Næringslivets sikkerhets-råd

Mørketalls-undersøkelsen 2026

Tittel	Mørketallsundersøkelsen 2026
Forfatter	Bjarte Malmedal
Utgave og år	Første utgave, 2026
Sponsorer	Utgitt med støtte av Abelia, Amedia, Coop, Defendable, DNV, Finans Norge, mnemonic, Norges Bank, Orange Cyberdefense, Ruter, Sykehuspartner, TEK-Norge, Telenor, Try og Visma
Faglig bidrag	Spørreundersøkelsen og rapporten er kvalitetssikret av NSRs Utvalg for digital sikkerhet. Medlemmer i utvalget: Andrea Neverdal Skytterholm (SINTEF Digital), Tønnes Ingebrigtsen (mnemonic), Anna McCarthy (Posten Bring), Kenneth Eide (Visma), Johnny Mathisen (Telenor), Vibeke Reigstad (TV2), Martha Eike (Storebrand), Ole Tom Seierstad (Microsoft), Soner Sevin (Coop), Boye Tranum (DNV), Else Gun Ommundsen/Espen Skogstad (Politiet), Eirik Gulbrandsen (Datatilsynet) og Harald Kristian Næss (NSM)
Opphavsrett	Opphavsrett © 2026 Næringslivets Sikkerhetsråd
Medvirkende	Omslagsdesign og innvendig design: Christian von Schack
Bilder	Forsidebilde: Pixabay Bilde side 9, 21, 65, 75 og 89: NSR Bilde side 15, 29, 38 og 83: Pixabay
ISBN	ISBN 978-82-694361-1-2
Kopierings-informasjon	Det må ikke kopieres fra rapporten i strid med åndsverksloven. Ta kontakt med Næringslivets Sikkerhetsråd dersom du ønsker å kopiere eller bruke deler av rapporten.

SPONSORER

INNHOLD

FORORD

Mørketallsundersøkelsen er en av de viktigste kildene vi har til kunnskap om norsk næringslivs faktiske møte med digitale trusler. Dette er 15. gang undersøkelsen gjennomføres, og serien representerer noe sjeldent: et sammenhengende bilde av et trusselbilde i utvikling, dokumentert og analysert i over to tiår.

Funnene i denne rapporten er viktige, ikke fordi de er overraskende, men fordi de gir et bilde av hverdagen i norske virksomheter, offentlige og private. Hendelser underrapporteres, sårbarhetene er kjente, og tiltakene utsettes. Det er ikke mangel på kunnskap som er problemet. Det er mangel på handling, og det er nettopp her undersøkelsen har sin kraft. Den gjør det vanskeligere å se bort. Vi befinner oss i en helt ny sikkerhetspolitisk situasjon. Digitale angrep mot kommuner, sykehus, mediehus og næringsliv er ikke lenger sjeldne hendelser. Angrep gjennom digitale leverandørkjeder, på operasjonsteknologi og gjennom svindelforsøk er den nye hverdagen.

Trusselvurderingene fra PST, NSM og Etterretningstjenesten er entydige: statlige aktører og kriminelle nettverk retter seg systematisk mot norske virksomheter. Digitale angrep er ikke lenger et sidespor i norsk sikkerhets- og forsvarstenkning — de er en integrert del av den hybride trusselen vi som samfunn må forholde oss til. Næringslivet er ikke en tilskuer til dette bildet. Det er en sentral aktør.

Kunstig intelligens har endret angrepsflatene. Terskelen for å gjennomføre troverdige, skalerbare cyberangrep er senket dramatisk. Det stiller nye krav til teknologisk robusthet, til menneskelig årvåkenhet, og til ledelse. Virksomheter som forstår dette, og handler deretter, vil stå sterkere. De som venter, tar en risiko de sannsynligvis undervurderer. Hvordan vi oppfatter og forstår trusselen er avgjørende for hvordan vi håndterer risikoen som følger med. Kunnskap kan gjøre oss mer bekymret, men bedre i stand til å håndtere risiko.

NSR har de siste årene styrket sin rolle i det nasjonale beredskapsarbeidet. Med etableringen av Næringslivets beredskapssenter og vår funksjon som sektorvis responsmiljø for åtte næringssektorer, er koblingen mellom kunnskap og handling mer direkte enn noensinne. Mørketallsundersøkelsen er en viktig del av dette arbeidet. Den bidrar til et bredere og bedre grunnlag vi trenger for å prioritere riktig, rådgi mer treffsikkert og reagere raskt.

Takk til alle virksomheter som har delt sine erfaringer og besvart årets undersøkelse. Takk også til våre samarbeidspartnere og bidragsytere som gjør dette arbeidet mulig. Dere bidrar til noe langt mer enn en rapport. Dere bidrar til at norsk næringsliv kan se seg selv tydelig i et krevende trusselbilde. Det er et solid bidrag som kan gjøre oss alle bedre.

Odin Johannessen

Direktør NSR

SAMMENDRAG

Mørketallsundersøkelsen 2026 er den femtende i rekken og bygger på svar fra 2 500 norske virksomheter. Den kartlegger mekanismene som gjør at hendelser forsvinner ut av statistikken: manglende oppdagelse, bagatellisering og manglende rapportering.

Sikkerhetsorganisering er svakest der behovet er størst. 38 prosent av virksomhetene mangler en informasjonssikkerhetsansvarlig. Blant de minste stiger andelen til 48 prosent. 51 prosent oppgir å ha et rammeverk for informasjonssikkerhet, men 68 prosent av disse vet ikke hvilken standard det bygger på. Dette er et funn som reiser spørsmål om rammeverket er reelt forankret eller delegert til en leverandør uten at ledelsen forstår hva det innebærer.

Trygghetsfølelsen er høy, men ujevnt fordelt. 83 prosent føler seg trygge. Virksomheter med rammeverk er tryggere (90 prosent) enn de uten (73 prosent). Sosial manipulering, hacktivisme og datatyveri dominerer bekymringsbildet, men bekymring og faktisk forekomst henger ikke sammen. Datatyveri bekymrer 29 prosent, men rammer under 2 prosent. Virksomheter uten sikkerhetsansvarlig vet i større grad ikke hvilke trusler de bør bekymre seg for, noe som sannsynligvis reflekterer manglende bevissthet snarere enn lavere risiko.

Hendelsesraten er lav i rapporten, men trolig høyere i virkeligheten. Sosial manipulering er den vanligste hendelsestypen og rammer 13 prosent. Store virksomheter rapporterer hendelser to til tre ganger oftere enn små. Virksomheter med rammeverk rapporterer *flere* hendelser enn de uten. Ikke fordi de er mer utsatt, men fordi de oppdager mer. Det er deteksjonsevnen, ikke hendelsesraten, som skiller gruppene.

Mørketallene er store. 79 prosent anmeldte ikke hendelsen. 42 prosent vurderte den som ubetydelig. 4 prosent mangler tillit til politiets evne til å hjelpe. I tillegg svarte 3 til 6 prosent «vet ikke» på om de overhodet hadde vært utsatt for de ulike hendelsestypene. Dette er virksomheter som ikke engang vet om de er rammet. Virksomheter som anmelder, iverksetter i langt større grad strukturelle oppfølgingstiltak i etterkant: 42 prosent mot 24 prosent blant de som ikke anmelder.

Privat sektor forstår ikke sin beredskapsrelevans. 58 prosent mener virksomheten ikke spiller noen rolle for nasjonal beredskap. I privat sektor er andelen 71 prosent.

Dette står i direkte kontrast til NSMs fremstilling av leverandørkjeder som de viktigste inngangsportene for trussel-aktører mot norsk infrastruktur. De sårbare segmentene, små og private virksomheter, er også de som i minst grad ser seg som del av en større beredskapshelhet.

Mørketallene oppstår ikke gjennom én mekanisme, men gjennom en kjede. Virksomheter uten rammeverk ser mindre. Virksomheter med rammeverk ser mer, men ledelsen forstår ikke alltid hva rammeverket innebærer. Oppdagede hendelser bagatelliseres. Bagatelliserte hendelser anmeldes ikke. Ikke-anmeldte hendelser følges sjeldnere opp strukturelt, og lærings-sløyfen brytes. Resultatet er at både det nasjonale trusselbildet og den enkelte virksomhetens handlingsrom forblir dårligere forstått enn de kunne ha vært.

INNLEDNING

Mørketallsundersøkelsen kartlegger digitale sikkerhetshendelser som ikke anmeldes til politiet. Undersøkelsen har vært gjennomført siden 2003 og utgis av Næringslivets Sikkerhetsråd (NSR). Årets undersøkelse er den femtende i rekken og bygger på svar fra 2 500 norske virksomheter i privat og offentlig sektor.

Begrepet «mørketall» betyr hendelser som forblir usynlige i offisiell statistikk. De gir et ufullstendig bilde av det faktiske trussellandskapet og gjør det vanskelig for myndigheter og næringsliv å dimensjonere tiltak korrekt. Rapporten undersøker ikke bare omfanget av hendelser, men også mekanismene som gjør at hendelser faller ut av statistikken: manglende oppdagelse, manglende vurdering av alvorlighet og manglende rapportering.

Rapporten kommer i en tid der trusselbildet skjerpes. NSMs Risiko 2026[1] fastslår at det er vesentlige mangler i det forebyggende sikkerhetsarbeidet til norske virksomheter, at cyberoperasjoner rammer bredt på tvers av sektorer, og at russisk etterretning ifølge PST[2] kan se seg tjent med å utføre sabotasjeaksjoner mot mål i Norge. Digital-sikkerhetsloven trådte i kraft 1. oktober 2025 og stiller nye krav til virksomheter som leverer samfunnsviktige tjenester. NIS2-direktivet ventes implementert i norsk rett og vil utvide kravene til enda flere sektorer. Mørketallsundersøkelsen gir et innblikk i hvordan norske virksomheter faktisk står rustet.

1 https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2026

2 https://www.pst.no/wp-content/uploads/2026/02/Nasjonal-trusselvurdering-2026.pdf


Deloitte.

1

Om undersøkelsen

Mørketallsundersøkelsen 2026 ble gjennomført som en kvantitativ spørreundersøkelse blant 2 500 norske virksomheter. Utvalget er stratifisert etter sektor (privat/offentlig) og virksomhetsstørrelse. Respondentene er primært personer med leder- eller sikkerhetsansvar. Datainnsamlingen ble gjennomført av Norstat i januar og februar 2026.

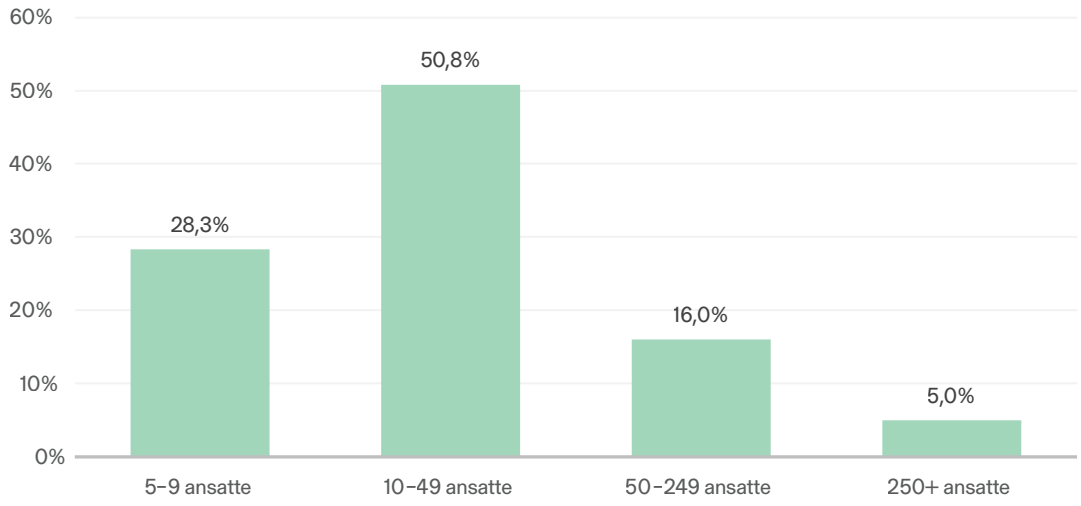
1.1 Om mørketall

Begrepet «mørketall» betegner i denne sammenhengen hendelser som inntreffer, men som aldri fanges opp i offisiell statistikk. Politiet og øvrige sikkerhetsmyndigheter bygger sitt situasjonsbilde på hendelser som anmeldes eller rapporteres til dem. Mørketalls-undersøkelsen er utformet for å komplettere dette bildet ved å kartlegge hendelser som forblir usynlige i de offisielle kildene.

1.2 Respondentprofil

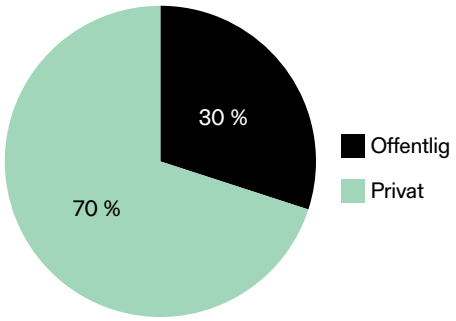
Halvparten av virksomhetene (51 %) har mellom 10 og 49 ansatte. 28 prosent har 5 til 9 ansatte, 16 prosent har 50 til 249 ansatte, og 5 prosent har 250 ansatte eller flere.
70 prosent tilhører privat sektor, 30 prosent offentlig.

Figur 1. Virksomhetsstørrelse

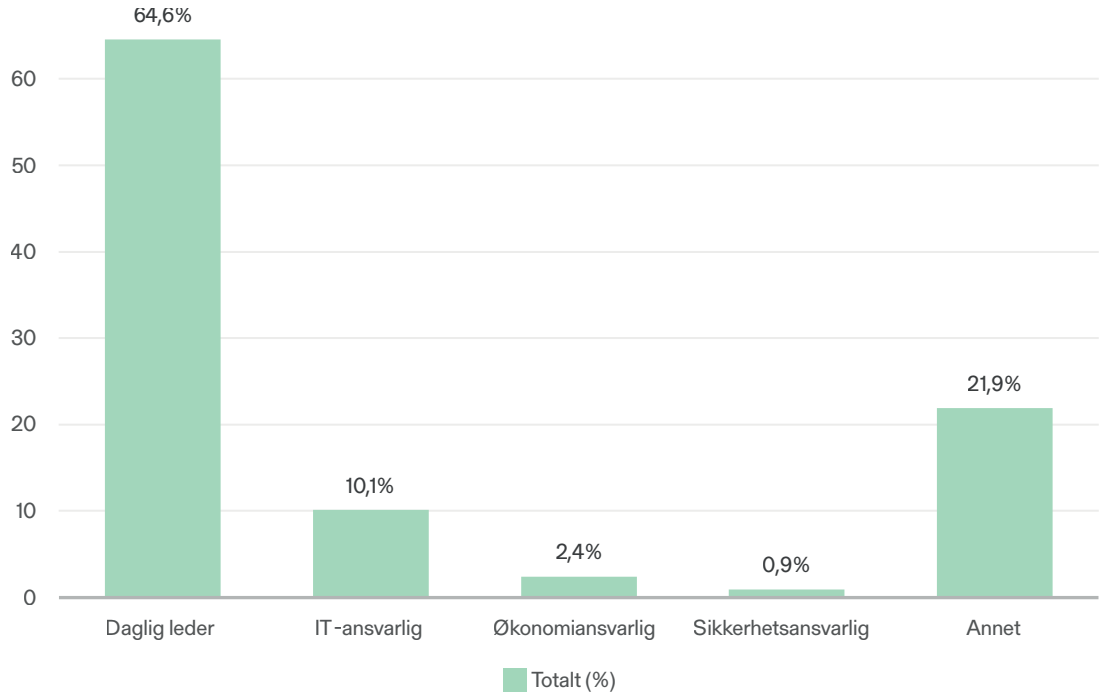


65 prosent av respondentene er daglige ledere. 10 prosent er IT-ansvarlige, under 1 prosent er dedikerte sikkerhetsansvarlige. Andelen IT-ansvarlige stiger fra 4 prosent blant de minste til 37 prosent blant de med over 100 ansatte. I små virksomheter er daglig leder som regel også den som håndterer sikkerhetsansvaret. Det bør ses i sammenheng med den lave rammeverksandelen i dette segmentet.

Figur 2. Fordeling etter sektor



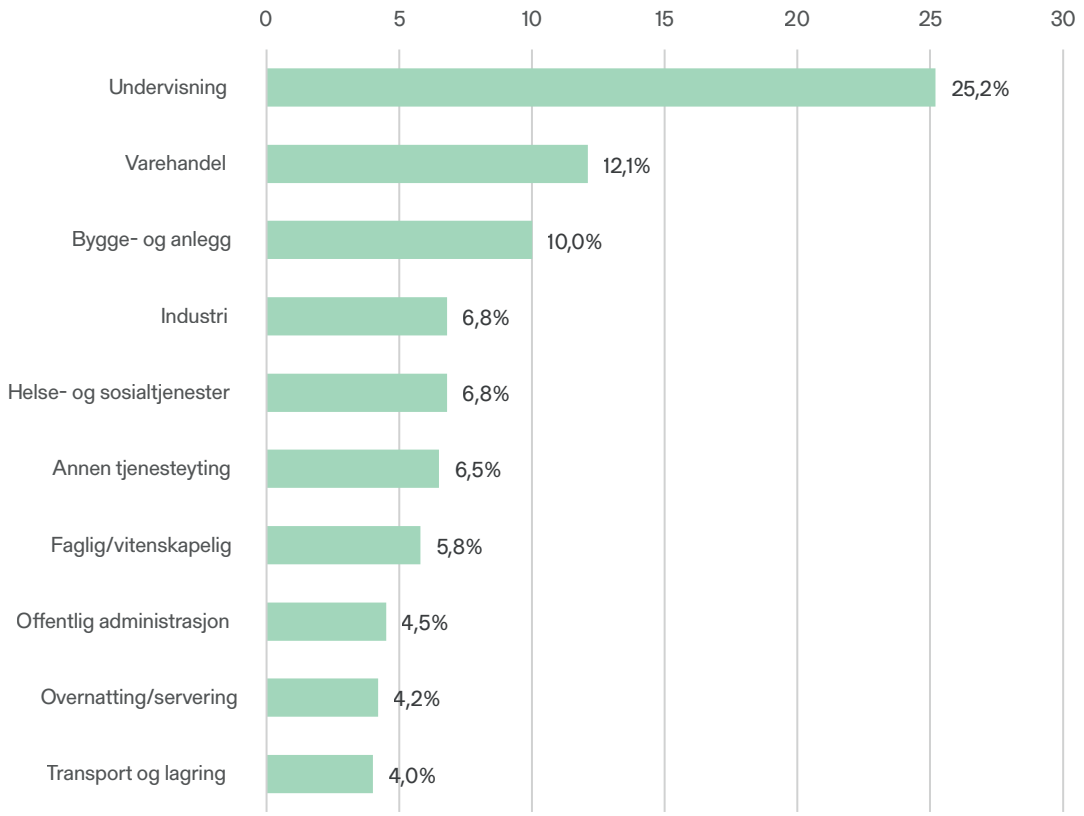
Figur 3. Respondentenes stilling



1.3 Bransjefordeling

Undervisningssektoren utgjør 25 prosent av utvalget og dominerer blant offentlige virksomheter. Varehandel (12 %), bygg og anlegg (10 %) og helse- og sosialtjenester (7 %) følger. Denne sammensetningen påvirker svarene. Bekymringen for personvern og sensitive data i fritekstbesvarelsene, der mange nevner elever og barn, er trolig drevet av den store andelen skoler og utdanningsinstitusjoner.

Figur 4. Bransjefordeling



1.4 Metodiske merknader

Datainnsamlingen ble gjennomført av Norstat som en kvantitativ spørreundersøkelse. Utvalget er stratifisert etter sektor (privat/offentlig) og virksomhetsstørrelse for å sikre tilstrekkelig representasjon i alle segmenter. Resultatene bør tolkes med følgende forbehold:

Respondentprofil. 65 prosent av respondentene er daglige ledere, mens under 1 prosent er dedikerte sikkerhetsansvarlige. Svarene reflekterer derfor i stor grad et ledelsesperspektiv, ikke nødvendigvis den operative sikkerhetssituasjonen.

Selvrapportering. Alle tall er basert på respondentenes egen vurdering. Virksomheter uten formalisert sikkerhetsarbeid kan mangle evne til å identifisere hendelser, noe som innebærer at de reelle mørketallene trolig er høyere enn det undersøkelsen viser.

Utvalgsskjevhet. Undervisningssektoren utgjør 25 prosent av utvalget og dominerer blant offentlige virksomheter. Dette kan påvirke resultatene for offentlig sektor samlet sett, særlig på spørsmål om personvern og beredskapsrelevans.

Størrelsesinndeling. Spørreskjemaet opererer med fire størrelsesgrupper (5–9, 10–49, 50–249, 250+ ansatte), men den statistiske analysen benytter tre grupper (5–19, 20–99, 100+ ansatte) for å sikre tilstrekkelig utvalgsstørrelse i hvert segment. Rapporten bruker begge inndelinger avhengig av kontekst.

Kryssanalyser. Flere kapitler presenterer kryssanalyser mellom spørsmål (for eksempel rammeverk og hendelsesrate). Disse analysene viser statistiske sammenhenger, men sier ikke noe sikkert om årsak og virkning. Undergruppenes utvalgsstørrelse (n) oppgis der det er relevant.

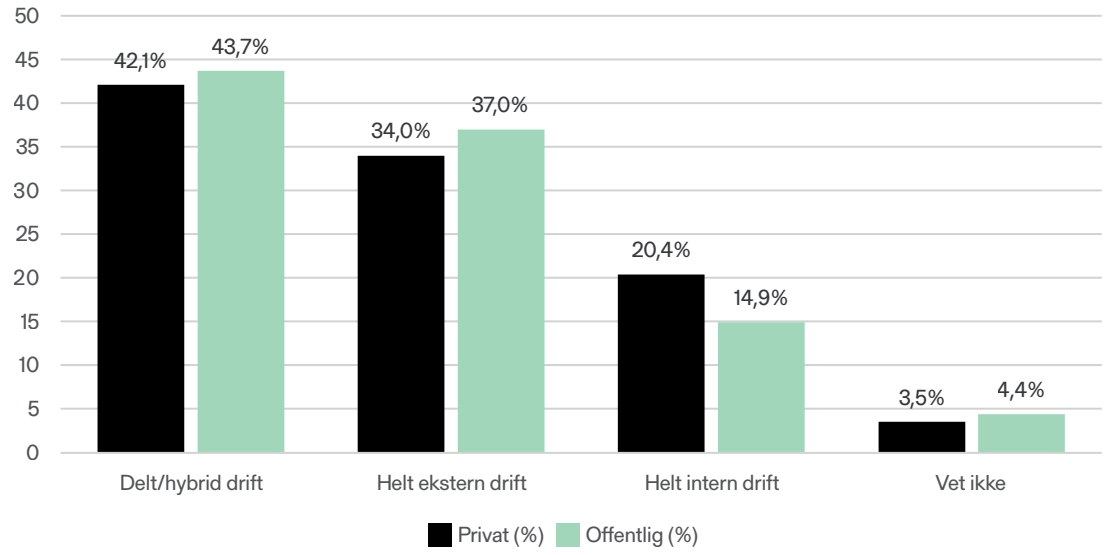
2

Organisering av digital sikkerhet

2.1 IT-organisering

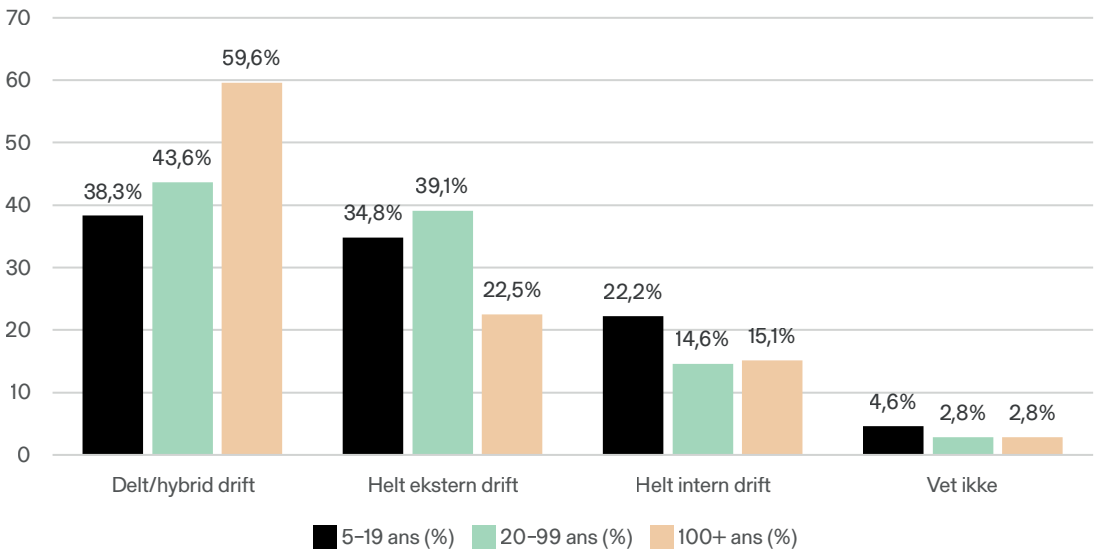
43 prosent av virksomhetene har delt eller hybrid IT-drift. 35 prosent baserer seg helt på ekstern drift. 19 prosent driver IT helt internt.

