Bevissthet og beredskap

Atea sikkerhetsrapport 2024

INNHOLD

04 Sammen sikrer vi Norge

05 Viktigste funn

06 Om undersøkelsen

08 Sikkerhet i offentlige anskaffelser

10 Dagens trusselbilde

12 Investeringer

14 Flaks som IT-sikkerhetsstrategi

16 Fokus på IT-sikkerhet

18 Forberedelse på krise

20 Hvor mange ledermøter med IT-sikkerhet som tema gjennomføres i 2024?

22 Flere har kjennskap til grunnprinsippene, men færre iverksetter

24 Hvor mange investerer i cyberforsikring?

26 Kunstig intelligens og sikkerhet

Sammen sikrer vi Norge

Nå er årets IT-sikkerhetsundersøkelse klar. Vi har spurt et representativt utvalg av daglige ledere og IT-ansvarlige i norske virksomheter. Svarene er godt spredt både geografisk, bransjemessig og når det kommer til virksomhetsstørrelse. Respondentene har svart på relevante spørsmål om hvordan de ser på dagens trusselbilde, egen sikkerhetskompetanse og investeringsvilje opp mot dagens trusselbilde.

Det er nå det andre året vi utfører denne undersøkelsen, og ser at resultatene gir et godt bilde på sikkerhets-situasjonen, og hjelper med å kartlegge hvordan det står til med IT-sikkerheten i Norge.

I fjorårets undersøkelse åpnet vi med å peke på at funnene var omtrent like skremmende som forventet. Årets undersøkelse viser at norske virksomheter har tatt grep innenfor noen områder. Men det er ingen tvil om at IT-sikkerheten i norske virksomheter er under press, og at det haster med å implementere nødvendige tiltak. Vi kan ikke lenger tillate oss å se bort fra trusselbildet. Tallenes tale er klar – Norge er for dårlig forberedt.

Jeg liker i utgangspunktet ikke å drive med skremselspropaganda, men norske virksomheter, og dermed samfunnet som helhet, er for dårlig forberedt. Vi må handle, og viktigst av alt, samhandle på tvers av privat og offentlig sektor for å møte utfordringene.

Det er flere og flere i både privat og offentlig sektor som har begynt å bruke emneknaggen **#SammenSikrerViNorge** med god effekt. Men hvem er det som eier denne emneknaggen? Svaret er; du, jeg, de, vi, alle. Det vil si alle vi som på en eller annen måte bidrar til å sikre Norges digitale verdier.

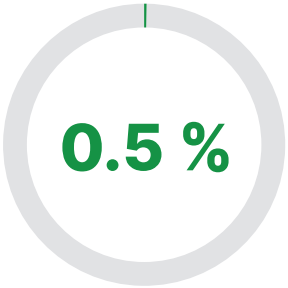
Så om du jobber hos myndighetene eller i det private næringslivet, er en tjenestetilbyder av sikkerhet, en produsent av IT-sikkerhetsteknologi, eller du rett og slett bare er opptatt av hvordan vi kan beskytte oss bedre digitalt, er du en like stor del av folkebevegelsen **#SammenSikrerViNorge** som alle andre.

Jeg håper du vil finne rapporten og resultatene interessante og bruker dette videre i planleggingen av hvordan vi sammen kan sikre Norges digitale verdier.

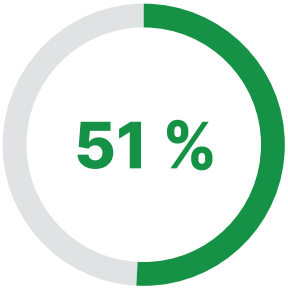
Med vennlig hilsen

Thomas Tømmernes
Leder IT-sikkerhet
Atea Norge

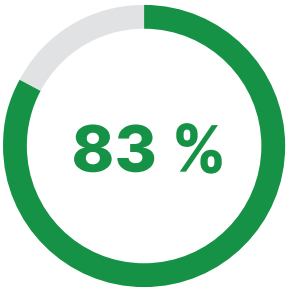
Viktigste funn



Norske virksomheter budsjetterer med å bruke 0.5 % av virksomhetens budsjett på IT-sikkerhet.

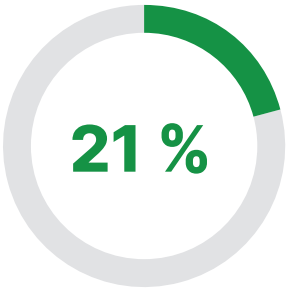


51 % av norske virksomheter har beredskapsplan.

