlig sette seg inn i kravene.

Dersom en virksomhet mottar krav fra kunder eller

samarbeidspartnere og ikke kan dokumentere samsvar, kan dette medføre tap av forretningsmuligheter. Det er derfor ikke bare en regulatorisk nødvendighet, men også et strategisk konkurransefortrinn å aktivt dokumentere og jobbe mot etterlevelse av regelverket.

AVSLUTNING

Dagens trusselbilde er mer komplekst og uforutsigbart enn noensinne. Cyberkriminelle opererer i stadig større grad som profesjonelle aktører, ofte med støtte fra statlige eller organiserte grupper. Vi ser en økning i sofistikerte angrep, hvor kunstig intelligens brukes både til å finne sårbarheter og til å automatisere angrepsprosesser. Ransomware-angrep, datalekkasjer og cyberangrep rammer ikke lenger bare enkeltbedrifter, men også kritisk infrastruktur, offentlige tjenester og globale verdikjeder.

Den geopolitiske situasjonen forsterker også IT-sikkerhetsutfordringene. Krigen i Ukraina har vist hvordan digitale angrep kan brukes som et våpen i hybride konflikter, og spenninger mellom stormakter reflekteres i cyberdomenet. Statlige aktører utnytter sårbarheter for spionasje og økonomisk manipulasjon.

For virksomheter betyr dette at **IT-sikkerhet må være en integrert del av forretningsstrategien**. Med strengere reguleringer som EUs NIS2-direktiv, forventes det at selskaper tar et større ansvar for digital sikkerhet, både internt og i sine verdikjeder. I denne globale situasjonen er samarbeid, beredskap og kontinuerlig overvåking avgjørende for å beskytte data, infrastruktur og samfunnskritiske funksjoner.

Thomas Tømmernes
Konserndirektør for IT-sikkerhet
Atea



**Din totalleverandør av
IT-sikkerhet:**

**Atea er en erfaren
– og den største –
totalleverandøren av
IT-sikkerhet**





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