Figur 5. IT-organisering



Størrelse påvirker driftsmodellen. 60 prosent av virksomheter med over 100 ansatte velger hybrid drift, mot 38 prosent blant de minste. Helt ekstern drift er vanligst blant mellomstore virksomheter (39 %).

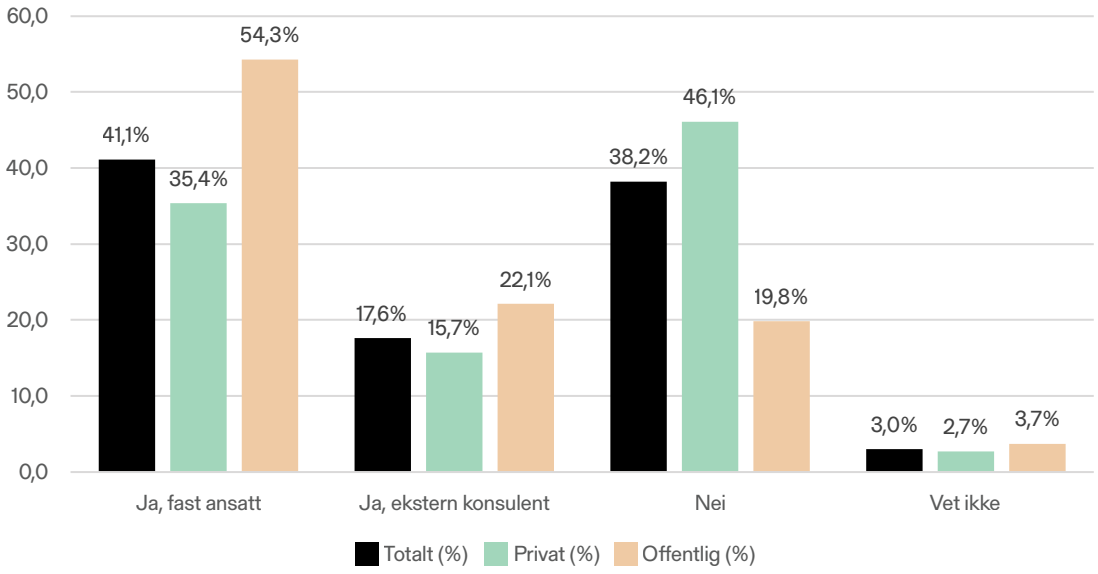
Figur 6. IT-organisering etter virksomhetsstørrelse



2.2 Informasjonssikkerhetsansvarlig

41 prosent har en fast ansatt informasjonssikkerhetsansvarlig, 18 prosent bruker ekstern konsulent. 38 prosent har ingen. Gapet mellom sektorene er påfallende: 46 prosent i privat sektor mangler sikkerhetsansvarlig, mot 20 prosent i offentlig. Blant virksomheter med over 100 ansatte har 70 prosent en fast ansatt, mens andelen blant de minste er 33 prosent.

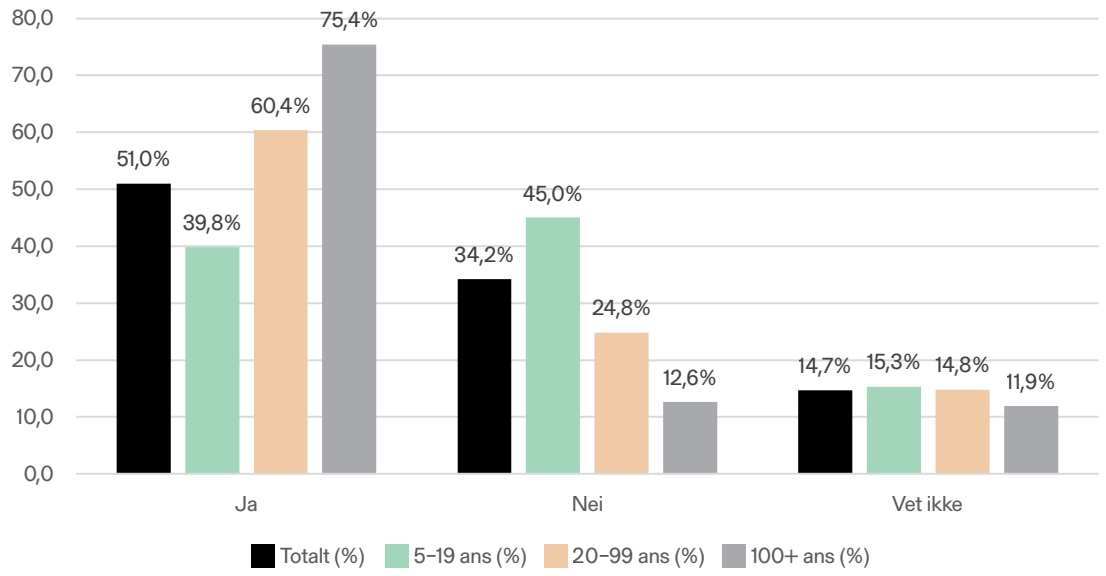
Figur 7. Virksomheten har sikkerhetsansvarlig



2.3 Rammeverk for informasjonssikkerhet

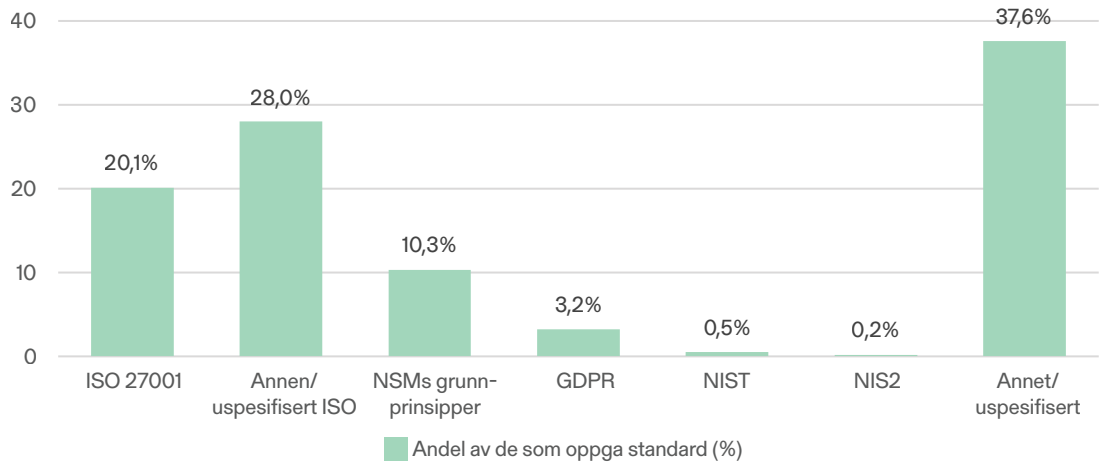
51 prosent oppgir å ha et rammeverk eller styringssystem for informasjonssikkerhet. 34 prosent svarer nei, 15 prosent vet ikke. I offentlig sektor har 68 prosent rammeverk, mot 44 prosent i privat sektor.

Figur 8. Rammeverk for informasjonssikkerhet



Blant de 407 som oppga hvilken standard rammeverket bygger på, dominerer ISO-familien: ISO 27001 (20 %), annen eller uspesifisert ISO (28 %) og NSMs grunnprinsipper (10 %). NIST forekommer knapt.

Figur 9 . Rammeverkstandard

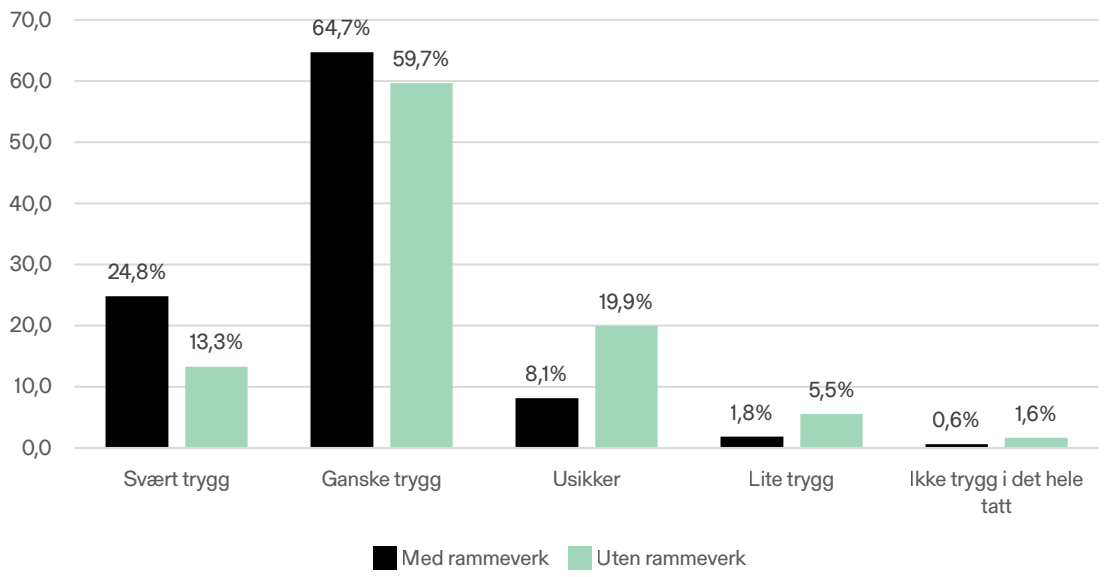


68 prosent av de med rammeverk visste ikke hvilken standard det bygger på. Dette funnet reiser spørsmål om hvor dypt rammeverket er forankret i virksomheten. Når to av tre ledere ikke kan identifisere standarden bak eget styringssystem, kan det tyde på at ansvaret er delegert til IT-leverandør uten tilstrekkelig intern forståelse av hva rammeverket faktisk innebærer. Et rammeverk som eksisterer på papiret, men ikke i praksis gir begrenset beskyttelse.

2.4 Rammeverk og trygghetsfølelse

Kryssanalysen mellom rammeverk (Q4) og trygghetsfølelse (Q6) viser en klar sammenheng. Blant virksomheter med rammeverk ($n = 1\,276$) føler 90 prosent seg trygge, mot 73 prosent blant de uten ($n = 856$). Andelen usikre er mer enn dobbelt så høy blant de uten rammeverk (20 % mot 8 %). Andelen som føler seg direkte utrygge tredobles, fra 2 til 7 prosent.

Figur 10. Bruk av rammeverk og trygghetsfølelse



Sammenhengen sier ikke nødvendigvis at rammeverket gir faktisk beskyttelse. Den kan like gjerne reflektere at rammeverk gir økt opplevd kontroll, eller at virksomheter som allerede prioriterer sikkerhet også velger å formalisere. Uansett kausalitet er mønsteret konsistent: formalisering av sikkerhetsarbeidet henger sammen med opplevd trygghet.

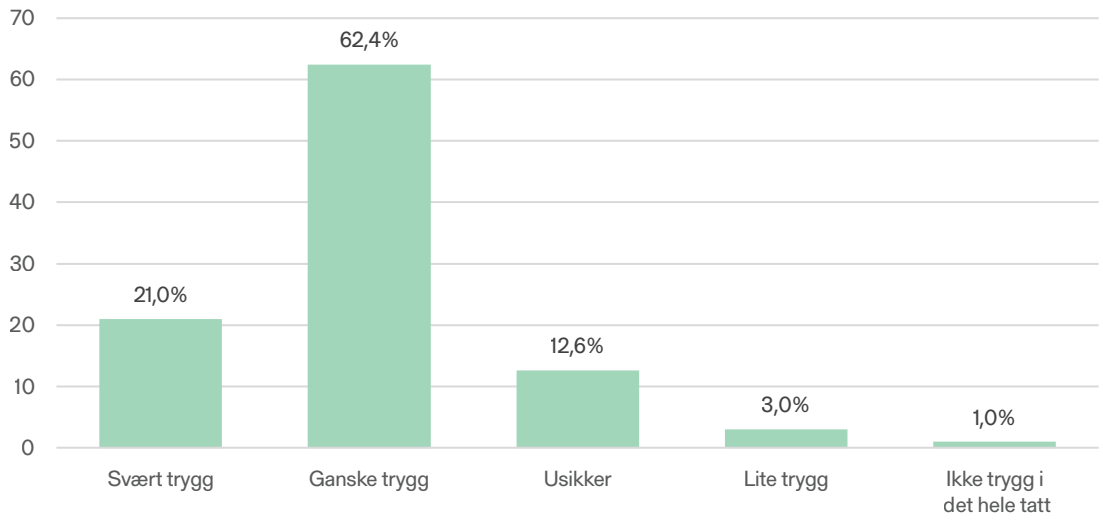
3

Trusseloppfatning

3.1 Trygghetsfølelse

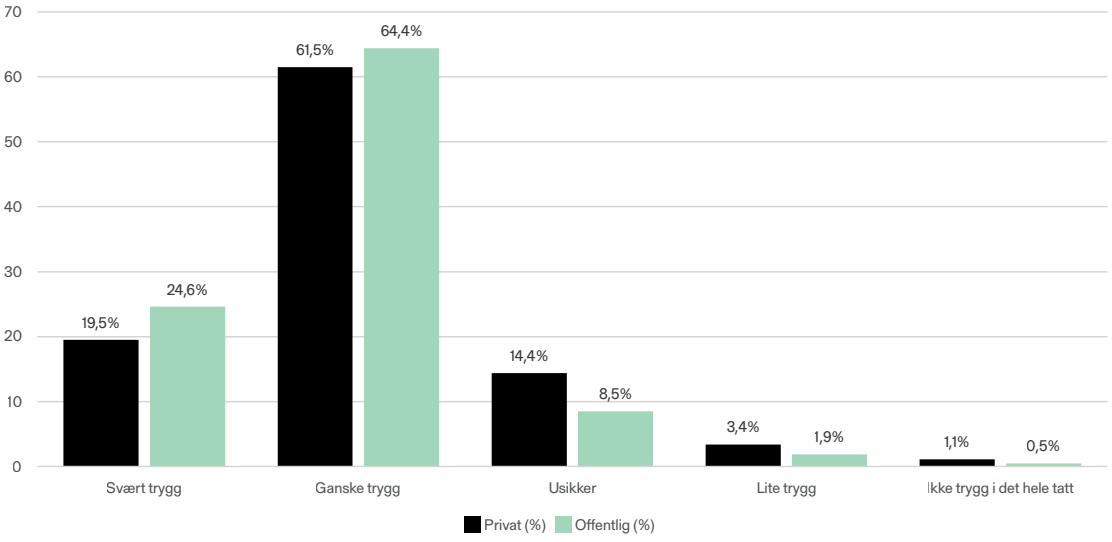
83 prosent føler seg svært trygge (21 %) eller ganske trygge (62 %). 13 prosent er usikre, 4 prosent føler seg lite eller ikke trygge.

Figur 11. Trygghetsfølelse



Offentlig sektor rapporterer marginalt høyere trygghet (89 % mot 81 %). Andelen som er usikre er betydelig høyere i privat sektor (14 %) enn i offentlig sektor (9 %). Denne forskjellen kan henge sammen med at offentlige virksomheter oftere har formalisert sikkerhetsarbeidet gjennom rammeverk og dedikerte roller. Denne sammenhengen bekreftes av kryssanalysen i kapittel 2.4.

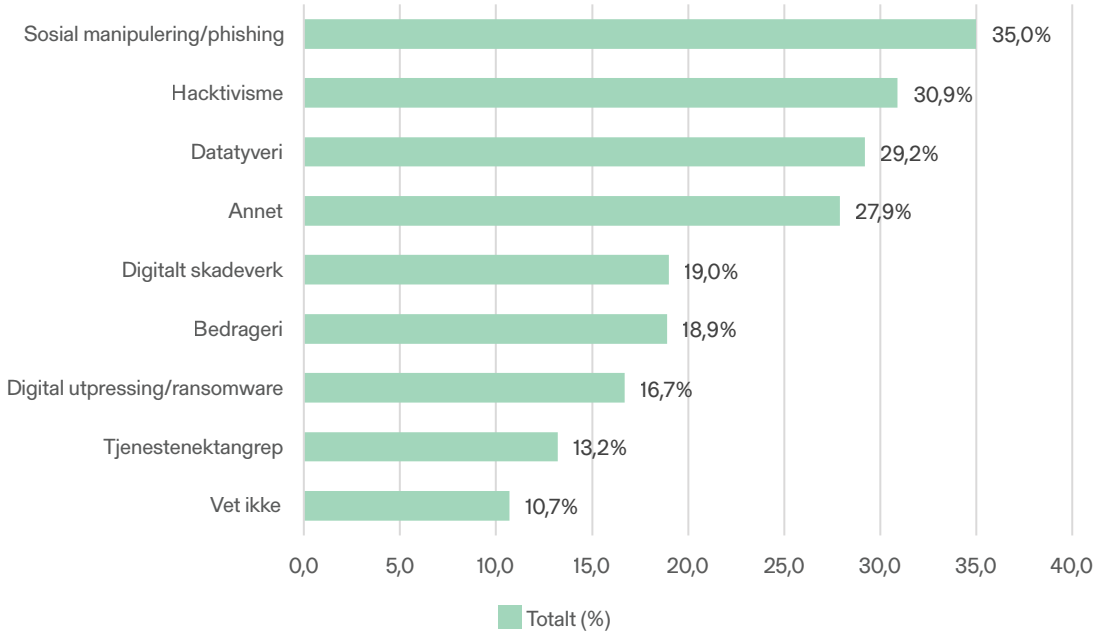
Figur 12. Trygghetsfølelse etter sektor



3.2 Bekymring for konkrete trusler

Sosial manipulering bekymrer flest (35 %), fulgt av hacktivisme (31 %), datatyveri (29 %), digitalt skadeverk (19 %), bedrageri (19 %) og digital utpressing (17 %). 11 prosent svarte «vet ikke», en andel som stiger til 14 prosent blant de minste virksomhetene, noe som antyder lavere bevissthet om trusselbildet.

Figur 13. Bekymring for konkrete digitale trusler



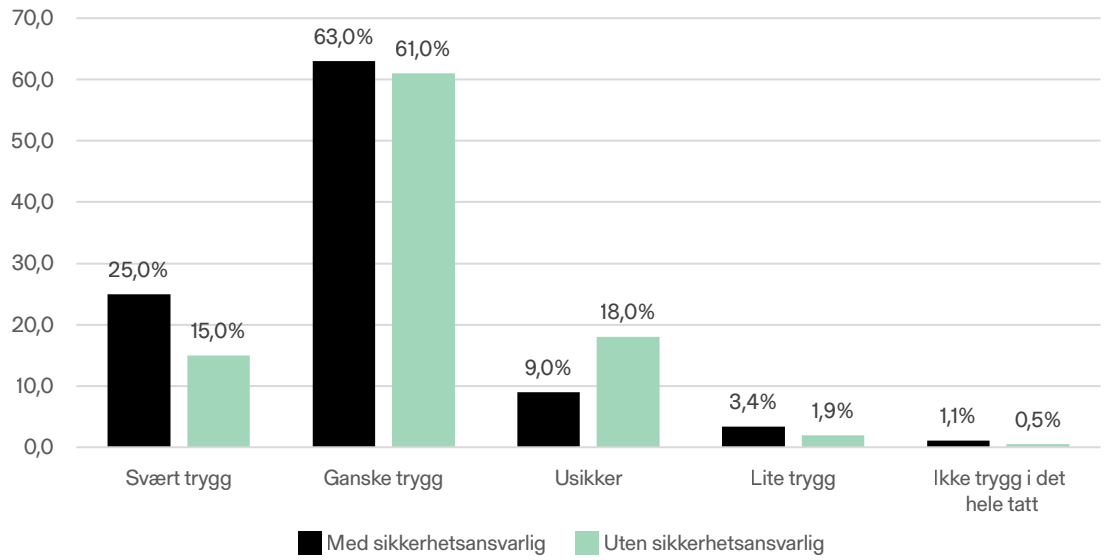
Store virksomheter (100+ ansatte) er gjennomgående mer bekymret. 53 prosent frykter phishing mot 30 prosent blant de minste. For digital utpressing er forskjellen enda større: 33 prosent mot 14 prosent. Denne gradienten gjenspeiler trolig at større virksomheter opplever flere faktiske forsøk og har bedre innsikt i trusselbildet gjennom sikkerhetsmonitorering, og ikke at mindre virksomheter er mindre eksponert.

Fritekstanalysen av «andre trusler» (697 svar) avdekker bekymringer utenfor de predefinerte kategoriene. Hacking i generell forstand nevnes av 19 prosent. Personvern og sensitive data, særlig om elever og barn, utgjør 13 prosent, trolig drevet av den store andelen undervisningsvirksomheter i utvalget. AI-relaterte trusler, inkludert deepfakes, nevnes av 2 prosent. Statlige trusler og sabotasje nevnes sjelden blant respondentene, til tross for at NSMs *Risiko 2026* fremhever sabotasje og cyberoperasjoner som sentrale risikofaktorer. Diskrepansen kan tyde på at virksomhetene primært tenker på trusler de selv har erfart, ikke de som preger det nasjonale trusselbildet.

3.3 Sikkerhetsansvarlige og bekymring for trusler

Virksomheter med en sikkerhetsansvarlig føler seg tryggere, men er mer bekymret. 25 prosent føler seg svært trygge, mot 15 prosent blant de uten. Andelen usikre eller utrygge er 12 prosent i den første gruppen, mot 20 prosent i den andre. Forskjellen er statistisk signifikant.

Figur 14. Trygghetsfølelse etter sikkerhetsansvarlig



Samtidig er de mer bekymret for konkrete trusler. Virksomheter med sikkerhetsansvarlig oppgir gjennomgående høyere bekymring på seks av syv trusselområder. Kombinasjonen av høyere trygghet og høyere bekymring er ikke et paradoks. De som kjenner trusselbildet best, vet hva de bør være bekymret for. En mulig forklaring er at de føler seg trygge fordi de har tiltak, men bekymret fordi de forstår hva som står på spill.

Størst forskjell på datatyveri og phishing

Datatyveri viser den største forskjellen. 35 prosent av virksomhetene med sikkerhetsansvarlig er bekymret, mot 22 prosent uten. Differansen på 13 prosentpoeng er den høyeste på tvers av alle trusselområder.