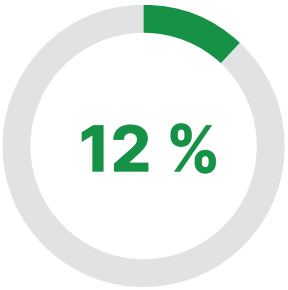


83 % sier de ikke har egne ansatte som jobber med IT-sikkerhet som hovedoppgave.

30 000 færre ledelsesmøter hvor IT-sikkerhet er på agendaen.



Kun 1 av 5 øver på hva man skal gjøre i virksomheten dersom de blir utsatt for en IT-sikkerhetshendelse.



Kun 12 % fra de private virksomhetene opplever at myndighetene har bidratt til å styrke virksomhetens IT-sikkerhet.

De små virksomhetene bruker gjennomgående mindre ressurser og fokus på IT-sikkerhet. Dette gjelder både offentlig og privat sektor:

- 10 % av de minste virksomhetene har egne ansatte hvor hoveddelen av arbeidsoppgavene omhandler IT-sikkerhet, mot 38 % for de største virksomhetene.
- 45 % av de største virksomhetene planlegger å øke investeringene i IT-sikkerhet de neste 12 månedene, mot kun 16 % av de minste virksomhetene.
- 70 % av de største virksomhetene gjennomfører regelmessig brukeropplæring av egne ansatte mot kun 34 % av de minste virksomhetene.
- 37 % av de minste virksomhetene har en beredskapsplan dersom de blir utsatt for en IT-sikkerhetshendelse, mens 75 % av de største virksomhetene har en beredskapsplan.
- 26 % av de minste virksomhetene kjenner til NSM sine grunnprinsipper for IKT-sikkerhet, mot 82 % av de største virksomhetene.

Det er også mye usikkerhet i virksomhetene rundt IT-sikkerhet. 18 % av virksomhetene vet ikke hvor mye av IT-budsjettet som går til IT-sikkerhet. 23 % vet ikke om de skal øke investeringene i IT-sikkerhet de neste 12 månedene. 29 % vet ikke om de har cyberforsikring. 43 % vet ikke om kunsig intelligens (AI) utgjør en sikkerhetsrisiko for virksomheten.

Om undersøkelsen

Intervjumetode:	Telefon- og webintervju
Antall intervju:	804
Periode datainnsamling:	Februar-mars 2024
Målgruppe:	Daglig leder/ansvarlig for IT/IT-sikkerhet i norske bedrifter med mer enn 5 ansatte
Populasjon:	Det er omtrent 105 000 virksomheter i Norge med 5 eller flere ansatte
Gjennomført av:	Kantar

I årets undersøkelse hadde vi totalt 804 respondenter. Av disse var 418 daglige ledere og 386 ansvarlige for IT-sikkerhet i offentlige og private virksomheter. Virksomhetene er fordelt utover hele Norge, der 154 Oslo-baserte virksomheter, 259 fra Østlandet, 199 fra Sør- og Vestland, 123 fra Midt-Norge og 68 fra Nord-Norge gjennomførte årets undersøkelse. Det var jevn fordeling mellom små-, mellomstore og store virksomheter, både i antall ansatte og omsetning.

Dette har dermed gitt oss et solid totalbilde på situasjonen i norske virksomheter.


IT SECURITY

Sikkerhet i offentlige anskaffelser

Veileder om ivaretakelse av sikkerhet i offentlige anskaffelser

Større fokus på sikkerhet i anskaffelser har kommet gjennom et «kvalitetssikringsverktøy» i form av en veileder (Veileder om ivaretakelse av sikkerhet i offentlige anskaffelser). Litt forenklet, har denne veilederen gjort det lettere for IT-avdelingene å slå i bordet og kreve at deres ønsker og vurderinger rundt IT-sikkerhet blir ivaretatt i offentlige anskaffelser.

Veilederen gir IT-sjefen i det offentlige flere lissepasninger når det kommer til å argumentere for hvorfor pris blir sekundert, når man mener at det er store kvalitetsforskjeller i tilbudene. Blant annet kravet om at en i forkant av et innkjøp, som kan påvirke eller relateres til sikkerhet, må foreta en risikovurdering av anskaffelsen. Det burde gi store muligheter for innkjøpsavdelingen til å involvere IT-avdelingen i begrunnelsen for valget av løsningen.