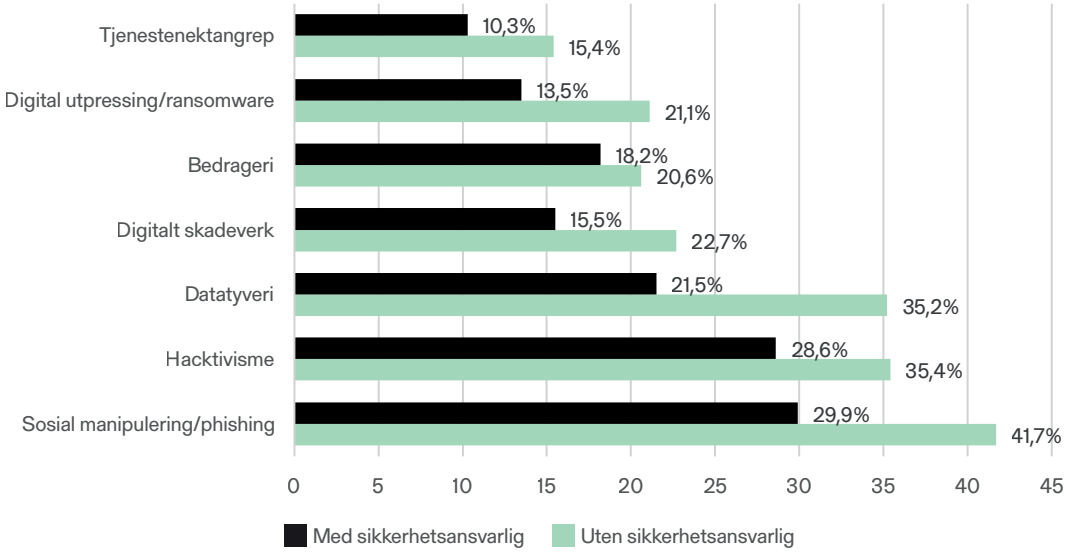
Sosial manipulering og phishing følger med 9 prosentpoeng: 42 prosent mot 30 prosent. For løsepengevirus er forskjellen 6 prosentpoeng (21 % mot 14 %), for digitalt skadeverk tilsvarende (22 % mot 16 %).

Bedrageri er unntaket.

Her er bekymringen praktisk talt lik: 20 prosent mot 18 prosent. Forskjellen er ikke signifikant. Bedrageri er den trusselen som treffer bredest uavhengig av sikkerhetskompetanse,

trolig fordi det rammer gjennom alminnelige forretningsprosesser som fakturering snarere enn gjennom teknisk infrastruktur.

Figur 15. Bekymring for digitale trusler etter sikkerhetsansvarlig



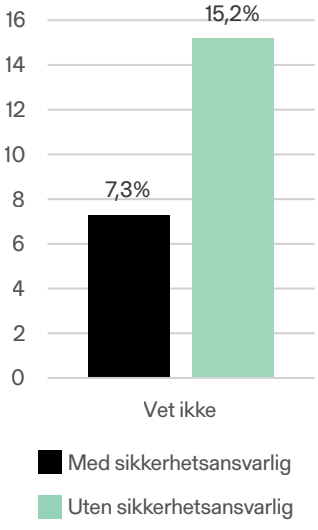
Det mest slående funnet ligger i «vet ikke»-kategorien. 15 prosent av virksomhetene uten sikkerhetsansvarlig vet ikke hvilke trusler de er bekymret for. Blant de med er andelen 8 prosent. Forskjellen er signifikant.

Denne forskjellen forsterker mørketallslogikken: virksomheter som mangler kompetanse til å forstå trusselbildet, kan heller ikke rapportere hendelser de ikke gjenkjenner som hendelser. Det lave bekymringsnivået blant virksomheter uten sikkerhetsansvarlig er sannsynligvis ikke et uttrykk for faktisk lavere risiko, men for lavere bevissthet.

Virksomheter med sikkerhetsansvarlig er altså mer bekymret for konkrete trusler, men føler seg tryggere. Virksomheter uten er mindre bekymret, men mer usikre. Mønsteret støtter tolkningen at lav bekymring i denne konteksten signaliserer manglende innsikt, ikke fravær av risiko. Særlig på datatyveri, phishing og løsepengevirus, de områdene som krever mest teknisk forståelse, er gapet størst.

Unntaket bedrageri bekrefter mørketallslogikken fra motsatt side: når trusselen treffer gjennom alminnelige forretningsprosesser, jevnes forskjellen mellom gruppene ut.

Figur 16. «Vet ikke» hvilke trusler man er bekymret for



3.4 Finans Norge: Analyse

Finansnæringen opererer i et trusselbilde som over tid har blitt både mer komplekst og krevende å håndtere. Erfaringene fra våre medlemsvirksomheter viser en tydelig utvikling der tradisjonelle skiller mellom ulike typer trusselaktører og angrepsformer i økende grad viskes ut. Statlige aktører, organiserte kriminelle og opportunistiske aktører benytter i dag mange av de samme metodene, og angriper ofte de samme sårbarhetene. Særlig knyttet til digitale verdikjeder, data og tillit.

Et sentralt utviklingstrekk er økt avhengighet av digitale leverandørkjeder. Finansielle tjenester produseres i dag gjennom komplekse økosystemer av tredjepartsleverandører, skytjenester og programvarekomponenter. Dette øker innovasjonstakten, men utvider samtidig angrepsflaten betydelig. Erfaringene viser at trusselaktører i økende grad får tilgang via svakheter i leverandørkjeder for å få indirekte tilgang til større og bedre sikrede mål. Sårbarheter hos én aktør kan raskt få konsekvenser på tvers av sektoren.

Samtidig ser vi et økende fokus på datasuverenitet og kontroll over egne data. Finansnæringen håndterer store mengder sensitiv informasjon, og både regulatoriske krav og geopolitiske forhold bidrar til økt oppmerksomhet rundt hvor data lagres, behandles og hvem som har tilgang. Utfordringen er å balansere behovet for effektiv bruk av globale skyløsninger med krav til nasjonal kontroll, sikkerhet og tillit. Dette er ikke lenger kun et teknologisk spørsmål, men i økende grad et strategisk og sikkerhetspolitisk anliggende.

Innenfor økonomisk kriminalitet er svindel fortsatt den mest utbredte trusselen, og utviklingen går i retning av mer målrettede og sofistikerte angrep. Angriperne utnytter både tekniske og menneskelige sårbarheter, ofte i kombinasjon. Erfaringene viser at angriperne i større grad enn tidligere benytter tilgjengelig informasjon om virksomheter og ansatte for å tilpasse angrepene og øke sannsynligheten for suksess. Dette forsterker behovet for helhetlige tiltak som kombinerer teknologi, kompetanse og bevisstgjøring.

Bruken av kunstig intelligens (KI) er en tydelig forsterker i dette bildet. På den ene siden gir KI betydelige muligheter for bedre deteksjon, analyse og håndtering av trusler. På den andre siden bidrar teknologien til å senke terskelen for å gjennomføre avanserte angrep. Generativ KI brukes allerede til å utvikle mer troverdige phishing-kampanjer, automatisere angreps-prosesser og for å tilpasse skadevare. KI-modeller blir også mer og mer avanserte, er i stand til å avdekke hittil ukjente sårbarheter, og kan vise hvordan disse sårbarhetene kan utnyttes mye raskere enn hva vi har vært vant til. Dette innebærer at forskjellen mellom enkle og avanserte aktører reduseres, og at volumet og kvaliteten på angrepene øker.

På tvers av disse utviklingstrekkene fremstår ett forhold som særlig tydelig. Trusselbildet er ikke bare mer alvorlig, men også mer sammenvevd. Cyberhendelser oppstår sjelden isolert, men er ofte et resultat av sammensatte forhold som inkluderer teknologi, organisering, leverandøravhengigheter og menneskelige faktorer. Dette stiller nye krav til virksomhetenes evne til å forstå og håndtere risiko på tvers av organisatoriske og teknologiske prosesser.

Finansnæringens erfaring er at robust digital sikkerhet i økende grad må bygges gjennom samarbeid. Informasjonsdeling, felles situasjonsforståelse og koordinert håndtering av hendelser er avgjørende for å møte et trusselbilde i utvikling. Ingen virksomhet håndterer dette alene. Motstandsdyktighet i sektoren er avhengig av at både offentlige og private aktører trekker i samme retning. Det samme vil gjelde tverrsektorielt, for cyberkriminelle kjenner ingen sektorgrenser.


3 4
6 7
3 4 5
3 4
delete

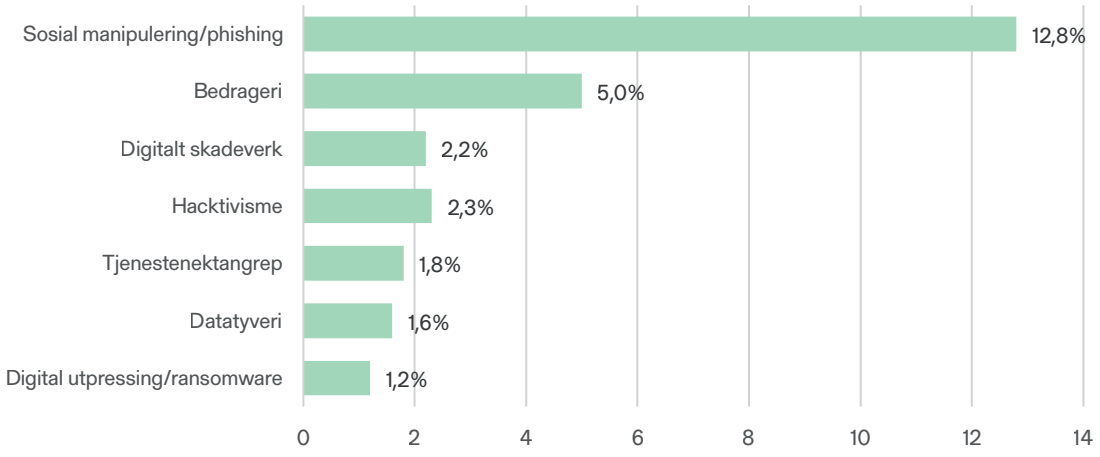
4

Hendelser

4.1 Forekomst

Sosial manipulering rammer 13 prosent av virksomhetene. Bedrageri rammer 5 prosent. Øvrige hendelsestyper (hacktivisme, digitalt skadeverk, tjenestenektangrep, datatyveri og digital utpressing) rammer mellom 1 og 2 prosent hver.

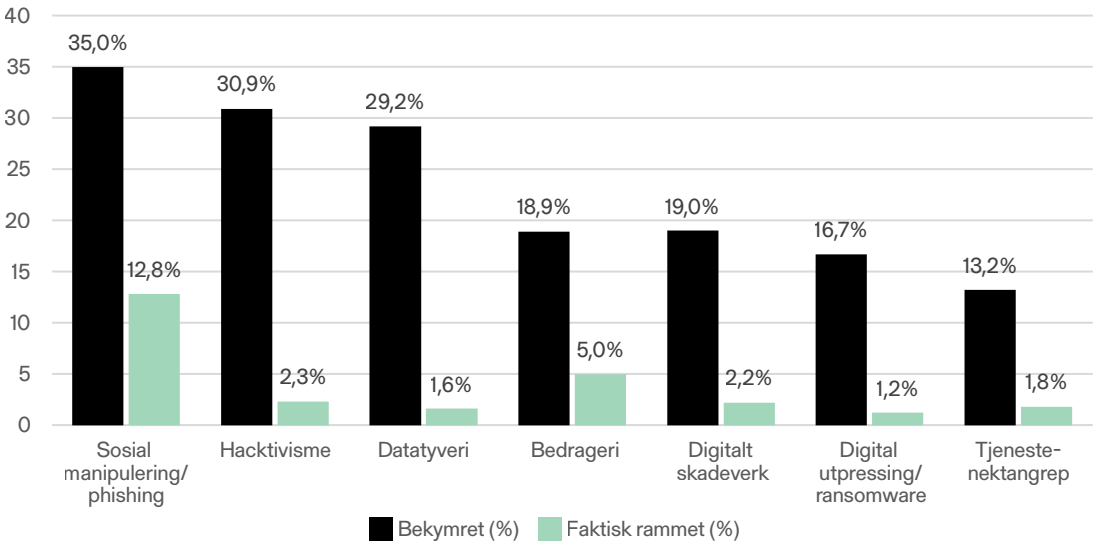
Figur 17. Andel utsatt for hendelse siste 12 måneder



4.2 Gapet mellom bekymring og virkelighet

Datatyveri bekymrer 29 prosent, men rammer under 2 prosent. Hacktivisme bekymrer 31 prosent, men rammer 2 prosent. Sosial manipulering er det eneste området der faktisk forekomst (13 %) nærmer seg bekymringsnivået (35 %). Gapet kan bety at tiltakene fungerer, at hendelsene ikke oppdages, eller at de ikke gjenkjennes som sikkerhetshendelser.

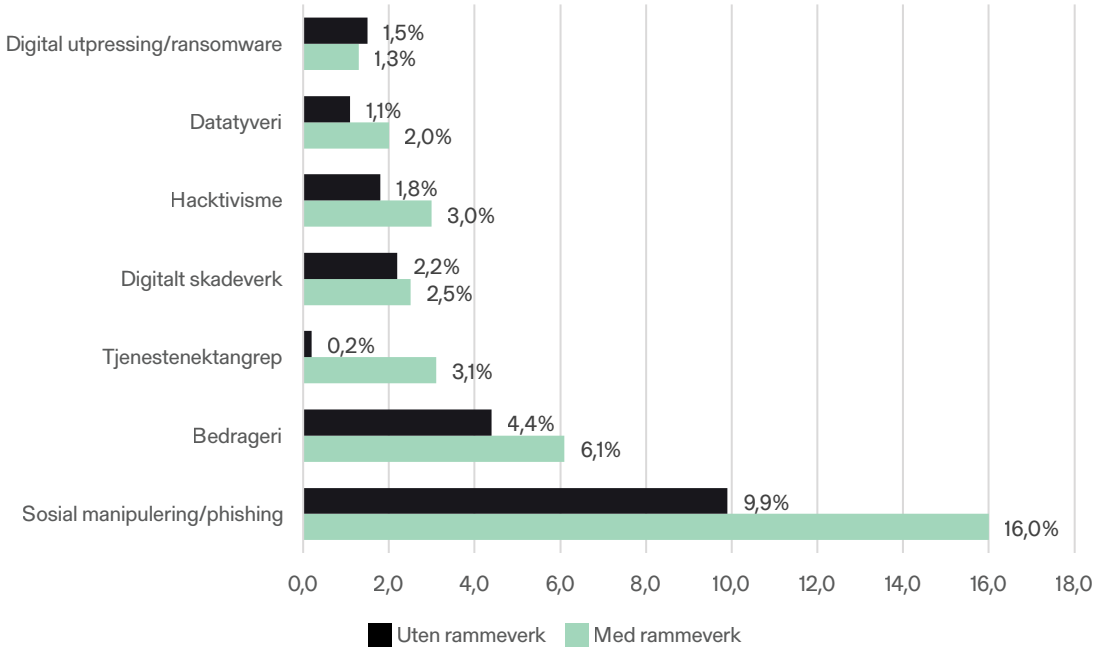
Figur 18. Gap mellom bekymring og faktiske hendelser



4.3 Rammeverk og hendelsesrate

Kryssanalysen mellom rammeverk (Q4) og hendelser (Q8) gir et tilsynelatende paradoksalt resultat. Virksomheter med rammeverk rapporterer flere hendelser (22 %, $n = 286$ av 1 276) enn de uten (16 %, $n = 138$ av 856). For phishing er forskjellen enda tydeligere: 16 prosent mot 10 prosent.

Figur 19. Hendelsesrate etter rammeverk

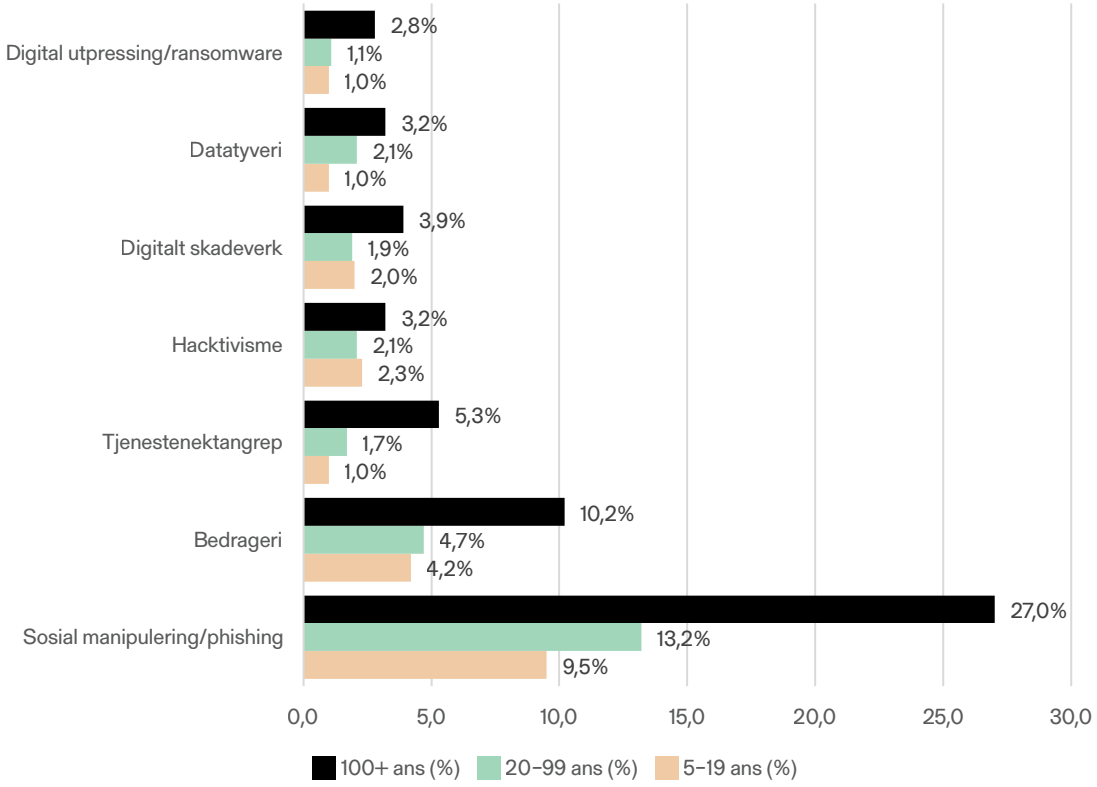


Resultatet er trolig et uttrykk for deteksjonsbias. Virksomheter med formaliserte sikkerhetssystemer har bedre evne til å oppdage, klassifisere og rapportere hendelser. Funnet speiler et kjent mønster: økt deteksjon gir økte tall, ikke nødvendigvis flere reelle hendelser. NSMs *Risiko 2026* understreker at cyberoperasjoner rammer bredt og at både små og store virksomheter må være forberedt på å håndtere hendelser i cyberdomenet. Samme logikk gjelder her: virksomheter uten rammeverk oppdager mindre, og de lavere tallene kan skjule et høyere faktisk omfang.

4.4 Hendelser etter størrelse og sektor

Store virksomheter rapporterer hendelser langt oftere enn små. 27 prosent av virksomheter med over 100 ansatte har vært utsatt for phishing, mot 10 prosent blant de minste. For tjenestenektangrep er forskjellen femdobbel: 5 prosent mot 1 prosent. Forskjellen skyldes en kombinasjon av faktisk eksponering (flere ansatte, flere systemer, høyere synlighet) og bedre deteksjonsevne.

Figur 20. Hendelser etter virksomhetsstørrelse

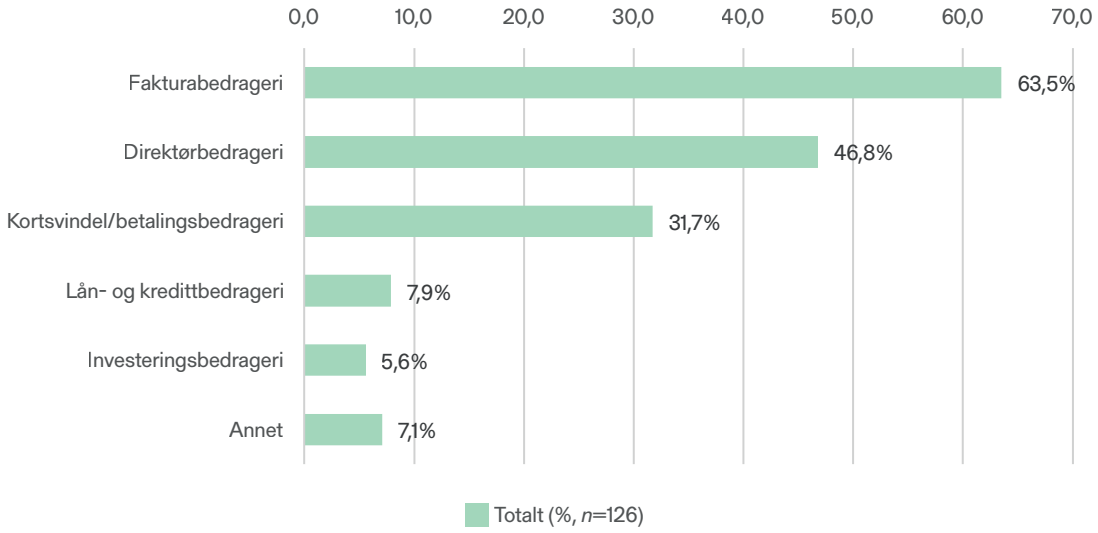


Sektorforskjellene er mer moderate. Phishing-raten er tilnærmet lik (13 % i begge sektorer). Bedrageri rammer privat sektor oftere (5,4 % mot 4,1 %), mens tjenestenektangrep er vanligere i offentlig sektor (2,5 % mot 1,4 %), trolig fordi offentlige virksomheter har mer eksponert digital infrastruktur.

4.5 Bedrageri: Typer og omfang

Blant de 126 virksomhetene som var utsatt for bedrageri dominerer fakturabedrageri (64 %) og direktørbedrageri (47 %). Kortsvindel rammer 32 prosent. Direktørbedrageri er mer utbredt i offentlig sektor (58 %) enn privat (43 %), muligens fordi offentlige virksomheter har synlige hierarkier og kjente titler som svindlere kan utnytte.

Figur 21. Type bedrageri



4.6 Telenor: Analyse

Når sikkerhetshendelser rammer norske bedrifter og virksomheter, starter det sjelden med «avansert hacking». Det starter med noe enkelt: en e-post som ser troverdig ut, en brukerkonto med for vide rettigheter, et system som er feilkonfigurert eller ikke er oppdatert, og ansatte som mangler sikkerhetskunnskap.

Erfaringene fra faktiske angrep og penetrasjonstester viser ofte det samme: Angriperne hopper over gjerdet der det er lavest.

Mange små og mellomstore bedrifter tror de er for små til å være interessante. I realiteten er de ofte attraktive nettopp fordi sikkerhetsnivået er lavere, og fordi de er koblet på større kunder, samarbeidspartnere eller leverandørkjeder. Dermed kan en mindre virksomhet bli inngangsporten til et større angrep, uten selv å være hovedmålet – eller de blir helt enkelt ofre for opportunistiske angrep for økonomisk vinning.

Angrepene utnytter mennesker og hverdagsrutiner

Når sikkerhetshendelser analyseres i etterkant, avdekkes sjelden én enkelt kritisk feil. I stedet finner man en kombinasjon av kjente risikoer og svakheter.

- Systemer er feilkonfigurert
- Gjenbrukte eller svake passord
- Manglende multifaktorautentisering
- For mange brukere med for vide rettigheter
- Brukerkontoer som ikke brukes, er ikke fjernet
- Utdatert programvare og manglende sikkerhetsoppdatering
- Manglende barrierer og segmentering i nettverk og løsninger

Dette handler ikke om uansvarlige ansatte, men om manglende struktur. Når sikkerhet ikke er en del av arbeidshverdagen, blir mennesker det svakeste leddet – helt utilsiktet.

Sikkerhet er ledelse, ikke IT

En gjennomgående lærdom er at virksomheter som er gode på sikkerhet har etablert en sikkerhetskultur. De har gjort sikkerhet til et lederansvar, ikke et sideprosjekt i IT-avdelingen. Ledere har definert hva som er viktig å beskytte, hvem som har ansvar når noe skjer, og hvilke minimumstiltak som alltid skal være på plass. Alt dette rammet inn i et styringssystem.

Dette krever ikke alltid store investeringer, men det krever prioritering, systematikk og bevissthet.

Å bygge sikkerhet er kontinuerlig arbeid

Teknologi kan kjøpes. Motstandskraft må bygges. Virksomheter som lykkes, snakker jevnlig om sikkerhet, øver på hendelser og lærer av nesten-feil. De gjør det tydelig at sikkerhet ikke handler om skyld, men om ansvar.

Når ansatte forstår hvorfor sikkerhet er viktig for drift, kunder og tillit, blir de også en del av forsvaret.

Trusselbildet blir mer komplekst, og digitale angrep rammer bredere enn før. For små og mellomstore bedrifter er det ikke realistisk å beskytte seg mot alt. Men det er fullt mulig å gjøre det vanskeligere å lykkes – og dermed redusere både sannsynlighet og, ikke minst, konsekvens.

Å ta sikkerhet på alvor handler ikke om frykt. Det handler om ansvar. Overfor egne ansatte, kunder og samarbeidspartnere.

4.7 Defendable: Analyse

Det siste året har Defendable sett mange tusen eksempler på små og mellomstore bedrifter som «angriper» våre kunder – uten at de vet det selv.

Et av de viktigste funnene i årets mørketallsrapport er at selve grunnmuren i norsk næringsliv, de små og mellomstore bedriftene, ikke ser på seg selv som del av den digitale beredskapen. Vi vet likevel at de spiller en kritisk rolle i det totale sikkerhets-bildet i Norge.

Defendable er blant Norges største spesialistmiljøer på cybersikkerhet, og vi overvåker private og offentlige virksomheter for å oppdage og stoppe cyberangrep døgnet rundt.

Felles for alle kundene våre er en jevn strøm av phishing-forsøk som prøver å lure til seg brukernavn og passord – og i mange tilfeller også forsøker å komme seg rundt tofaktorautentiseringen de fleste har implementert i dag.

I takt med at teknologien har blitt bedre på å kjenne igjen de «klassiske» e-postene som prøver å lure brukerne, har angriperne funnet nye veier til mål. De siste årene har vi sett en stor økning av phishing-kampanjer som kommer fra legitime norske kontoer – og da gjerne fra personer eller selskaper kundene våre allerede har en relasjon til.

Disse forsøkene sender ofte en lenke til en kompromittert Microsoft SharePoint-side, hvor angriperne har plassert neste steg for å lure til seg innloggingsdetaljer.

Fra mai 2025 til mai 2026 har vårt operasjonssenter stoppet nesten 3500 slike forsøk fra 268 forskjellige norske virksomheter. Her telles kun phishing-forsøk som bruker kompromitterte SharePoint-kontoer fra norske virksomheter. Det totale antallet phishing-forsøk er mange ganger større, og for selskaper med kontakter i utlandet har vi sett flere eksempler på at disse kampanjene starter der og spres raskt videre i Norge.

Ved å ta i bruk denne metoden utnytter angriperne tilliten som er bygget opp mellom norske bedrifter. Ofte er det de små og mellomstore bedriftene som blir de første ofrene, og som legitime leverandører kan de være en effektiv vei inn hos større og mer samfunnskritiske aktører.

Vår erfaring er at bedriften ofte ikke vet at de er angrepet før det er for sent, og at det først blir satt inn tiltak når angriperne har utnyttet tilliten de har bygget opp over år til å angripe andre.

Forståelsen av egen rolle i leverandørkjeden må vi få løftet, men det er også et ansvar for oss som sikkerhetsbransje å hele tiden utvikle oss slik at vi kan levere bedre, billigere og mer effektive tjenester til også mindre selskaper i årene som kommer.

4.8 mnemonic: Analyse

mnemonic ser et vedvarende komplekst og ustabilt trusselbilde. Trusselbildet er i stor grad preget av en dreining mot identitetsdrevne og tillitsbaserte angrepsmetoder, hvor målet er å få brukere og administratorer til å gi legitim tilgang. Angripere manipulerer i større grad tillit og legitimitet fremfor å bryte tekniske barrierer.

Sosial manipulasjon

Sosial manipulering har utviklet seg fra å hovedsakelig være et epostproblem til et identitets- og tilgangsproblem, der angripere i økende grad bruker målrettede og interaktive teknikker som utnytter tillit i forretningsprosesser, brukerstøttekanaler, søkemotorer, samhandlingsverktøy og brukerfeil. Vi ser at vishing har blitt en effektiv inngangsmetode, og ClickFix (FakeCaptcha) er fremdeles utbredt. I det sistnevnte manipulerer angripere brukere til å kopiere og kjøre kommandoer under dekke av feilsøking eller teknisk hjelp, ofte via kompromitterte nettsider og gjennom legitim søkemotoroptimalisering (SEO-forgiftning). Videre ser vi at QRkodephishing (quishing) har etablert seg som en varig forlengelse av identitetsfokusert sosial manipulering. Teknikken ser ut til å bli brukt for å unngå sikkerhetsmekanismer på sentralt forvaltede enheter.

Omgåelse av flerfaktorautentisering (MFA)

Vår erfaring er at AdversaryintheMiddle (AitM)phishing fremdeles er det vanligste inntrengningspunktet, og vishingasaservice er utbredt i mange hendelser. Samtidig har device code phishing hatt en kraftig økning[3]. Teknikken utnytter legitim Microsoft-funksjonalitet og gir angripere tilgang til gyldige sesjonstoken etter at offeret autentiserer seg. Informasjonstyveri er fortsatt en sentral inngangsvei, særlig i miljøer uten tilstrekkelig endepunktssikkerhet. I den sammenheng ser vi en økt målretting mot macOS via blant annet ClickFix og SEO-forgiftning[4]. I tillegg gjør bruk av residential proxies det vanskeligere å oppdage angrep, ved at angripere kan operere fra tilsynelatende legitime IP-adresser og geografiske lokasjoner.

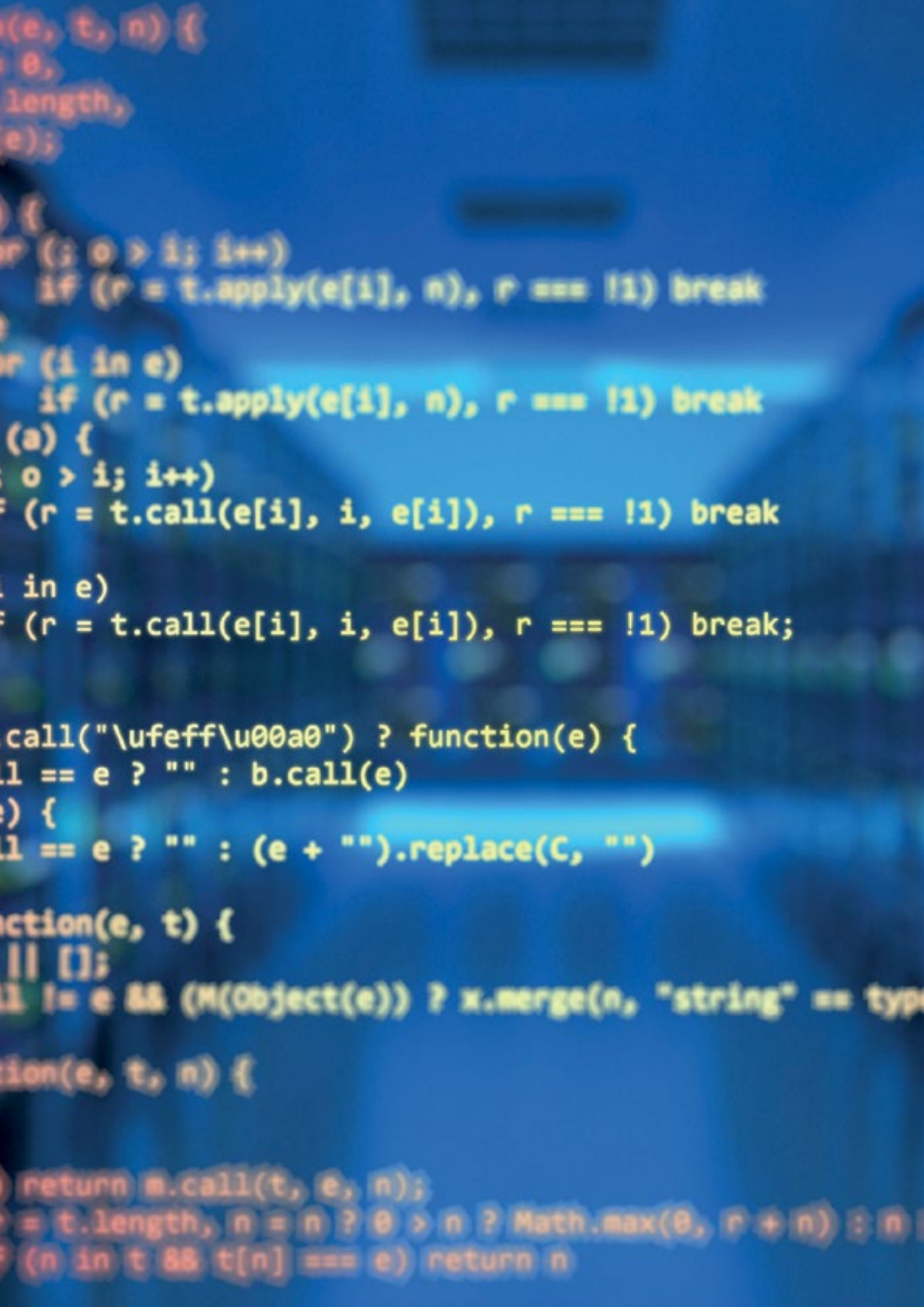
Endepunkt, sky og nettverk

Når det gjelder endepunkt, sky- og nettverksinfrastruktur ser vi at angripere i økende grad utnytter legitime verktøy, brukeratferd og svake kontrollpunkter. Selv om bruk av potensielt uønskede programmer (PUA) ikke var fremtredende i Q1 2026, fortsetter misbruk av legitime fjernstyringsverktøy (RMM) å øke som en effektiv og lite mistenkelig tilgangsmetode. Samtidig utvikler trusselaktører avanserte teknikker for å omgå EDR-løsninger, blant annet ved å utnytte legitime systemfunksjoner, sårbare enhetsdrivere og infrastruktur uten tilstrekkelig overvåkning. I sky- og SaaS-miljøer er datatyveri og utpressing sentrale virkemidler, ofte gjennom kompromitterte identiteter og tredjepartsintegrasjoner. Utviklingsmiljøer og programvareforsyningskjeder er attraktive mål på grunn av deres høye påvirkningspotensial. I tillegg forblir nettverks- og endepunktsenheter kritiske angrepspunkter, spesielt gjennom utnyttelse av nulldagssårbarheter.

3 https://www.mnemonic.io/resources/blog/eviltokens-from-device-codes-to-token-theft/
4 https://www.mnemonic.io/resources/blog/seo-campaign-targeting-claude-code/

Kunstig intelligens (KI)

Per Q1 2026 har ikke mnemonic observert fullt automatiserte, KIdrevne cyberangrep, men KI brukes i økende grad til å effektivisere og skalere angrepskjeden. Det gjelder blant annet i phishing, malvertising og avansert skadevare som kan tilpasse seg og unngå deteksjon. Dette øker tempo og volum i angrep, noe som kan overbelaste forsvars- og responskapasiteter. Man ser også at KI gir økt evne til å identifisere sårbarheter, noe som gir angripere en stor fordel. Parallelt etterspør virksomheter i økende grad støtte til sikker bruk av KI, da teknologien i seg selv utformer nye sårbarheter. Denne utviklingen forventes å øke videre utover året.



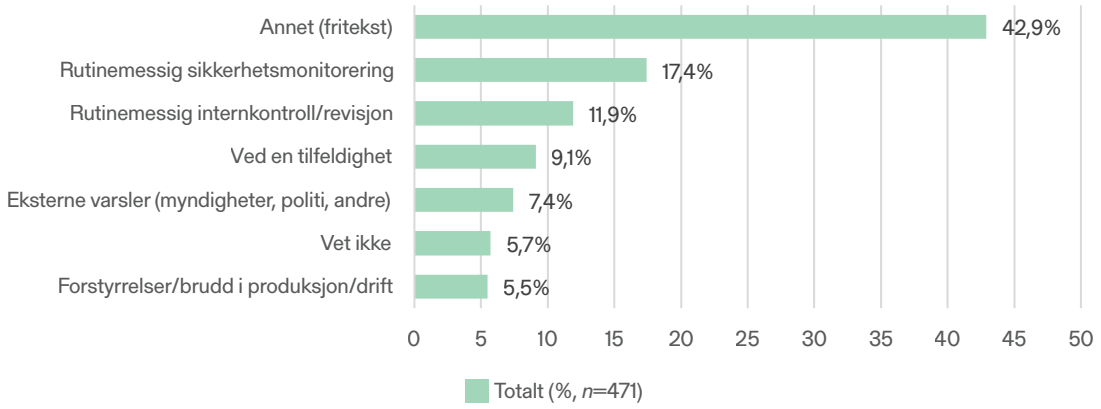
5

Oppdagelse og årsaker

5.1 Oppdagelse

Blant de 452 virksomhetene med hendelse oppga 17 prosent rutinemessig sikkerhetsmonitorering som oppdagelsesmetode. 12 prosent nevnte internkontroll, 9 prosent tilfeldighet, 7 prosent eksterne varsler og 6 prosent driftsforstyrrelser. 43 prosent svarte «annet».

Figur 22. Hvordan hendelsen ble oppdaget



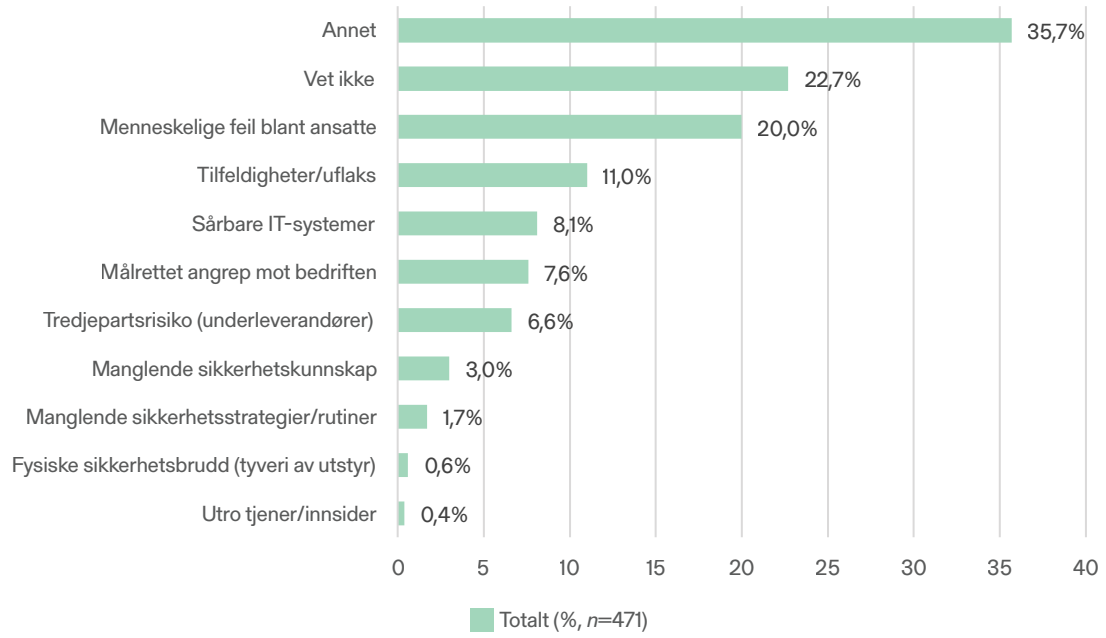
Fritekstbesvarelsene (202 svar) avdekker at mange hendelser oppdages av ansatte som reagerer på mistenkelige e-poster (16 %), av tekniske filtre og varslingssystemer (14 %) eller av oppmerksomme medarbeidere (17 %). Banker og regnskapsførere oppdager hendelser i 5 prosent av tilfellene. Samlet bilde: menneskelig oppmerksomhet, ikke avansert teknologi, er den viktigste oppdagelsesmekanismen for mange virksomheter.

5.2 Medvirkende faktorer

Menneskelige feil blant ansatte var den hyppigst nevnte faktoren (20 %). Tilfeldigheter og uflaks utgjør 11 prosent. Sårbare IT-systemer og målrettede angrep følger med 8 prosent hver. Tredjepartsrisiko, altså sårbarheter hos underleverandører, nevnes av 7 prosent.

23 prosent svarte «vet ikke» på hva som forårsaket hendelsen. Dette er en betydelig andel og illustrerer at mange virksomheter ikke gjennomfører årsaksanalyse etter en hendelse. Uten slik analyse er det vanskelig å iverksette målrettede tiltak, og virksomheten forblir sårbar for gjentakelse.

Figur 23. Medvirkende faktorer



5.3 Orange Cyberdefense: Analyse

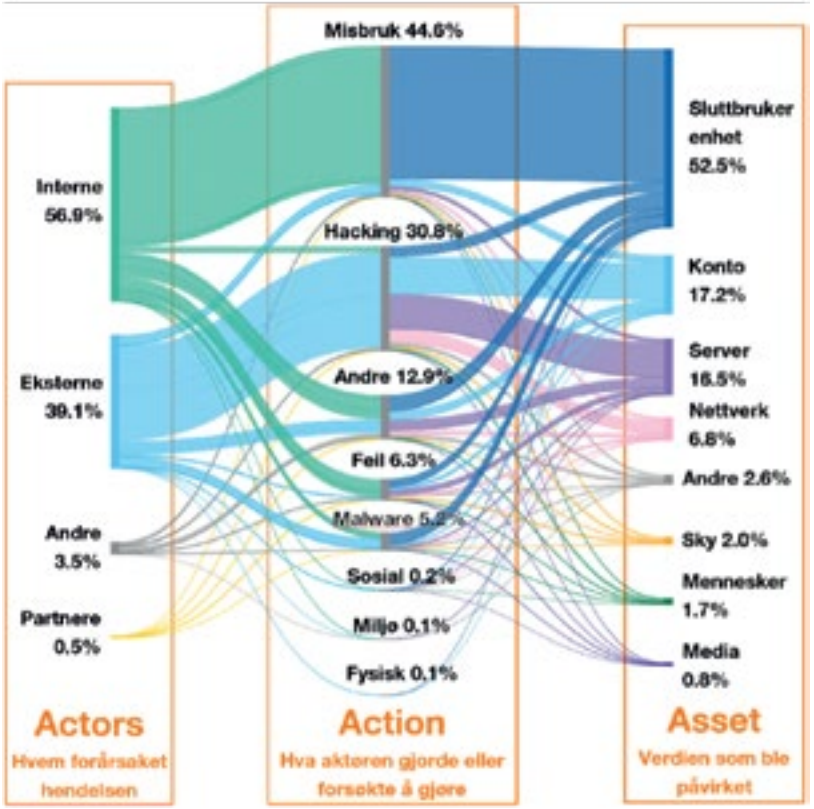
Orange Cyberdefense er en europeisk leverandør av cybersikkerhetsløsninger, inkludert driftede deteksjons- og respons-tjenester (MDR) for hundrevis av store virksomheter på kontinentet. Våre MDR-kapasiteter leveres fra 15 globalt distribuerte sikkerhetsoperasjons-sentre (SOC).

Hvert år gjennomgår våre etterretnings- og forskerteam alle sikkerhetshendelser som er håndtert på tvers av disse SOC-ene, og publiserer resultatene i vår årlige strategiske sikkerhetsrapport, Security Navigator[5].

I årets Security Navigator rapport fremgår det at fra 1. oktober 2024 til 31. august 2025 håndterte vi totalt 139 373 sikkerhetshendelser. Av disse ble 19 053 hendelser (13,7%) bekreftet å utgjøre en reell trussel mot kundens sikkerhet (sann positive). Figuren på neste side viser disse 19 053 bekreftede hendelsene i det åpne VERIS[6]-rammeverket, som vi bruker til å kartlegge hvem som forårsaket hendelsen (actor), hva de gjorde galt (action), og hvilken verdi hos kunden som var truet (asset).

I kapittel 5.2 av årets mørketallsundersøkelse fremkommer det at den største andelen av respondentene (20%) peker på menneskelige feil blant ansatte som en medvirkende faktor

5 https://www.orangecyberdefense.com/no/insights/inspiration/security-navigator
6 https://verisframework.org



til alvorlige sikkerhetshendelser. Dette samsvarer godt med våre funn, hvor flertallet av bekreftede sikkerhetshendelser (56,9%) skyldes interne aktører, altså virksomhetens egne ansatte. Siden de fleste av disse hendelsene involverer misbruk (44,6%) av egne sluttbruker-enheter (52,5%), kan det tolkes som en kombinasjon av brukernes uaktsomhet, manglende etterlevelse av retningslinjer eller ondsinnet hensikt.

Vi tror imidlertid trenden kan tilskrives en generell økt sikkerhetsmodenhet – vi ser stadig flere organisasjoner innfører strengere sikkerhetskontroller, skjerper monitorering og kontroll av endepunkter, som igjen utløser en «oppryddingsprosess» etter hvert som endepunkter og brukere lærer etterlevelse av disse nye kontrollene.

Vi mener imidlertid at denne trenden kan tilskrives en økt sikkerhetsbevissthet og modenhet i organisasjonene. Vi ser stadig flere virksomheter innfører strengere sikkerhetskontroller, skjerper overvåkning og kontroll av endepunkter, noe som ofte utløser en «oppryddings-prosess» etter hvert som brukere og endepunkter lærer å etterleve de nye kravene.

Selv om forbedret overvåkning hjelper oss å filtrere ut falske positive hendelser, viser dette også at teknologiske fremskritt gir økt innsikt - både på godt og vondt. Skjerpet overvåkning gjør det mulig å oppdage flere reelle trusler før skaden er skjedd, forutsatt at man evner å håndtere den økte mengden data og varsler.

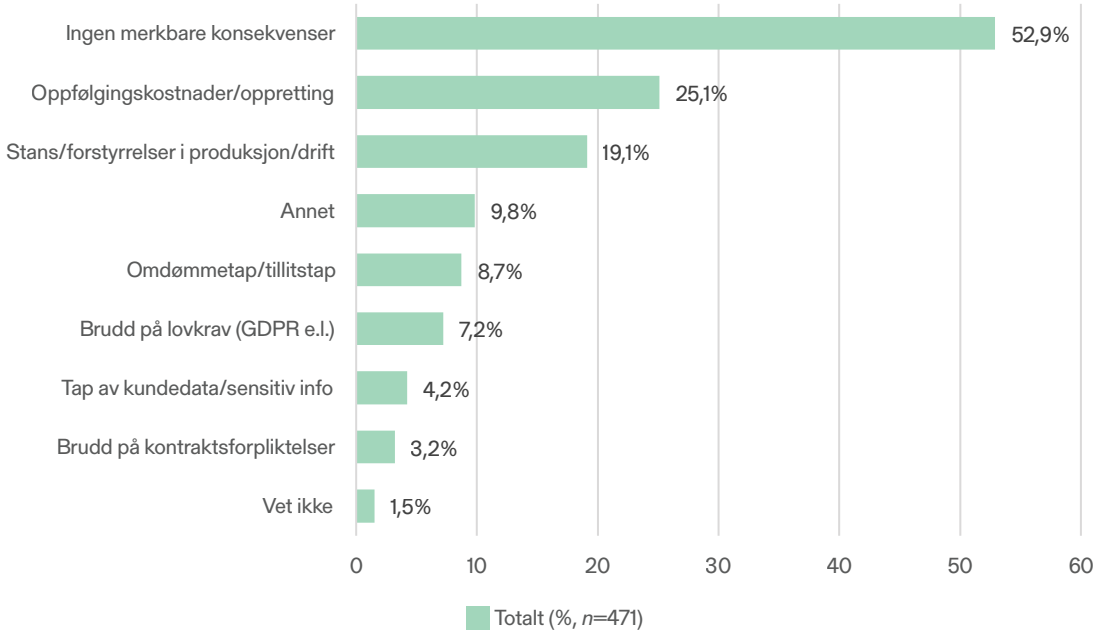
6

Konsekvenser og tap

6.1 Konsekvenser

53 prosent rapporterer ingen merkbare konsekvenser. Oppfølgingskostnader (25 %), driftsforstyrrelser (19 %) og omdømmetap (9 %) er de vanligste konsekvensene. Store virksomheter rapporterer konsekvenser oftere. 24 prosent opplevde driftsforstyrrelser mot 18 prosent blant de minste. For brudd på lovkrav er forskjellen firedobbel: 12 prosent mot 3 prosent.

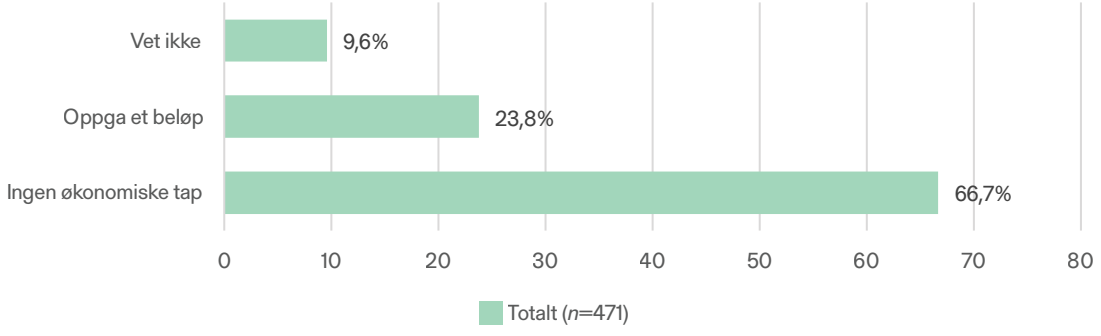
Figur 24. Konsekvenser



6.2 Økonomiske tap

Spørsmålet om økonomiske tap ble stilt til de 452 virksomhetene som rapporterte minst én digital sikkerhetshendelse de siste tolv månedene. Disse ble bedt om å oppgi det totale tapet knyttet til den mest alvorlige hendelsen, både direkte og indirekte. To av tre svarte at hendelsen ikke medførte økonomiske tap, mens ca. én av fire oppga et beløp. Resten svarte vet ikke.

Figur 25. Økonomisk tap blant virksomheter med hendelse



Tabell 6.1 viser fordelingen totalt og brutt ned på sektor og størrelse. Andelen som svarer ingen økonomiske tap er stabil på rundt 66 prosent på tvers av nedbrytningene. Offentlige virksomheter svarer noe oftere vet ikke (12 prosent mot 8,5 prosent i privat sektor), og oppgir samtidig sjeldnere et konkret beløp. De minste virksomhetene oppgir et beløp i 27,2 prosent av tilfellene, mot 21,6 prosent blant de største.

Tabell 6.1. Fordeling av svar på spørsmål om økonomiske tap. Base: virksomheter som rapporterte minst én digital sikkerhetshendelse siste tolv måneder.

	Totalt	Sektor		Antall ansatte		
Kategori	*n* = 471	Privat *n* = 329	Offentlig *n* = 142	5–19 *n* = 191	20–99 *n* = 183	100 + *n* = 97
Ingen økonomiske tap	66,7 %	66,3 %	67,6 %	65,4 %	67,8 %	67,0 %
Oppga et beløp	23,8 %	25,2 %	20,4 %	27,2 %	21,3 %	21,6 %
Vet ikke	9,6 %	8,5 %	12,0 %	7,3 %	10,9 %	11,3 %

Av de 112 som oppga et beløp inneholder ikke alle svar et tall som kan brukes i statistisk analyse. 19 respondenter skrev 0 i feltet for beløp, åtte svar var fritekst eller intervaller som ikke kan parses som ett enkelt tall (eksempler: «arbeidstimer», «usikker på beløp», «under 100 000», «700 000–1 000 000»). Disse 27 svarene er holdt utenfor distribusjonsanalysen. Distribusjonsstatistikken bygger derfor på de 85 respondentene som oppga et entydig positivt beløp.

Beløpene spenner fra 100 kroner til 5 millioner kroner. Halvparten av virksomhetene rapporterte tap på 25 000 kroner eller mindre. Tre virksomheter rapporterte tap på én million kroner eller mer, hvorav den høyeste enkeltverdien er 5 millioner kroner. Åtte virksomheter rapporterte tap på 500 000 kroner eller mer. Det store spennet trekker gjennomsnittet kraftig opp i forhold til medianen: gjennomsnittet på 165 000 kroner er nesten syv ganger medianen.

Tabell 6.2. Deskriptiv statistikk for de 85 virksomhetene som oppga et entydig positivt beløp. Beløp i hele kroner.

Statistikk	Verdi
Antall observasjoner	85
Median	25 000 kr
Gjennomsnitt	165 085 kr
Maksimum	5 000 000 kr
Sum av rapporterte tap	14 032 200 kr

Tap under 10 000 kroner og tap mellom 10 000 og 100 000 kroner utgjør hver ca. en tredjedel av observasjonene. De resterende 27 prosent gjelder tap over 100 000 kroner. Fordelingen er nær symmetrisk i de to lavere kategoriene, mens tyngden av store tap ligger i privat sektor.

Privat sektor står for 65 av de 85 positive beløpene og for 12,8 millioner av de 14 millionene som er rapportert totalt. Median i privat sektor er 30 000 kroner, mot 17 500 kroner i offentlig sektor. Tap over 100 000 kroner forekommer hyppigere i privat sektor (36,9 prosent mot 25 prosent), mens tap mellom 10 000 og 100 000 kroner er overrepresentert i offentlig sektor.

Tallene representerer sannsynligvis et minimumsnivå. Spørsmålet ber om både direkte og indirekte tap, men i praksis vil mange virksomheter ikke ha system for å beregne indirekte kostnader som tapt arbeidstid, omdømmetap, kundeavgang eller styrkning av kontrollrutiner i etterkant. At 19 respondenter oppga 0 kroner og 45 svarte vet ikke, peker også i retning av at den reelle kostnaden er underestimert. Gapet mellom median (25 000 kroner) og gjennomsnitt (165 000 kroner) viser samtidig at konsekvensene av digitale sikkerhetshendelser er svært ujevnt fordelt: et lite mindretall står for det meste av det dokumenterte tapet.

7

Rapportering og mørketall

Rapporteringsatferden er kjernen i rapporten. Hendelser som ikke rapporteres forblir usynlige og gjør det umulig å dimensjonere tiltak korrekt.

7.1 Mørketallskjeden

Tallene i undersøkelsen avdekker en trinnvis filtreringsprosess der hendelser forsvinner fra statistikken:

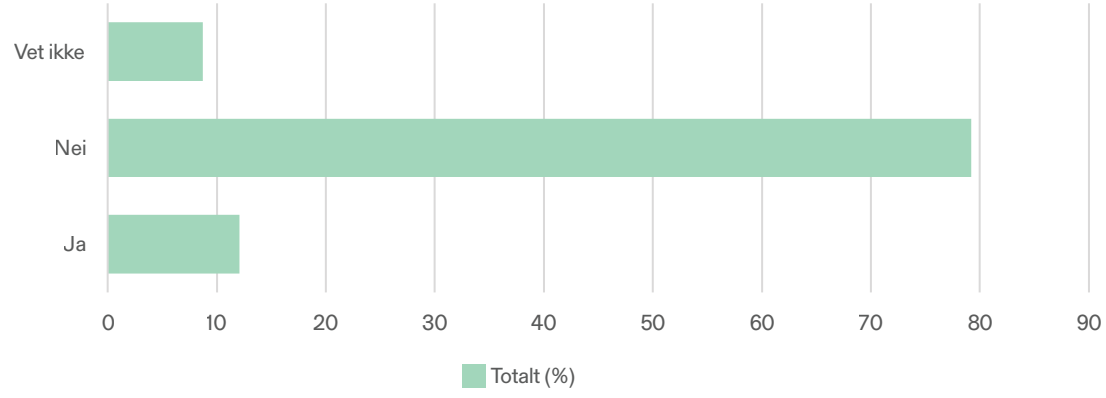
- **2 500** virksomheter ble spurt.
- **452** (18 %) opplevde minst én hendelse siste 12 måneder.
- **373** (79 % av de med hendelse) anmeldte ikke til politiet.
- **157** av disse begrunnet det med at hendelsen var «ubetydelig».

Kjeden undervurderer sannsynligvis det reelle omfanget. 3 til 6 prosent svarte «vet ikke» på om de var utsatt for ulike hendelsestyper. Det tilsvarer opptil 150 virksomheter som mangler innsyn i egen sikkerhetssituasjon. Når vi i tillegg vet at virksomheter med rammeverk oppdager langt flere hendelser enn de uten (kapittel 4.3), er det grunn til å anta at de 19 prosentene som rapporterer hendelser bare fanger opp en brøkdel av virkeligheten.

7.2 Anmeldelsesrate

Bare 12 prosent anmeldte hendelsen til politiet. 79 prosent lot være. 9 prosent vet ikke.

Figur 26. Anmeldelsesrate



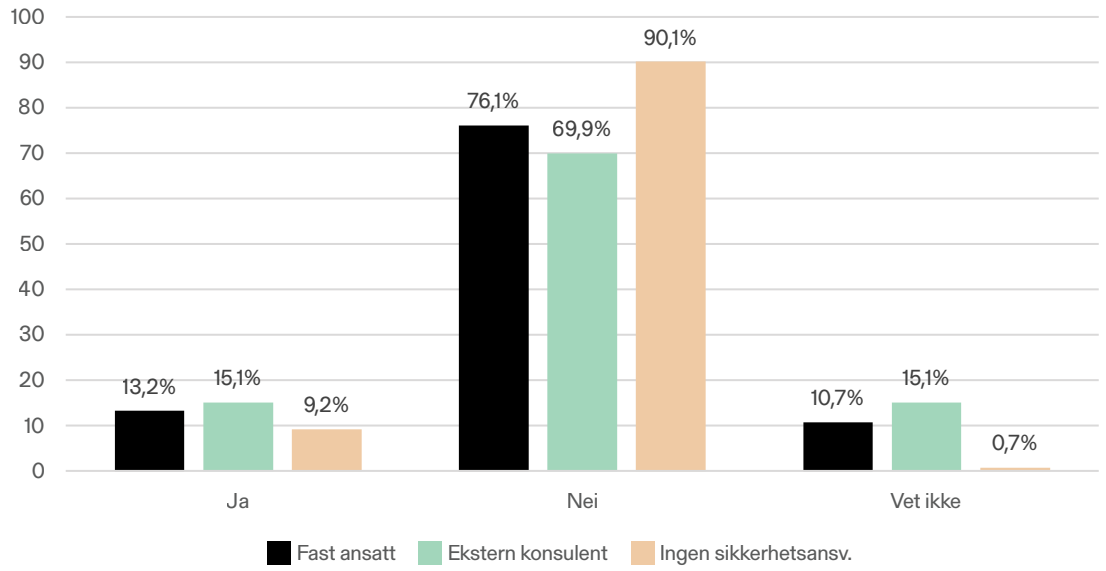
Anmeldelsesraten er praktisk talt lik uavhengig av om virksomheten har rammeverk (12 %, $n = 286$) eller ikke (13 %, $n = 138$). Formaliserte sikkerhetssystemer forbedrer altså deteksjon, men påvirker ikke rapporteringsatferden. Terskelen for anmeldelse ligger et annet sted enn terskelen for oppdagelse.

7.3 Sikkerhetsansvarlig og anmeldelsesrate

Undersøkelsen viser at rammeverk ikke påvirker anmeldelsesraten (12 % mot 13 %). Spørsmålet er om det samme gjelder for tilstedeværelse av sikkerhetsansvarlig. Dersom svaret er ja, styrkes mistanken om at rapporteringsbarrierene ikke er kapasitetsbaserte, men snarere kulturelle og tillitsbaserte.

Blant de 452 virksomhetene som opplevde en hendelse, varierer anmeldelsesraten noe etter type sikkerhetsansvarlig. Virksomheter med ekstern konsulent anmelder i størst grad (15 %). Virksomheter med fast ansatt sikkerhetsansvarlig ligger på 13 prosent. Virksomheter uten sikkerhetsansvarlig anmelder i minst grad (9 %). Forskjellene er ikke statistisk signifikante.

Figur 27. Anmeldelsesrate etter type sikkerhetsansvarlig

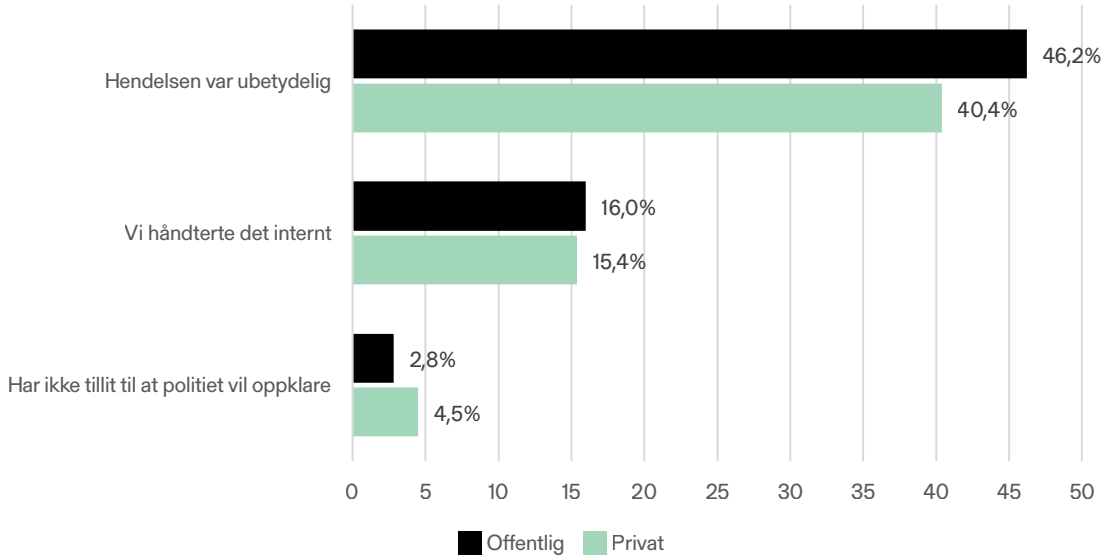


Resultatet speiler funnet for rammeverk: formell sikkerhetsorganisering øker evnen til å oppdage hendelser, men påvirker ikke viljen til å anmelde dem.

Begrunnelsene for ikke å anmelde er praktisk talt identiske på tvers av gruppene. Hendelsen var ubetydelig: 42 prosent blant de med sikkerhetsansvarlig, 43 prosent blant de uten. Intern håndtering: 17 mot 14 prosent.

Den eneste forskjellen av interesse er tilliten til politiet. 6 prosent av virksomhetene uten sikkerhetsansvarlig oppgir manglende tillit til politiet som hovedgrunn, mot 3 prosent blant de med. Tallene er små, men antyder at virksomheter uten formell sikkerhetskompetanse også har lavere tillit til det offentlige apparatet.

Figur 28. Årsaker til at hendelsen ikke ble anmeldt



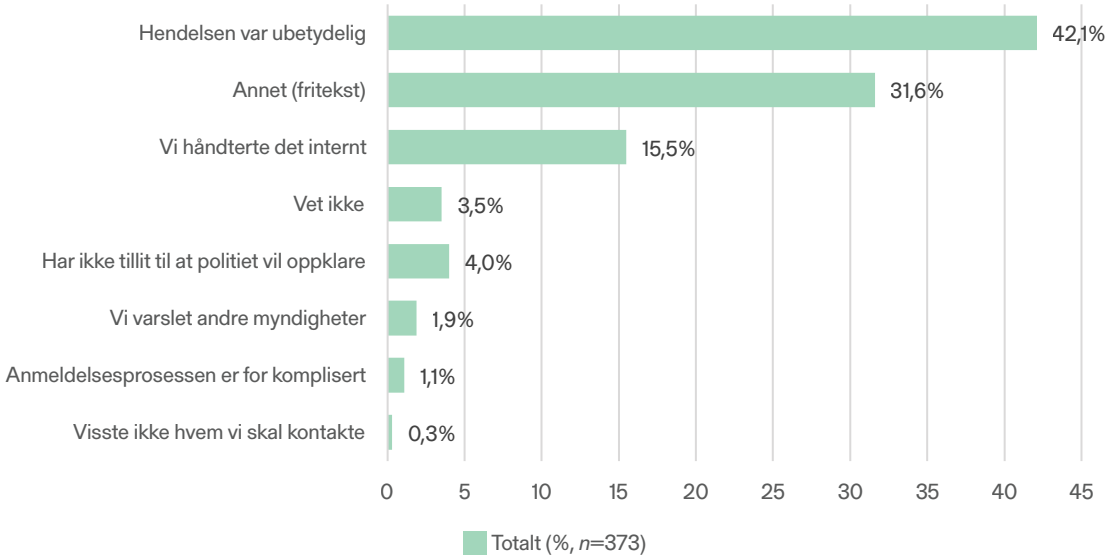
Anmeldelsesraten er lav uavhengig av om virksomheten har sikkerhetsansvarlig. Vi kan derfor konkludere med at formell sikkerhetsorganisering ikke øker anmeldelsesviljen. Barrierene må altså ligge et annet sted. Vurderingen av hendelsen som ubetydelig dominerer i begge grupper. Intern håndtering og manglende tillit til politiet forsterker mønsteret.

Funnet underbygger at tiltak for å øke anmeldelsesraten må rettes mot rapporteringskultur og tillit til rettssystemet, ikke mot økt sikkerhetskompetanse alene.

7.4 Årsaker til ikke-anmeldelse

Den vanligste begrunnelsen er at hendelsen var ubetydelig (42 %). 16 prosent håndterte internt. 4 prosent mangler tillit til politiets evne til oppklaring. 2 prosent varslet andre myndigheter.

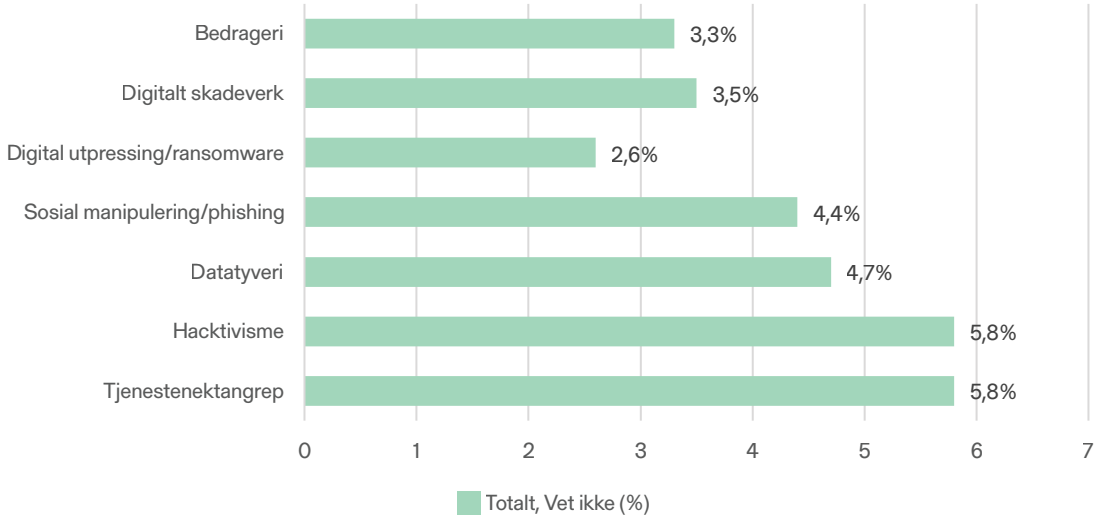
Figur 29. Hovedårsak til at hendelsen ikke ble anmeldt



Fritekstbesvarelsene (118 svar) forsterker bildet. Gjengangere: hendelsen ble stoppet før den fikk konsekvenser, IT-leverandøren anbefalte å ikke anmelde, «politiet har ikke kapasitet», «det blir uansett henlagt». Denne tillitskrisen overfor rettshåndhevelsen bidrar direkte til mørketallene.

Mørketallene forsterkes av flere parallelle mekanismer: virksomheter uten sikkerhets-monitorering oppdager ikke hendelser. Virksomheter som oppdager dem, vurderer dem som ubetydelige. Og virksomheter som anerkjenner alvorligheten, velger likevel å håndtere internt. I hvert ledd faller hendelser ut av statistikken.

Figur 30. Andel som svarte «Vet ikke» på om de var utsatt for ulike hendelsestyper



Figuren viser andelen som svarte «vet ikke» på om de var utsatt for ulike hendelsestyper. Mellom 3 og 6 prosent mangler oversikt over egen eksponering, avhengig av hendelsestype. Disse virksomhetene representerer et ytterligere lag av mørketall: hendelser som verken er oppdaget eller avvist, men som faller utenfor virksomhetens synsfelt.

7.5 Kripos/NC3: Kommentar - Hvorfor virksomheter bør anmelde cyberrettet kriminalitet til politiet

For politiet er det viktig at virksomheter anmelder cyberrettet kriminalitet. Anmeldelser gir politiet informasjon som kan bidra til å avdekke og forebygge ny datakriminalitet, mulighet til å se saker i sammenheng og bidra til en helhetlig nasjonal situasjonsforståelse.

Gjennom etterforskning kan politiet identifisere trusselaktører, metoder, sårbarheter og infrastruktur som brukes i angrep. Dette gjør det mulig å varsle andre potensielle fornærmede og avverge fremtidige hendelser både i Norge og utlandet, samt gi råd om tiltak som kan redusere skadeomfanget. Informasjon fra enkeltsaker kan også bidra til større nasjonale og internasjonale etterforskninger mot aktører som opererer mot norske virksomheter.

Anmeldelser er også viktige for politiets evne til å produsere etterretning og gi beslutningsstøtte til både myndigheter og rammede virksomheter. I enkelte saker kan politiets etterforskning støtte virksomhetens egen hendelseshåndtering, blant annet gjennom attribusjon, avdekking av hvordan kompromitteringen har skjedd og vurderinger knyttet til videre risiko. Politiets bruk av tvangsmidler kan i enkelte tilfeller være avgjørende for å avdekke om data er på avveie, hvordan aktører har fått tilgang til systemer og hvilke motiver som kan ligge bak handlingene. Politiet har også erfaring med håndtering av trusselaktører og kan gi råd i situasjoner som involverer utpressing og løsepengekrav.

Samtidig er tilfanget av anmeldelser avgjørende for at politiet skal kunne videreutvikle kompetanse, metoder og beredskap innen bekjempelse av datakriminalitet. Selv saker som isolert sett vurderes som mindre alvorlige kan bidra til å avdekke større mønstre og gi viktig kunnskap som styrker den samlede innsatsen mot datakriminalitet.

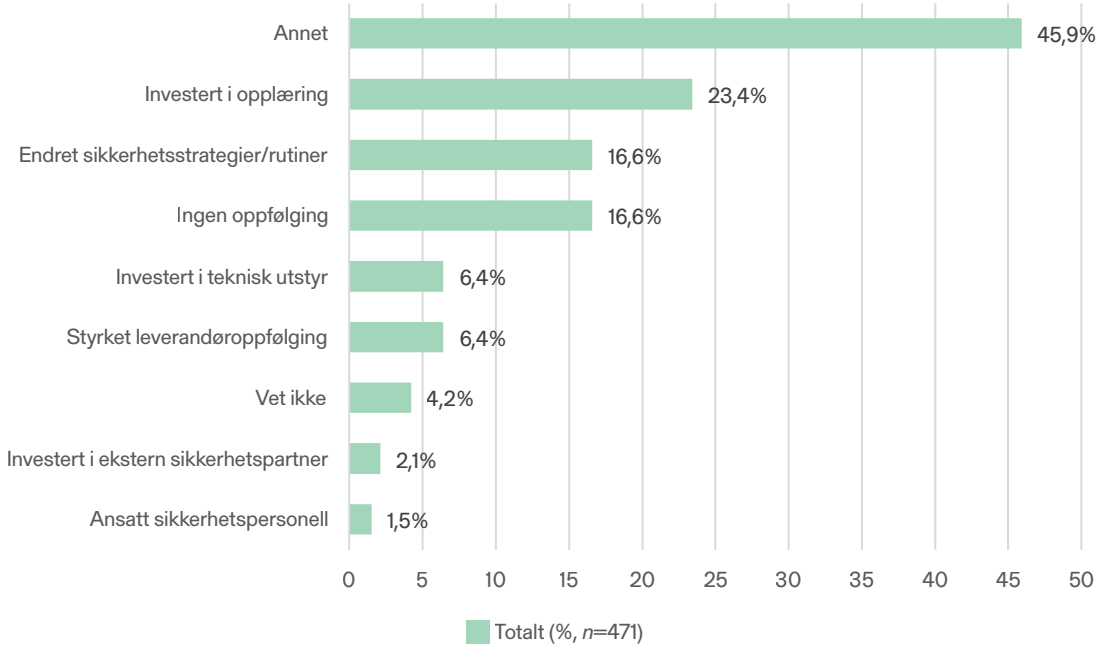
8

Oppfølging etter hendelse

23 prosent investerte i opplæring i digital sikkerhet. 17 prosent endret sikkerhetsstrategier og rutiner. 6 prosent investerte i teknisk utstyr, 6 prosent styrket leverandøroppfølgingen.

Like mange – 17 prosent – fulgte ikke opp hendelsen i det hele tatt. Denne andelen er nesten dobbelt så høy blant de minste virksomhetene (24 %) som blant mellomstore (10 %) og store (12 %). Ressursbegrensninger er en sannsynlig forklaring.

Figur 31. Oppfølging etter hendelse



Fritekstbesvarelsene (216 svar) avdekker at den vanligste oppfølgingen er uformell: «vi har snakket om det på personalmøte», «vi har bedt ansatte være mer oppmerksomme». Strukturelle tiltak som nye rutiner, tekniske oppgraderinger og sikkerhetspartnere forekommer sjeldnere. Mønsteret tyder på at oppfølgingen for mange handler om bevisstgjøring heller enn systemendring. Bevisstgjøring er nødvendig, men utilstrekkelig uten endringer i rutiner, verktøy og ansvar.

8.1 Betydningen av IT-driftsmodell ved oppfølging av hendelser

Driftsmodellen påvirker hvordan virksomheter følger opp sikkerhetshendelser. Blant de 452 virksomhetene som opplevde minst én hendelse, varierer andelen uten oppfølging betydelig etter hvordan IT-funksjonen er organisert.

24 prosent av virksomhetene med helt intern drift fulgte ikke opp hendelsen. Blant virksomheter med helt ekstern drift var andelen 21 prosent. Hybridvirksomhetene skiller seg ut: bare 12 prosent lot være å følge opp. Forskjellene er statistisk signifikante.

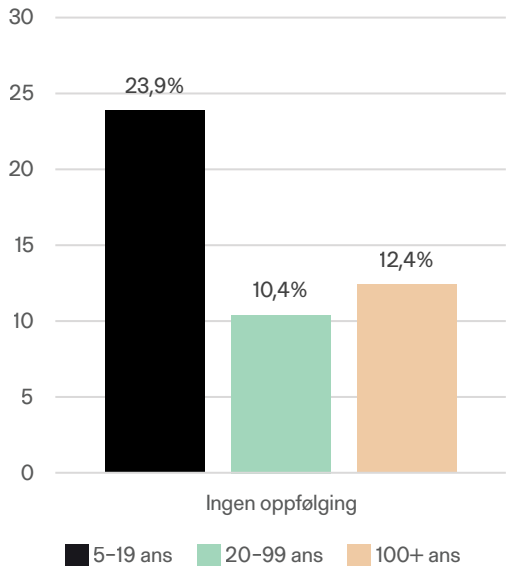
Både helt ekstern og helt intern drift har dobbelt så høy andel uten oppfølging som hybridmodellen. Forskjellen mellom ekstern og intern er ikke signifikant. Det er hybridmodellen som skiller seg positivt ut, ikke ekstern drift som skiller seg negativt ut.

En mulig forklaring er at hybridvirksomheter kombinerer intern kompetanse til å forstå og prioritere hendelser med ekstern kapasitet til å gjennomføre tiltak. Virksomheter med ren ekstern drift mangler kanskje eierskap til hendelsene. Virksomheter med ren intern drift mangler kanskje spesialistkompetanse og kapasitet.

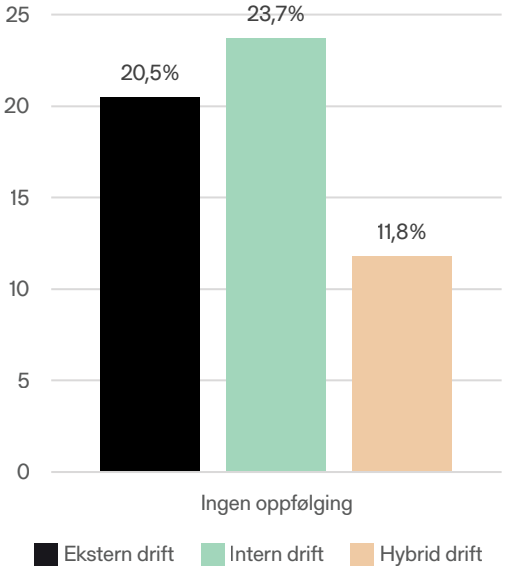
Hvilke tiltak velges?

Oppfølgingstiltakene varierer også med driftsmodell. Opplæring er det vanligste tiltaket i alle grupper, men hybridvirksomhetene ligger høyest (26 %) mot ekstern (20 %) og intern (24 %).

Figur 32. Ingen oppfølging etter hendelse

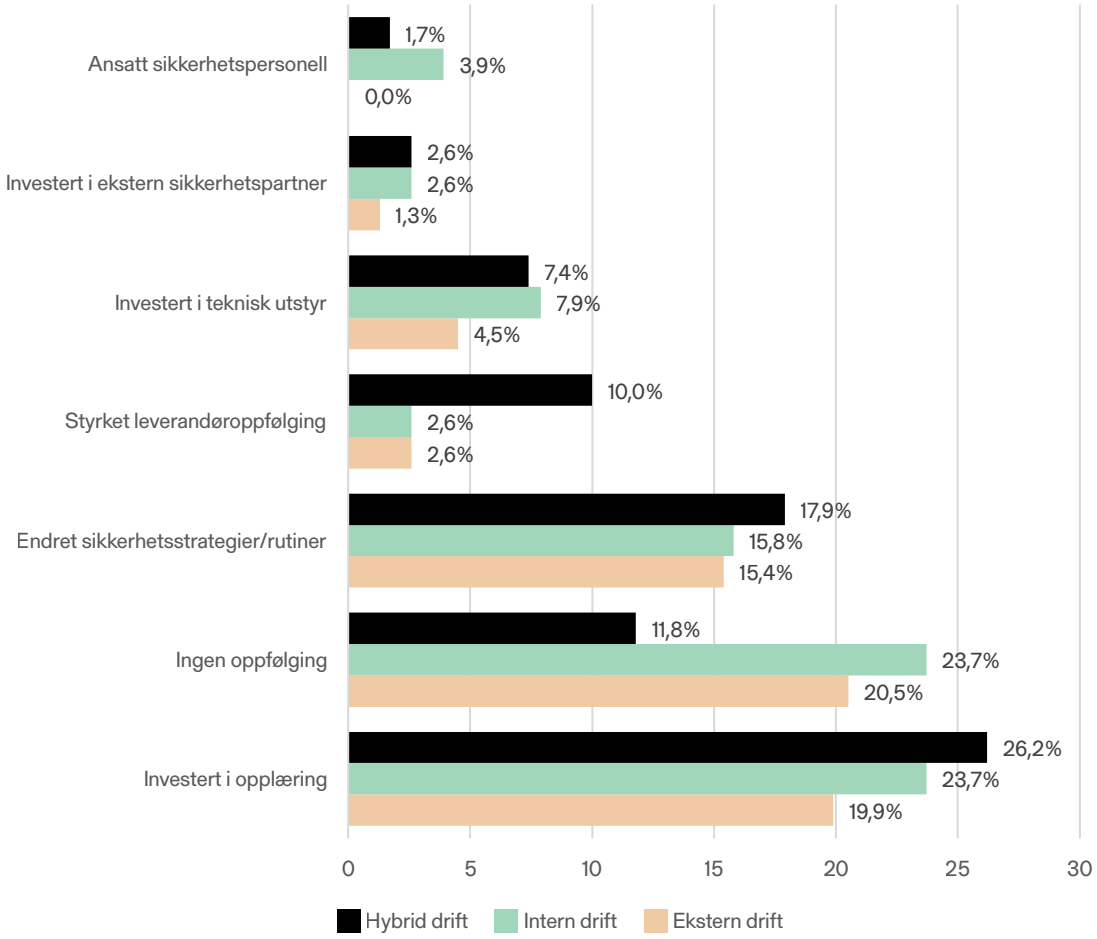


Figur 33. Ingen oppfølging etter hendelse, etter IT driftsmodell



10 prosent av hybridvirksomhetene styrket leverandøroppfølgingen etter hendelsen. Bare 3 prosent av ekstern- og intern-gruppene gjorde det samme. Hybridvirksomhetene er de eneste som i praksis stiller krav til leverandørene sine etter en hendelse.

Figur 34. Oppfølgingstiltak etter IT-driftsmodell



Endring av strategier og rutiner ligger jevnt på tvers av gruppene (15–18 %). Investering i teknisk utstyr er noe vanligere blant intern (8 %) og hybrid (7 %) enn ekstern (5 %). Ingen virksomheter med helt ekstern drift ansatte flere sikkerhetsfolk etter hendelsen.

Undersøkelsen bekrefter at både ekstern og intern drift gir dårligere oppfølging enn hybrid. Det avgjørende ser derfor ut til å være om virksomheten har en hybridmodell der intern kompetanse og ekstern kapasitet virker sammen.

8.2 Anmeldelse og strukturell oppfølging

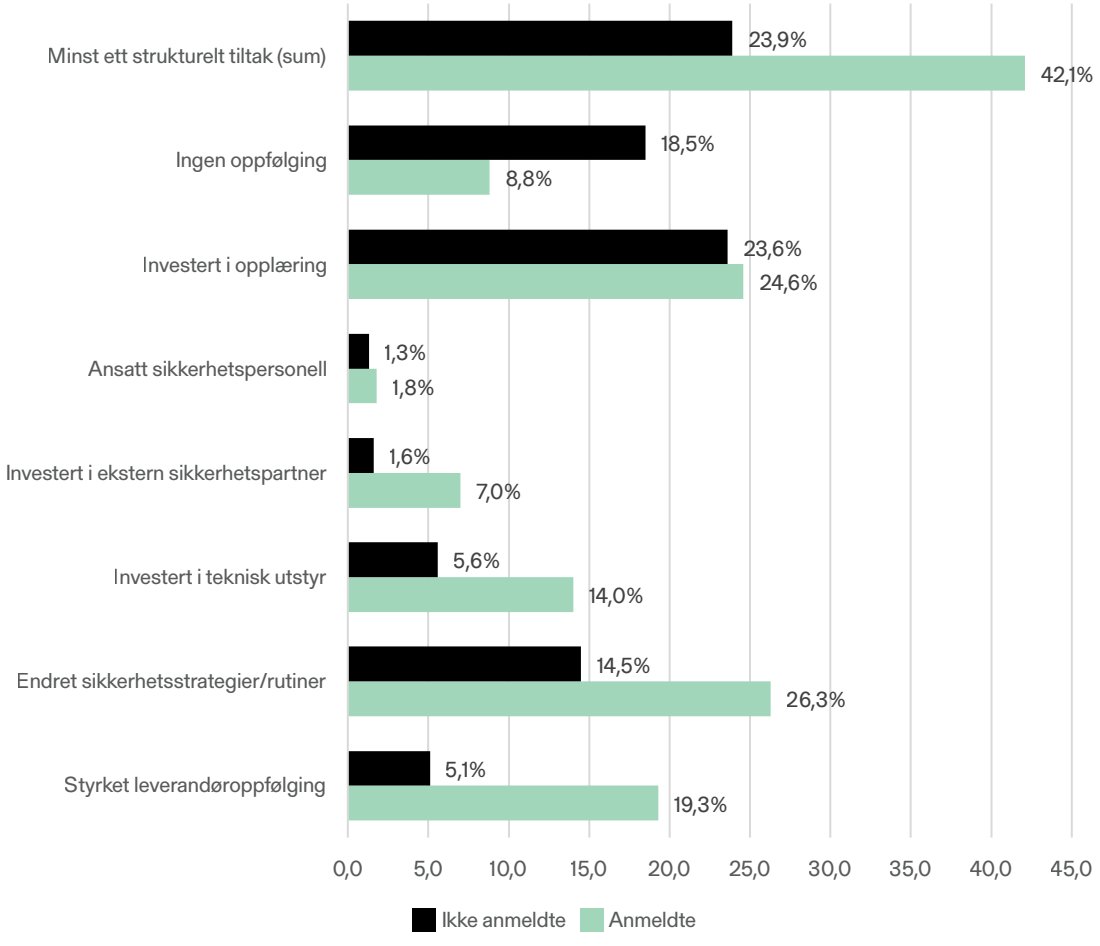
Rapporten behandler anmeldelse (kapittel 7) og oppfølging (kapittel 8) som separate tema. Spørsmålet er om de henger sammen: er anmeldelse et signal om generell seriøsitet i sikkerhetsarbeidet, ikke bare en isolert handling?

Blant de 57 virksomhetene som anmeldte hendelsen skiller oppfølgingen seg klart fra de 373 som lot være. Størst forskjell viser leverandøroppfølgingen: 19 prosent av de som anmeldte styrket leverandøroppfølgingen, mot 5 prosent av de som ikke anmeldte. Forskjellen er signifikant.

Endring av strategier og rutiner følger: 26 prosent mot 15 prosent. Investering i teknisk utstyr: 14 prosent mot 6 prosent. Ekstern sikkerhetspartner: 7 prosent mot 2 prosent.

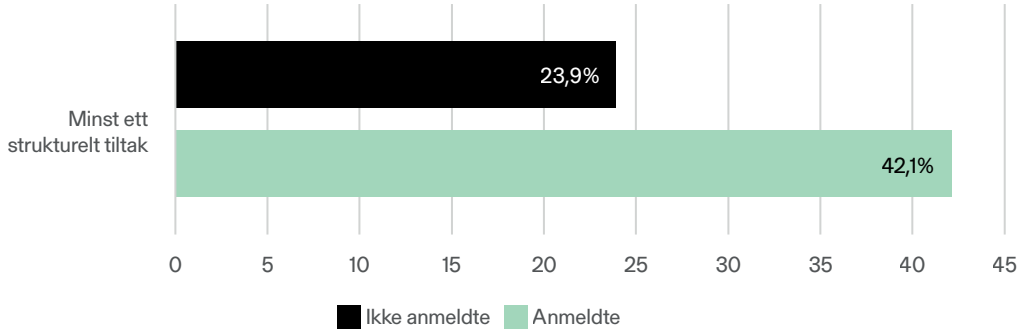
Opplæring er det eneste tiltaket uten forskjell. 25 prosent i begge grupper investerte i opplæring. Bevisstgjøring og kompetanse er tilsynelatende det tiltaket som iverksettes uavhengig av hvor seriøst hendelsen håndteres forøvrig.

Figur 35. Oppfølgingstiltak etter anmeldelse



Når man slår sammen alle strukturelle tiltak (nye rutiner, teknisk utstyr, leverandøroppfølging, ekstern partner og nyansettelser), har 42 prosent av de som anmeldte gjennomført minst ett strukturelt tiltak, mot 24 prosent blant de som ikke anmeldte. I snitt gjennomførte de som anmeldte 0,68 strukturelle tiltak per virksomhet, mot 0,28 blant de som ikke anmeldte.

Figur 36. Andel med minst ett strukturelt oppfølgingstiltak, etter anmeldelse



Andelen uten oppfølging peker i samme retning: 9 prosent blant de som anmeldte, mot 19 prosent blant de som ikke anmeldte. Forskjellen er ikke signifikant, men retningen er konsistent med øvrige funn.

Hva forklarer sammenhengen?

Sammenhengen mellom anmeldelse og oppfølging kan tolkes på to måter. Den første er at anmeldelse og oppfølging begge reflekterer en underliggende seriøsitet i sikkerhetsarbeidet. Virksomheter som tar hendelsen alvorlig nok til å anmelde, tar den også alvorlig nok til å endre rutiner og investere i sikkerhet.

Den andre er at anmeldelsesprosessen i seg selv utløser oppfølging. Kontakten med politiet kan øke bevisstheten om sårbarheter, føre til at hendelsen dokumenteres grundigere, og skape forventninger internt om at noe må endres.

Datagrunnlaget kan ikke skille mellom disse forklaringene. Virksomheter som anmeldte har noe høyere andel med sikkerhetsansvarlig (74 % mot 61 %), noe som antyder at kapasitet spiller en rolle. Men også blant virksomheter med sikkerhetsansvarlig er det bare et mindretall som anmelder, så sikkerhetsansvarlig alene forklarer ikke sammenhengen.

Dette funnet styrker imidlertid argumentet for å øke anmeldelsesraten som et systemtiltak, ikke bare et statistikktiltak. Anmeldelse ser ut til å være del av en bredere respons der virksomheten aktivt lærer av hendelsen. Alternativt kan anmeldelsesprosessen i seg selv bidra til å utløse oppfølging. Uansett årsaksretning gir koblingen mellom anmeldelse og strukturell oppfølging et konkret argument for tiltak som senker terskelen for slike anmeldelser.

8.3 Coop: Analyse

Hvorfor cyber, fysisk sikkerhet og svindel må håndteres som én samlet risiko.

Handelsbransjen er blant de mest digitaliserte sektorene i Norge. Betalinger, logistikk, kundedialog og leverandørkjeder er tett integrert gjennom teknologi. Dette gir effektiv drift og gode kundeopplevelser, men også en stor og sammensatt angrepsflate.

Samtidig ser vi at trusselbildet endrer seg raskt. Angrep holder seg ikke lenger innenfor ett domene. De beveger seg mellom mennesker, teknologi og fysiske prosesser. Et digitalt angrep kan på få minutter få økonomiske og operative konsekvenser i den fysiske verden.

I handelsbransjen ser vi dette tydelig. Kompromitterte kontoer eller betalingskort brukes til kjøp av digitale betalingskort og andre verdibærere. Verdiene flyttes raskt videre gjennom flere ledd. Når dette først har skjedd, er muligheten for å stoppe eller tilbakeføre midlene ofte svært begrenset. Tid blir dermed en kritisk faktor.

Denne utviklingen viser hvorfor cyber, fysisk sikkerhet, svindelhåndtering og beredskap ikke lenger kan behandles som separate fagområder. Angripere utnytter overgangene mellom systemer, mennesker og prosesser. Da må også sikkerhetsarbeidet henge sammen.

Vi ser også hvordan kunstig intelligens senker terskelen for troverdige phishingforsøk, falske innloggingssider og målrettet manipulering. Angrepene fremstår mer profesjonelle og mer overbevisende enn tidligere. Dette utfordrer tradisjonelle sikkerhetstiltak. Brukerbevissthet alene er ikke nok. Virksomheter må kombinere tekniske, organisatoriske og operative tiltak for å redusere risiko og oppdage hendelser tidlig.

Samtidig har handelsbransjen over tid bygget solide mekanismer for å håndtere svindel og sikre betalinger. Samarbeidet med finanssektoren og mellom aktører i egen bransje er godt. Erfaringer deles, og mange virksomheter har høy modenhet innen operativ hendelseshåndtering.

Likevel ser vi et tydelig behov for raskere og mer relevant informasjonsdeling. Når kriminelle opererer hurtig og koordinert, blir tidlig varsling avgjørende. Deling av indikatorer, modus og hendelsesforløp kan bidra til å stoppe eller begrense skade før flere virksomheter rammes.

Her møter vi samtidig viktige rammebetingelser. Informasjonsdeling må skje innenfor gjeldende regelverk, særlig knyttet til personvern og behandling av sensitiv informasjon. Samtidig må vi videreutvikle strukturer som gjør det mulig å dele nødvendig informasjon raskt, trygt og kontrollert når situasjonen krever det.

Internt i virksomheter er det også behov for en mer helhetlig tilnærming. Cybermiljøer, fysisk sikkerhet, svindelhåndtering og beredskap sitter ofte på hver sin del av virkeligheten. Når disse miljøene ikke kobles sammen, mister man viktige sammenhenger. Når de derimot arbeider tettere sammen, øker evnen til å oppdage mønstre, forstå trusselbildet og håndtere hendelser mer effektivt.

Dette handler ikke bare om virksomhetsrisiko. Handelsbransjen er en sentral del av samfunnets daglige infrastruktur. Evnen til å opprettholde stabile leveranser, trygge betalinger og tillit til digitale tjenester har betydning langt utover den enkelte virksomhet.

Trusselbildet fremover vil bli mer sammensatt, ikke mindre. Angripere utnytter helheten.

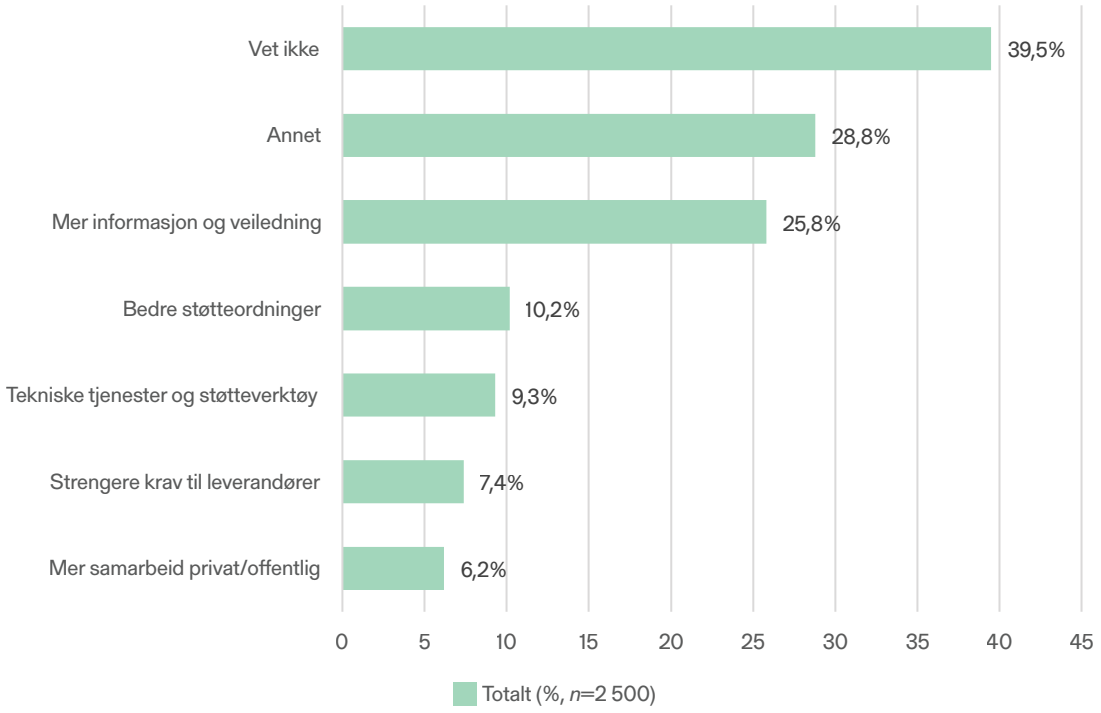
Da må også responsen være helhetlig: Når truslene møtes, må vi møte dem samlet.

9

Myndighetenes rolle

40 prosent svarte «vet ikke» på hva myndighetene bør gjøre. Det er den høyeste «vet ikke»-andelen i undersøkelsen. Blant de som svarte, dominerer ønsket om informasjon og veiledning (26 %). Bedre støtteordninger (10 %), tekniske tjenester (9 %) og strengere krav til leverandører (7 %) følger.

Figur 37. Hva bør myndighetene gjøre for SMB-er?



Fritekstanalysen av 721 svar utdyper behovene. 19 prosent etterlyser informasjon og kunnskap, altså konkrete råd, kampanjer og veiledningsmateriell tilpasset små virksomheter. 9 prosent ønsker strengere lovgivning. 6 prosent vil ha bedre politiinnsats mot digital kriminalitet. 6 prosent ber om direkte økonomisk støtte.

Undersøkelsen viser at virksomhetene etterspør praktisk hjelp. Med digitalsikkerhetsloven som trådte i kraft 1. oktober 2025 og NIS2-implementeringen som ventes, skjerpes kravene ytterligere. Utfordringen for myndighetene er å kombinere regulering med støtte, slik at også små virksomheter uten dedikerte sikkerhetsressurser kan etterleve kravene. NSMs grunnprinsipper for IKT-sikkerhet er et konkret tilbud, men undersøkelsen viser at bare 10 prosent av de med rammeverk oppgir dette som sin standard.

9.1 Abelia: Analyse

Stadig flere norske virksomheter og institusjoner er blitt utsatt eller forsøkt utsatt for angrep fra fiendtlige aktører de siste årene. Kripos regner det som sannsynlig at angrep på operasjonell teknologi med følgekonsekvenser i forsyningskjeder eller kritisk infrastruktur vil inntreffe, og NSM har registrert cyberhendelser mot så å si alle samfunnssektorer.

I et stadig mer digitalisert samfunn er cybersikkerhet blitt en forutsetning for nasjonal sikkerhet, økonomisk stabilitet og tillit mellom mennesker, virksomheter og myndigheter.

Abelia mener derfor at:

- Norge bør aktivt og strategisk søke samarbeid og harmonisering med EU på digital sikkerhet, og forsterke sikkerhetssamarbeidet i Norden.
- Norge må forsterke anvendt forskning innen cybersikkerhet og trening av relevante selskaper og fagmiljøer i mitigering og håndtering av cyberangrep.
- Det er behov for økt satsing på kompetanse innen sikker IT, spesielt innen AI og cybersikkerhet
- Informasjonsdeling mellom tilsynsmyndigheter og andre offentlige aktører må styrkes, slik at virksomheter kan forholde seg til et sentralt varslingspunkt for sikkerhetshendelser
- Det bør etableres en felles informasjonskanal for digital sikkerhet til bedrifter og innbyggere etter dansk modell.
- NSMs ulike roller og funksjoner bør utredes med formål å skape et tydeligere skille mellom de ulike rollene, og et tydeligere skille mellom hva som er det offentliges ansvar og hvilke funksjoner som kan overlates markedet.
- Norge bør opprette et nasjonalt langsiktig investeringsprogram rettet mot cybersikkerhet.

10

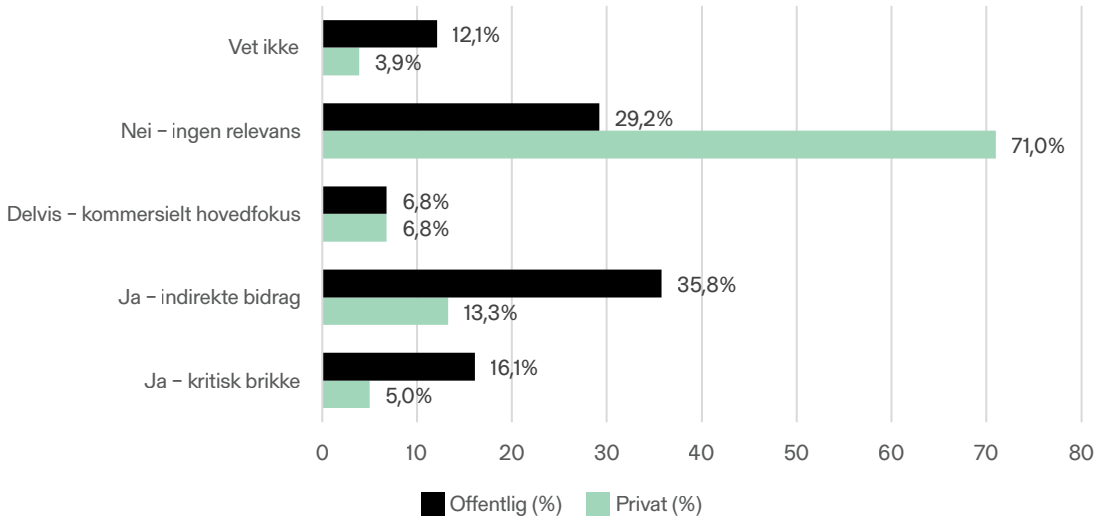
Nasjonal beredskap og samarbeid

10.1 Rolle i nasjonal beredskap

58 prosent mener virksomheten ikke har relevans for nasjonal beredskap. 20 prosent anser seg som indirekte bidragsytere, 8 prosent som en kritisk brikke. 7 prosent svarer «delvis».

Sektorforskjellen er markant. 71 prosent i privat sektor avviser beredskapsrelevans, mot 29 prosent i offentlig. 16 prosent av offentlige virksomheter anser seg som en kritisk brikke, mot 5 prosent i privat sektor.

Figur 38. Rolle i nasjonal beredskap

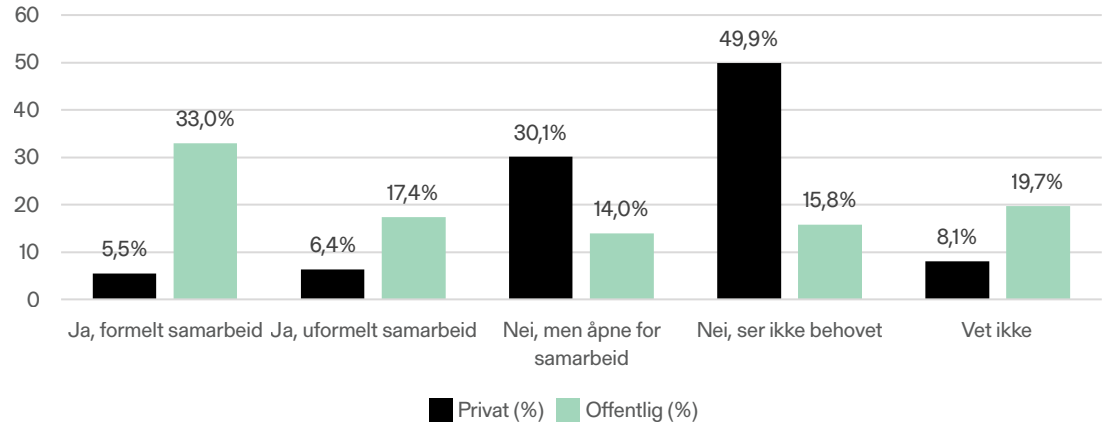


Kontrasten til NSMs budskap er påfallende. *Risiko 2026* understreker at digital avhengighet, komplekse leverandørkjeder og mangelfull sikkerhetsstyring øker risikoen for alvorlige konsekvenser. NSM peker på at trusselaktører som får innpass i leverandørkjeder i en tidlig fase kan utgjøre en sårbarhet også på lengre sikt. Når 71 prosent av privat sektor avviser enhver beredskapsrelevans, mangler denne forståelsen.

10.2 Samarbeid med myndigheter

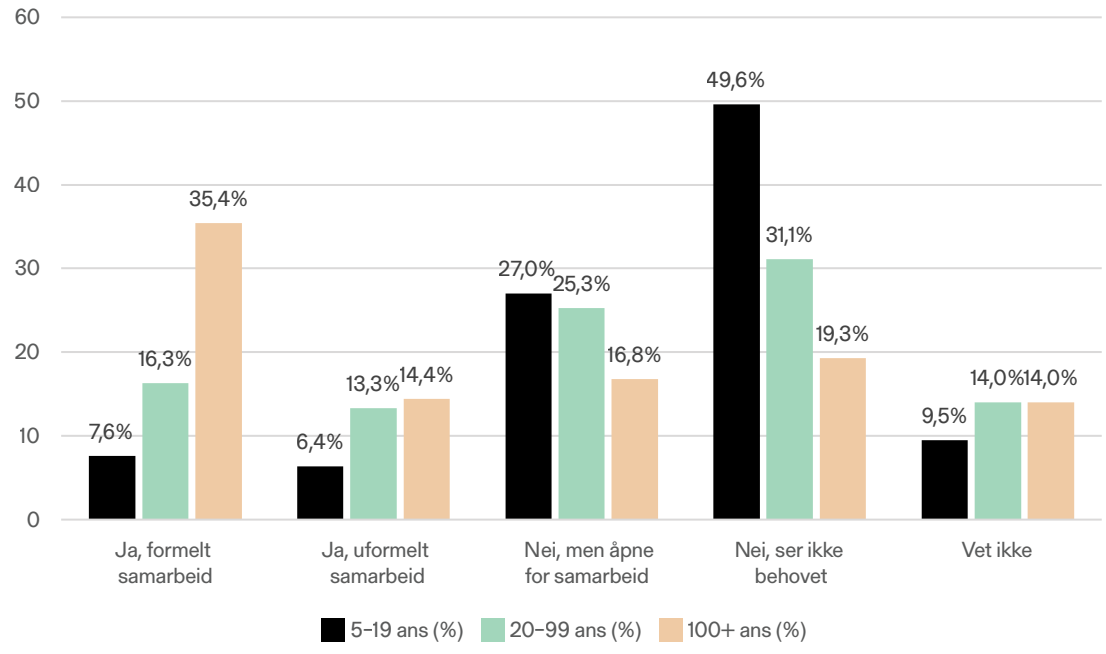
14 prosent har formelt samarbeid med myndigheter om sikkerhet, 10 prosent uformelt. 25 prosent er åpne for samarbeid. 40 prosent ser ikke behovet. Sektorforskjellen dominerer: 33 prosent av offentlige virksomheter har formelt samarbeid, mot 6 prosent i privat sektor. Halvparten av private virksomheter ser ikke behovet.

Figur 39. Samarbeid med myndigheter etter sektor



Størrelse forsterker mønsteret. 35 prosent av virksomheter med over 100 ansatte har formelt samarbeid, mot 8 prosent blant de minste.

Figur 40. Samarbeid med myndigheter etter størrelse



Funnene avdekker et dobbelt gap. Små, private virksomheter, som utgjør flertallet av norsk næringsliv, anser seg verken som beredskapsrelevante eller interessert i myndighetssamarbeid. Samtidig er det nettopp disse virksomhetene som kan utgjøre sårbare ledd i kritiske leverandørkjeder. Å lukke gapet krever målrettet kommunikasjon om hva beredskapsrelevans faktisk betyr, og hvorfor også en liten underleverandør spiller en rolle.

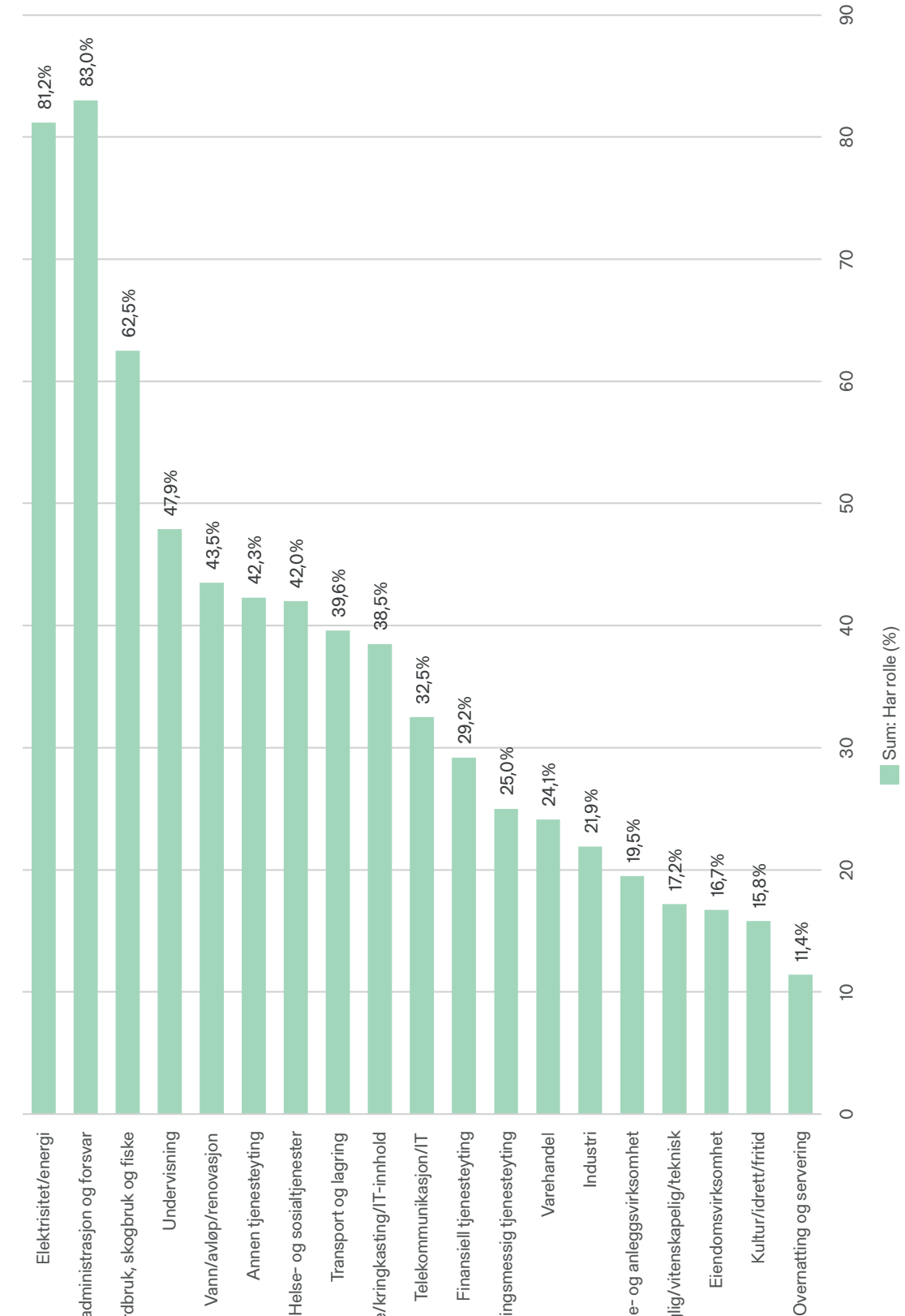
10.3 Bransjetilhørighet og synet på rollen i totalforsvaret

Vi har sett nærmere på hvorvidt bransjetilhørighet påvirker virksomhetenes oppfatning om sin rolle i totalforsvaret

Variasjonen er markant. Offentlig administrasjon og forsvar skiller seg kraftig ut: 79 prosent oppgir en rolle i nasjonal beredskap. Til sammenligning svarer bare 7 prosent det samme i overnattings- og serveringsbransjen. Andre bransjer med relativt høy beredskapsbevissthet er jordbruk/skogbruk/fiske (44 prosent), undervisning (39 prosent) og helse- og sosialtjenester (38 prosent).

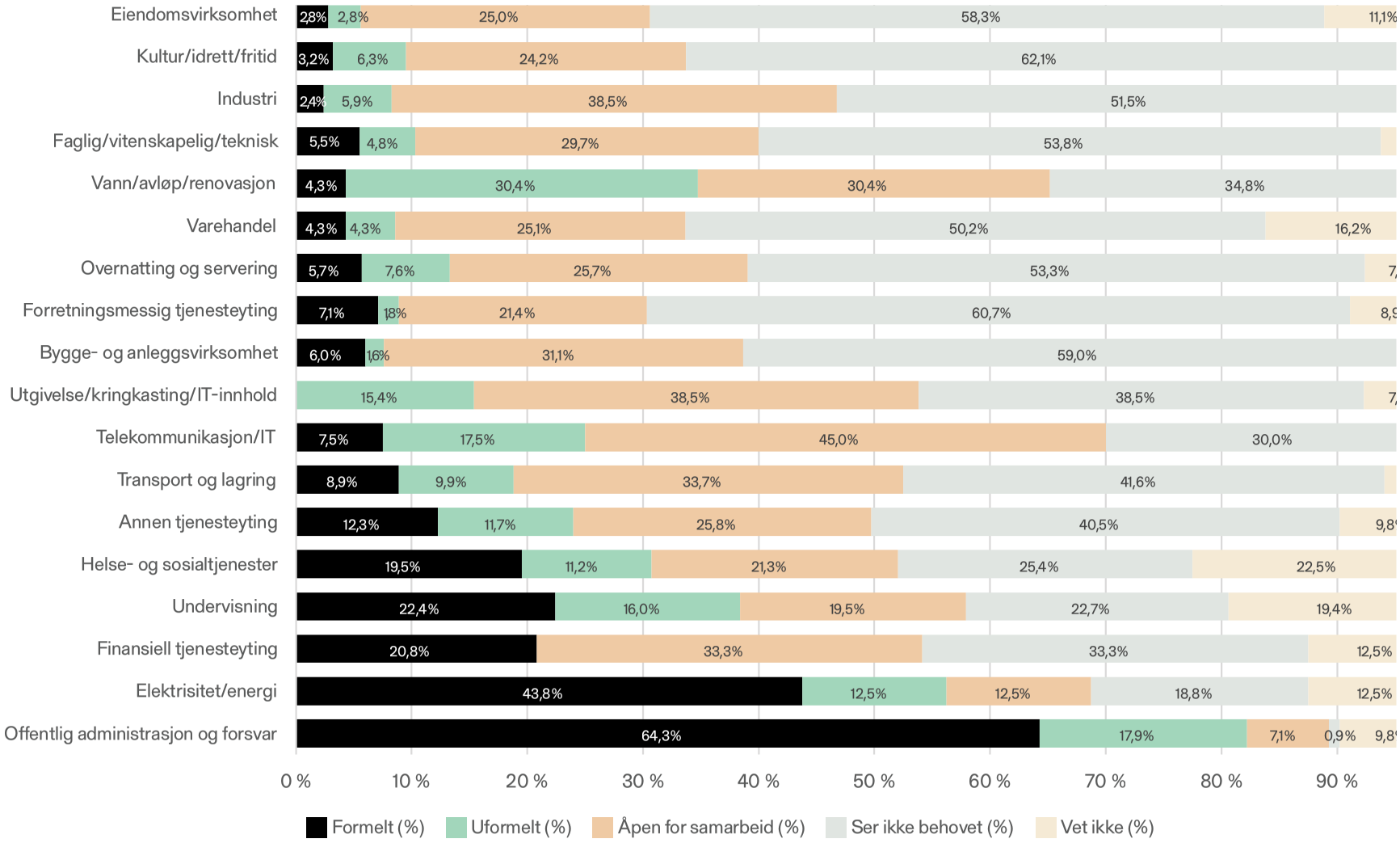
På spørsmålet om myndighetssamarbeid ser vi også her at offentlig administrasjon dominerer, der 64 prosent har formelt samarbeid. Undervisning (22 prosent) og helse- og sosialtjenester (20 prosent) følger, men med stor avstand. I bygge- og anleggsvirksomhet og eiendom er andelen med formelt samarbeid under 6 prosent.

Et viktig funn er kategorien «Nei, men vi er åpne for det». Flere bransjer som i dag har lite samarbeid, uttrykker villighet. Industri har lav formell samarbeidsandel (2 prosent), men hele 39 prosent er åpne for det. Tilsvarende gjelder transport og lagring (9 prosent formelt, 34 prosent åpne) og telekommunikasjon/IT (8 prosent formelt, 45 prosent åpne).



Figur 41. Virksomheten som en del av totalforsvaret

Figur 42. Alle svaralternativer for myndighetssamarbeid, per bransje



10.4 DNV Cyber: Analyse

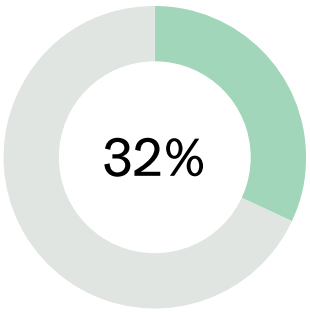
DNV Cyber leverer tjenester innen cybersikkerhet og støtter virksomheter i å redusere og håndtere digitale trusler. Arbeidet omfatter risikovurdering, regelverksrådgivning, integrering av sikkerhet i mål og styring samt overvåking, deteksjon og hendelseshåndtering. DNV Cyber har et globalt fagmiljø med mer enn 500 eksperter og over 30 års erfaring innen IT og OTsikkerhet.

Cybersikkerhet er en del av DNVs langsiktige strategi, og konsernet investerer årlig om lag seks prosent av omsetningen i forskning og utvikling. I 2026 etableres en forskningsenhet for cybertrusler og digital sårbarhet, som skal styrke kunnskapen om hvordan hendelser oppstår, gir sektorovergripende konsekvenser og hvordan læring faktisk skjer. Mørketallsundersøkelsen inngår i dette arbeidet.

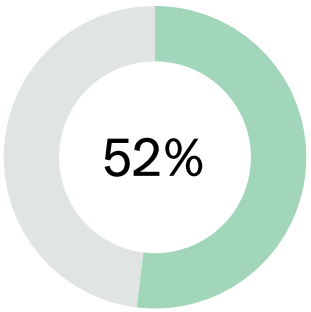
Mørketallsundersøkelsen 2026 viser at mange digitale sikkerhetshendelser ikke fanges opp gjennom formelle prosesser. For nasjonal beredskap svekker dette situasjonsforståelsen: hendelser forblir uoppdaget, vurderes som lite alvorlige eller rapporteres ikke, og avviket mellom faktiske hendelser og statistikk øker. Virksomheter som anmelder hendelser følger oftere opp med varige forbedringer: 42 prosent gjennomførte minst ett strukturelt tiltak, mot 24 prosent blant dem som ikke anmeldte, og gjennomsnittlig antall tiltak var mer enn dobbelt så høyt. Mørketall betyr derfor både mindre oversikt og tapte læringsmuligheter.

Funnene må ses i lys av virksomheters rolleforståelse i nasjonal cyberberedskap, særlig der de leverer eller understøtter kritiske samfunnsfunksjoner. DNV Cybers nasjonale undersøkelse *How Cyber Resilient is Norway?* (2026) viser at over halvparten av ledere i samfunnskritiske sektorer i liten eller noen grad oppfatter cybersikkerhet i kritisk infrastruktur som et eget ansvar, og én av tre er usikre på om egen virksomhet i det hele tatt er del av kritisk infrastruktur. Uklarhet om rolle og tilhørighet svekker ansvarslinjer og samordning, og kan bidra til lav rapportering og begrenset erfaringsdeling.

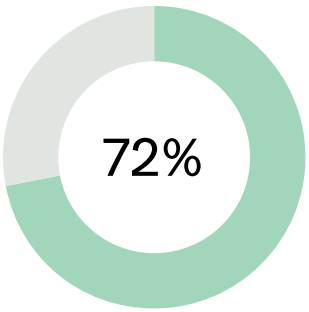
Avklare ansvar innen nasjonal cyberrobusthet



Ledere er ikke sikre på om deres organisasjon er del av kritisk infrastruktur



sier at ledere i deres organisasjon ser robustheten i kritisk infrastruktur som noen andres ansvar



sier at det er behov for større klarhet om hvilken rolle deres organiasjoner skal spille

Samtidig er risikobevisstheten høy: 58 prosent av ledere i kritisk infrastruktur vurderer at et alvorlig cyberangrep kan få politiske, økonomiske eller militære konsekvenser utover egen virksomhet, og 53 prosent av befolkningen forventer selv å bli berørt av en større cyberhendelse. Dette peker på behovet for samordnet håndtering på tvers av virksomheter og sektorer.

Mørketallsundersøkelsen tyder på et gap mellom erkjent risiko og operativ praksis: andelen hendelser som rapporteres formelt eller følges opp med strukturelle tiltak står ikke i forhold til det opplevde angrepstrykket. Samtidig er terskelen for å involvere myndigheter ofte høy, og mange virksomheter håndterer hendelser internt selv når de kan ha bredere konsekvenser. For beredskapssystemet reduserer dette muligheten til å identifisere mønstre og systemiske sårbarheter på tvers av sektorer, og svekker grunnlaget for forebygging, prioritering og planlegging.

Samlet peker Mørketallsundersøkelsen 2026 på at mørketall i stor grad skyldes organisatoriske og strukturelle forhold, ikke bare tekniske mangler. Når mange ledere i samfunnskritiske sektorer ikke ser cybersikkerhet som et tydelig eget ansvar, bidrar dette til lav rapportering og begrenset erfaringsdeling. Konsekvensen for nasjonal beredskap er svakere situasjonsforståelse og mindre læring på tvers av sektorer. Å redusere mørketall forutsetter tydeligere rolleforståelse og at rapportering og deling av erfaringer blir en integrert del av normal hendelseshåndtering.

10.5 TEK-Norge: Analyse

TEK Norge representerer om lag 350 medlemsvirksomheter i teknologi- og digitaliseringsnæringen – fra store systemleverandører og teleoperatører til spesialiserte sikkerhetsmiljøer og programvarehus. Mange befinner seg i selve ryggraden av de leverandørkjedene Mørketallsrapporten beskriver som sårbare inngangsporter for trusselaktører.

Det vi ser fra medlemsmassen, bekreftes av rapporten: norsk næringsliv er underinformert om truslene det faktisk står overfor. Virksomhetene frykter det de kjenner – phishing, bedrageri, sosial manipulering – og investerer deretter. Statlige aktørers målrettede operasjoner mot leverandørkjeder og profesjonaliseringen av det kriminelle cybermiljøet forblir utenfor synsfeltet til de fleste norske SMB-er. TEK Norges nordiske cyber benchmark-studie fra 2025 bekrefter dette: Norge havner konsekvent på sisteplass blant de nordiske landene på implementeringsgrad av grunnleggende sikkerhetskrav – selv når vi sammenligner virksomheter av tilsvarende størrelse og sektor.

Et strukturelt etterslep

Sverige, Danmark og Finland har enten implementert NIS2 eller har konkrete lovverk under iverksetting, mens Norge ikke har et fastlagt tidspunkt – antakelig først fra 2028. Det betyr to til fire tapte år der nabolandene allerede bygger ny sikkerhetspraksis. NIS2 tvinger frem det mange norske virksomheter mangler: formelle sikkerhetsstyringssystemer, dokumentert ledelsesinvolvering og rutiner for hendelsesrapportering. At 68 prosent av virksomhetene

som oppgir å ha et sikkerhetsrammeverk ikke kan identifisere hvilken standard det bygger på, viser omfanget av problemet.

Felles situasjonsforståelse og «gi og få»-prinsippet

Virksomhetene dimensjonerer sikkerhetstiltak mot det de har opplevd, ikke mot det som faktisk truer dem – fordi tilgang til relevant trusseletterretning er forbeholdt myndighetsaktører. Finland og Sverige har løst dette gjennom sektorvise ISAC-strukturer der nøkkelpersonell i privat sektor får bearbeidet etterretning. TEK Norges benchmark viser at Finland scorer høyest i Norden på offentlig-privat informasjonsdeling – og at dette har målbar effekt. Et «gi og få»-prinsipp, der virksomheter som rapporterer hendelser mottar trusseletterretning tilbake, ville gjort rapporteringen verdifull utover regeloverholdelse. I dag anmelder 79 prosent av virksomhetene som rammes ikke til politiet – en selvforsterkende tillitskrise.

Næringslivet mangler ikke vilje – men infrastruktur

58 prosent av virksomhetene mener de ikke har relevans for nasjonal beredskap; i privat sektor er andelen 71 prosent. I TEK Norges bransje – telekommunikasjon og IT – er 45 prosent interessert i myndighetssamarbeid, men bare 8 prosent har det formelt på plass. Det er den største avstanden mellom vilje og struktur i undersøkelsen. Totalforsvarsmodellen forutsetter privat næringsliv som en aktiv og informert partner. Undersøkelsen viser at dette ikke er tilfellet – ikke fordi viljen mangler, men fordi strukturene som gjør det mulig er ikke på plass.

11

Hovedfunn

Mørketallsundersøkelsen 2026 kartlegger digitale sikkerhetshendelser blant 2 500 norske virksomheter. Datagrunnlaget avdekker ikke ett enkelt problem, men en sammenkoblet kjede av mekanismer som hindrer at hendelser når statistikken og at virksomheter lærer av dem. Kapittelet presenterer åtte hovedfunn som til sammen tegner bildet: fra omfanget av selve mørketallene, via hvordan deteksjon og organisering fungerer, til hvordan kulturen rundt rapportering og oppfølging bestemmer hva som skjer etter at en hendelse er oppdaget.

Funnene er forankret i krysstabulering av undersøkelsens egne data og underbygges med offentlige norske og internasjonale kilder der mønstrene går igjen. Der andre kilder viser det samme, forsterkes funnet. Der de peker i andre retninger, gjøres dette eksplisitt.

11.1. Mørketallskjeden: fra 2 500 virksomheter til 57synlige saker

Av 2 500 respondenter oppga 452 (18 prosent) at de hadde opplevd minst én digital sikkerhetshendelse siste 12 måneder. Av disse anmeldte 57 (12 prosent) hendelsen til politiet. Fra utvalget som helhet tilsvarer det én anmeldt sak per 44 virksomheter. De resterende 373 som ikke anmeldte oppga i 42 prosent av tilfellene at hendelsen var «ubetydelig», i 16 prosent at den ble håndtert internt. Samtidig svarte mellom 3 og 6 prosent «vet ikke» på om de var utsatt for de ulike hendelsestypene, tilsvarende opptil 150 virksomheter uten oversikt over egen eksponering.

Mønsteret er i tråd med Kripos' vurderinger. Nasjonalt cyberkrimsenter (NC3) har i flere år beskrevet situasjonen slik at store mørketall og lav anmeldelsesrate gjør at cyberkriminelle opplever lav oppdagelsesrisiko og enda lavere risiko for straffeforfølgelse[7]. Politiets trusselvurdering 2026[8] beskriver at antallet straffesaker om innbrudd i datasystemer er tredoblet siden 2023, men understreker fortsatt at «virksomheter sjelden anmelder tjenestenektangrep og datainnbrudd». Undersøkelsens tall gir et kvantitativt grunnlag for denne vurderingen.

11.2. Rammeverket oppdager mer enn det forhindrer

Virksomheter med rammeverk rapporterer flere hendelser enn virksomheter uten: 22 prosent mot 15 prosent. For phishing er forskjellen enda tydeligere, 16 prosent mot 10 prosent. Det motsatte ville vært forventet dersom rammeverket reduserte eksponeringen; resultatet peker i stedet på deteksjonsbias. Virksomheter med formaliserte systemer ser mer av det som skjer.

7 https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2026.pdf
8 https://www.politiet.no/globalassets/tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2026.pdf

Et supplerende mønster bekrefter tolkningen. Blant virksomheter med rammeverk svarte 14 prosent «vet ikke» på minst én hendelsestype, mot 11 prosent blant de uten. Formaliseringen gjør virksomheten både bedre til å oppdage det som skjer og mer bevisst på hva den ikke kan verifisere. Virksomheter uten rammeverk har lavere usikkerhet fordi de stiller færre spørsmål, ikke fordi de har færre hendelser.

IBMs *Cost of a Data Breach Report 2025*[9] viser at den globale median-tiden for å identifisere og inneslutte et datainnbrudd er 241 dager, det laveste nivået på nesten ti år. Rapporten tilskriver forbedringen raskere deteksjon og responsautomatisering, som særlig store virksomheter og de med modne sikkerhetsprogrammer benytter seg av. Samme mønster gjør seg gjeldende i Norge: de virksomhetene som har rammeverk, ser mer. De uten ser mindre, men opplever trolig ikke mindre. Lavere rapporterte tall skjuler et høyere reelt omfang.

11.3. Rammeverk uten forankring er en blindflekk for ledelsen

Blant de 1 276 virksomhetene som har et rammeverk for informasjonssikkerhet, svarer 68 prosent at de ikke vet hvilken standard rammeverket bygger på. Dataene avdekker at manglende kunnskap er tydeligst hos de som sitter med det overordnede ansvaret: 75 prosent av de 742 daglige lederne med rammeverk kjenner ikke standarden. Blant IT-ansvarlige er andelen 38 prosent, og blant dedikerte sikkerhetsansvarlige 31 prosent. Differansen på 44 prosentpoeng mellom daglig leder og sikkerhetsansvarlig viser at kunnskapen eksisterer i virksomheten, men ikke hos de som skal forankre og følge den opp på strategisk nivå.

I NSMs Risiko 2026[10] beskrives denne utfordringen direkte. NSM ser jevnlig at ansatte er tildelt sikkerhetsroller uten å være klar over det eller uten å ha ressursene til å ivareta dem, med det resultat at sikkerhetsarbeidet ikke blir godt nok fulgt opp. Samme bilde går igjen i ENISAs NIS Investments 2025[11], der 63 prosent av små og mellomstore europeiske virksomheter ikke har gjennomført en sikkerhetsvurdering siste år, og over halvparten bruker mer enn tre måneder på å patche kritiske sårbarheter.

Med digitalsikkerhetsloven som trådte i kraft 1. oktober 2025 og forventet implementering av NIS2 i norsk rett, stilles det eksplisitte krav til at ledelsen i samfunnsviktige virksomheter forstår og følger opp sikkerhetsstyringen. Når tre av fire daglige ledere i dag ikke kan identifisere standarden bak sitt eget rammeverk, er etterlevelsen av disse kravene under press.

9 https://www.ibm.com/reports/data-breach
10 https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2026
11 https://www.enisa.europa.eu/publications/nis-investments

11.4. Terskelen for å anmelde handler mer om kultur enn om kompetanse

Anmeldelsesraten blant virksomheter som opplever en hendelse er 12,9 prosent med rammeverk og 13 prosent uten. Forskjellen er fraværende. Det samme gjelder etter type sikkerhetsansvarlig: virksomheter med fast ansatt anmelder i 14,8 prosent av tilfellene, de med ekstern konsulent i 15 prosent og de uten i 9,3 prosent. Gradienten er reell, men små utvalgsstørrelser gjør at forskjellen ikke er statistisk signifikant. Formell sikkerhetsorganisering endrer lite på anmeldelsesviljen.

Terskelen ligger et annet sted. Den vanligste oppgitte grunnen er at hendelsen er vurdert som ubetydelig (42 prosent). 16 prosent håndterte internt. Fire prosent oppgir manglende tillit til politiets evne til oppklaring. De 118 fritekstsvarene i kategorien «Annet» (32 prosent av ikke-anmeldere) avdekker likevel et mer sammensatt bilde: «IT tar seg av det», «henlegges uansett», «dårlig erfaring med tidligere anmeldelser», «for mye administrasjonskostnad». Summen tegner en kulturell holdning til anmeldelse der den oppleves som resultatløs før den er forsøkt.

NSR tolker dette slik at tiltak for økt anmeldelsesrate må rettes mot tillitsbygging og forenkling, ikke mot mer sikkerhetskompetanse.

11.5. Bagatellisering tross dokumenterte konsekvenser

Blant de 452 virksomhetene som opplevde en hendelse, rapporterte 46 prosent minst én merkbar konsekvens: oppfølgingskostnader (25 prosent), driftsforstyrrelser (19 prosent), omdømmetap (8 prosent), brudd på lovkrav (7 prosent) eller brudd på kontrakter (3 prosent). Likevel oppgir 42 prosent av ikke-anmelderne at hendelsen var «ubetydelig». Andelene overlapper: virksomheter som opplevde faktiske konsekvenser bagatelliserer likevel hendelsen.

Manglende årsaksanalyse forsterker mønsteret. 23 prosent av de med hendelse vet ikke hva som forårsaket den. Andelen er praktisk talt lik i virksomheter med og uten rammeverk (19 prosent i begge grupper), noe som indikerer at rammeverket ikke har bidratt til bedre forståelse av hva som gikk galt. Uten årsaksanalyse blir avgjørelsen om å bagatellisere tatt uten kunnskap om hendelsens omfang.

Internasjonale data viser at underestimering av kostnader er gjennomgående. IBMs rapport fra 2025 viser at gjennomsnittlig kostnad per sikkerhetsbrudd globalt er 4,44 millioner dollar, med betydelig spredning over bransjer og oppdagelsestid. Norske virksomheter som rapporterer tap, ligger under dette nivået (median 25 000 kroner), men en firedel tapte over 120 000 kroner og enkelttilfeller strekker seg til 5 millioner. Spredningen tilsier at klassifiseringen «ubetydelig» i 42 prosent av tilfellene trolig rommer hendelser med reell skade.

11.6. Privat sektor står utenfor nasjonal beredskap, men tre av ti er åpne for samarbeid

71 prosent av private virksomheter avviser enhver relevans for nasjonal beredskap, mot 29 prosent i offentlig sektor. Differansen på 42 prosentpoeng er en av de mest markante i hele undersøkelsen. Samtidig har 5,5 prosent av privat sektor formelt samarbeid med myndigheter om sikkerhet, mot 33 prosent i offentlig sektor.

NSM-direktør Arne Christian Haugstøyl beskrev situasjonen i *Risiko 2025* som at altfor mange norske virksomheter ikke har forstått sin egen verdi, og at det ofte ikke er produktet til den enkelte virksomhet som er interessant for trusselaktører, men muligheten til å bruke virksomhetens svakheter for å nå et annet mål. *Risiko 2026* understreker det samme: «det er vesentlige mangler i det forebyggende sikkerhetsarbeidet til virksomheter i Norge», og sårbarhetene går igjen på tvers av sektorer. Mørketallsundersøkelsen viser hvor stort gapet er mellom NSMs budskap og den faktiske selvoppfatningen i næringslivet.

Et viktig nyansering ligger i åpenhet. 30,1 prosent av privat sektor svarer at de ikke har samarbeid, men er åpne for det. Det er 5,5 ganger flere enn de som har formelt samarbeid. Selv blant de 1 461 virksomhetene som avviser all beredskapsrelevans, er 27,3 prosent åpne for samarbeid. Gapet mellom selvoppfatning og vilje er stort. De som tror de er irrelevante, er ikke lukket for å revurdere. Dette er et uutnyttet politisk handlingsrom.

11.7. To blindsoner: de minste virksomhetene og IT-sektoren

Undersøkelsen identifiserer to tydelig atskilte blindsoner med ulik dynamikk, men felles konsekvens: hendelser forblir usynlige for statistikken og for offentligheten.

Små virksomheter (5–19 ansatte) mangler grunnleggende sikkerhetsorganisering. 50 prosent mangler sikkerhetsansvarlig (mot 17 prosent i virksomheter med over 100 ansatte). 39 prosent har rammeverk (mot 74 prosent). 22,5 prosent av de med hendelse fulgte ikke opp i det hele tatt (mot 12 prosent blant mellomstore). 46 prosent svarer «vet ikke» på hva myndighetene bør gjøre for å hjelpe dem. Verizons DBIR 2025[12] viser at små og mellomstore virksomheter rammes av løsepengeangrep i 88 prosent av dokumenterte brudd, mot 39 prosent for store virksomheter. ENISAs undersøkelser har vist at 57 prosent av europeiske SMB-er vurderer at de ville gå konkurs eller opphøre etter en alvorlig sikkerhetshendelse[13].

Kombinasjonen av høy eksponering og lav organisering gjør dette segmentet særlig sårbart.

12 https://www.verizon.com/business/resources/reports/dbir/
13 https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

IT- og telekomsektoren representerer en helt annen type blindsone. Sektoren har 75 prosent rammeverksandel (høyere enn snittet) og 15 prosent uten sikkerhetsansvarlig (lavere enn snittet). Likevel rapporterer 42,5 prosent at de har hatt minst én hendelse siste 12 måneder, mer enn dobbelt så høyt som gjennomsnittet. Av de 17 virksomhetene i sektoren som opplevde hendelse, anmeldte ingen. 67,5 prosent av sektoren ser seg ikke som beredskapsrelevant. En sektor med høy formell modenhet fungerer altså ikke som rollemodell for anmeldelse eller beredskapsforståelse. Konsekvensen er betydelig: IT-leverandører inngår i leverandørkjedene til tusenvis av andre virksomheter.

11.8. Anmeldelse utløser strukturell læring

Kryssanalysen mellom anmeldelse (Q14) og oppfølgingstiltak (Q16) viser et mønster som styrker argumentet for å senke terskelen for anmeldelse. Av de 57 som anmeldte hendelsen, gjennomførte 42 prosent minst ett strukturelt tiltak i etterkant (endrede rutiner, teknisk utstyr, ekstern partner, leverandøroppfølging eller nyansettelser). Blant de 373 som ikke anmeldte, var andelen 24 prosent. Gjennomsnittlig antall strukturelle tiltak per virksomhet var 0,68 mot 0,28, en forskjell på 2,4 ganger.

Andelen uten oppfølging peker samme vei: 9 prosent blant anmelderne, 19 prosent blant ikke-anmelderne. Opplæring er det eneste tiltaket uten forskjell (omtrent 25 prosent i begge grupper). Det tyder på at opplæring skjer uavhengig av alvorlighet, mens strukturelle endringer utløses når hendelsen behandles formelt.

Leder for NC3 i Kripos har offentlig argumentert for at politidistriktene må etterforske flere datakrimsaker[14], med den begrunnelse at det er gjennom etterforskning man lærer om problemstillingen og får anledning til å forebygge nye hendelser. Mørketallsundersøkelsens data viser at det samme gjelder for den enkelte virksomhet: prosessen med å anmelde ser ut til å utløse mer systematisk respons enn når hendelsen håndteres internt. Årsaksretningen kan ikke avklares med dataene alene – det er mulig at mer seriøse virksomheter både anmelder og følger opp – men koblingen mellom anmeldelse og strukturell læring er tydelig.

14 https://www.politiforum.no/nc3-leder-politiet-ma-etterforske-mer-datakriminalitet/246426

Samlet bilde

De åtte funnene henger sammen. Mørketallene oppstår ikke på grunn av én enkelt mekanisme, men gjennom en kjede der hendelser filtreres ut på hvert trinn. Virksomheter uten rammeverk ser mindre. Virksomheter med rammeverk ser mer, men ledelsen forstår ikke alltid hva rammeverket innebærer. Oppdagede hendelser bagatelliseres. Bagatelliserte hendelser anmeldes ikke. Ikke-anmeldte hendelser følges i mindre grad opp strukturelt, og læringssløyfen brytes. Resultatet er at både det nasjonale trusselbildet og den enkelte virksomhetens handlingsrom blir dårligere forstått enn de kunne ha vært.

De sårbare segmentene – små virksomheter og privat sektor – er også de som i minst grad ser seg som en del av en større beredskapshelhet. Samtidig viser dataene at en betydelig andel er åpne for samarbeid, selv når de ikke har det i dag. Der finnes det handlingsrom. Kapittel 12 utdyper hvilke tiltak undersøkelsen peker mot.


LOYALTY CARD
UP TO 70
Featured Collections

12

Veien videre / Anbefalinger

Undersøkelsen avdekker gjennomgående mønstre som peker mot konkrete tiltak.

Senk terskelen for anmeldelser og rapportering.

79 prosent anmelder ikke. Årsakene er sammensatte, men manglende tillit til politiet og opplevelsen av at prosessen er meningsløs er gjengangere. Forenklede rapporteringskanaler som digitale meldingsskjemaer og lavterskel varsling til sektorvise responsmiljøer kan fange opp hendelser som i dag forsvinner.

Styrk sikkerhetsarbeidet i små virksomheter.

Virksomheter med 5 til 19 ansatte har sjeldnest rammeverk, oppdager færrest hendelser, følger opp minst og har høyest «vet ikke»-andel. Målrettede veiledningsressurser og gratis verktøy tilpasset denne gruppen vil trolig ha stor effekt.

Sats på deteksjon, ikke bare forebygging.

Virksomheter med rammeverk rapporterer flere hendelser enn de uten, trolig fordi de oppdager mer. Økt investering i deteksjonsevne vil sannsynligvis øke de rapporterte mørketallene, men gir et mer realistisk bilde av trussellandskapet og bedre grunnlag for tiltak.

Kommuniser beredskapsrelevans til privat sektor.

71 prosent av private virksomheter avviser enhver beredskapsrelevans. NSMs budskap om leverandørkjeder som inngangsporter har ikke nådd frem. Konkrete eksempler og bransjespesifikk veiledning kan gjøre budskapet relevant for den enkelte virksomhet.

Krev årsaksanalyse etter hendelse.

23 prosent vet ikke hva som forårsaket hendelsen. Uten årsaksanalyse kan ikke tiltak dimensjoneres. Digitalsikkerhetsloven og kommende NIS2-krav bør følges opp med veiledning om hendelseshåndtering som også inkluderer analyse i etterkant.

Forankre rammeverk i ledelsen.

68 prosent av de med rammeverk vet ikke hvilken standard det bygger på. Et rammeverk som bare eksisterer hos IT-leverandøren gir begrenset beskyttelse. Ledelsen må forstå hva rammeverket innebærer og aktivt følge opp etterlevelsen.

VEDLEGG A: SPØRSMÅL I UNDERSØKELSEN

Nedenfor følger en oversikt over spørsmålene som ble stilt i Mørketallsundersøkelsen 2026.

Spørsmål 1 (Q1) | Bakgrunn
Hvor mange ansatte er det i bedriften din?

Spørsmål 2 (Q2) | Bakgrunn
Hvordan er bedriftens IT-funksjon organisert?

Spørsmål 3 (Q3) | Bakgrunn
Har din bedrift en informasjonssikkerhetsansvarlig?

Spørsmål 4 (Q4) | Bakgrunn
Har bedriften et rammeverk/styringssystem for informasjonssikkerhet?

Spørsmål 5 (Q5) | Bakgrunn
Filter: Dersom «Ja» på spørsmål 4
Hvilken standard er rammeverket/styringssystemet hovedsakelig basert på?

Spørsmål 6 (Q6) | Trussel
Hvor trygg føler du deg på at din bedrift er rustet mot digitale trusler?

Spørsmål 7 (Q7) | Trussel
Hvilke digitale trusler er du bekymret for at din bedrift skal bli utsatt for?

Spørsmål 8 (Q8) | Hendelser
Har bedriften vært utsatt for en eller flere av disse digitale sikkerhetshendelsene i løpet av de siste 12 måneder?

- Datatyveri
- Digital utpressing (løsepengevirus/ransomware)
- Digitalt skadeverk
- Tjenestenektangrep
- Bedrageri
- Hacktivisme
- Sosial manipulering f.eks. phishing (e-post, SMS eller telefon)
- Annet

Spørsmål 9 (Q9) | Hendelse
Filter: Dersom «Ja» på alternativ 5. Bedrageri i spørsmål 8
Hvilke typer bedragerier har dere vært utsatt for?

- Direktørbedrageri (at gjerningspersonen utga seg for å være direktøren eller en annen person i toppledelsen)
- Fakturabedrageri (at gjerningspersonen sendte falske fakturaer til bedriften)

- Lån- og kredittbedrageri (at gjerningspersonen har tatt opp lån eller kreditt på vegne av bedriften)
- Investeringsbedrageri (at gjerningspersonen har lurt bedriften til å investere i verdiløse aksjer eller tilsvarende)
- Kortsvindel eller betalingsbedrageri
- Annet

Spørsmål 10 (Q10) | Hendelse
Filter: Dersom «Ja» på en eller flere av alternativene i spørsmål 8
Ta utgangspunkt i den mest alvorlige digitale sikkerhetshendelsen siste 12 måneder. Hva var den primære årsaken til at det ble oppdaget?

Spørsmål 11 (Q11) | Hendelse
Filter: Dersom «Ja» på en eller flere av alternativene i spørsmål 8
Ta utgangspunkt i den mest alvorlige digitale sikkerhetshendelsen siste 12 måneder. Hvilke faktorer mener du var direkte medvirkende til at den oppsto?

Spørsmål 12 (Q12) | Konsekvens
Filter: Dersom «Ja» på en eller flere av hendelsene i spørsmål 8
Hva var de økonomiske tapene knyttet til den digitale sikkerhetshendelsen i forrige spørsmål. Vi ber deg om å oppgi det totale tapet, både for direkte og indirekte tap.

Spørsmål 13 (Q13) | Konsekvens
Filter: Dersom «Ja» på en eller flere av hendelsene i spørsmål 8
Førte den mest alvorlige digitale sikkerhetshendelsen siste 12 måneder til noen av disse konsekvensene?

- Stans eller forstyrrelser i produksjon/drift
- Tap av kundedata eller sensitiv informasjon
- Omdømmetap/tillitstap
- Brudd på kontraktsforpliktelser
- Brudd på lovkrav (f.eks. brudd på GDPR eller annet)
- Oppfølgingskostnader/opprettingskostnader
- Annet
- Ingen merkbare konsekvenser
- Vet ikke

Spørsmål 14 (Q14) | Håndtering
Filter: Dersom «Ja» på en eller flere av hendelsene i spørsmål 8
Anmeldte dere den mest alvorlige digitale sikkerhetshendelsen de siste 12 måneder til politiet?

Spørsmål 15 (Q15) | Håndtering
Filter: Dersom «Ja» på en eller flere av hendelsene i spørsmål 8, og «Nei» på spørsmål 14
Oppgi hovedårsak til at det ikke ble anmeldt.

Spørsmål 16 (Q16) | Oppfølging
Filter: Dersom «Ja» på en eller flere av hendelsene i spørsmål 8
Ta utgangspunkt i den mest alvorlige digitale sikkerhetshendelsen siste 12 måneder. Hvordan har bedriften fulgt den opp i etterkant? Du kan oppgi flere tiltak.

Spørsmål 17 (Q17) | Oppfølging
Hva mener du at myndighetene bør gjøre for å hjelpe små- og mellomstore bedrifter med digital sikkerhet?

Spørsmål 18 (Q18) | Nasjonal sikkerhet
Har din bedrift en direkte eller indirekte rolle i Norges nasjonale beredskap?

Spørsmål 19 (Q19) | Nasjonal sikkerhet
Har din bedrift etablert formelt eller uformelt samarbeid med offentlige myndigheter (som f.eks. Nasjonal sikkerhetsmyndighet, Politiet eller Forsvaret) om sikkerhetsspørsmål?

Flere spørsmål inkluderte et åpent svaralternativ («annet, spesifiser») der respondentene kunne utdype med fritekst. Disse besvarelsene er analysert og integrert i rapporten som tematiske oppsummeringer.


Jernbaneverket
STATSBYGG

Næringslivets
sikkerhets-
råd

www.nsr-org.no