Veilederen viser handlingsrommet

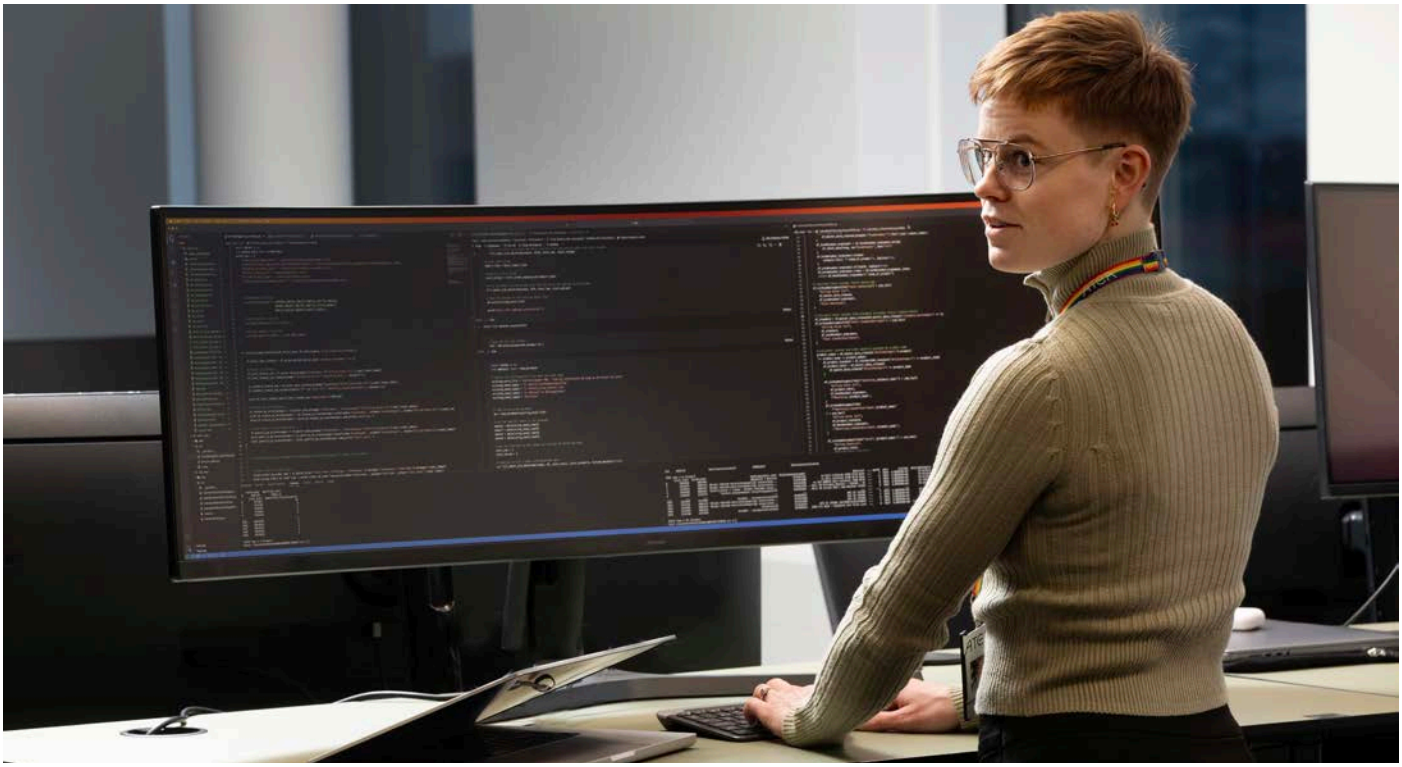
Veilederen har som mål å synliggjøre handlingsrommet i anskaffelsesregelverket, og gjennom dette hvordan offentlige oppdragsgivere kan ivareta norske sikkerhetsinteresser når de gjør innkjøp.

Den nye veilederen har derfor også en omtale av hvordan offentlige oppdragsgivere kan ivareta sikkerhet i anskaffelser som ikke faller inn under sikkerhetsloven, men hvor sikkerhet likevel er et sentralt element.

I tillegg gir veilederen informasjon om risikovurderinger i forkant av anskaffelsen, og hvordan oppdragsgiverne kan gå frem for å gjennomføre slik risikovurderinger.

Det betyr at det offentlige i større grad kan og bør benytte profesjonelle IT-sikkerhetstilbydere til å bidra med å forme sikkerhetskravene i forkant, og appellere til at man utfordrer der vi tydelig ser at utlysningen ikke har ivaretatt sikkerheten. Både Nasjonal sikkerhetsmyndighet (NSM) og Norsk senter for informasjonssikring (NorSIS) har uttalt gjentatte ganger at virksomheter uten egen IT-sikkerhetsavdeling, bør kjøpe inn denne kompetansen som en tjeneste.

Med andre ord; her gjelder det å spille på lag med og/eller utfordre innkjøperne om det er gjort risikovurderinger. I mange tilfeller vil dette innebære å bruke fagspesialistene og rådgiverne fra den kommersielle aksen, slik at man også får en ekstern vurdering.



Fire tips til krav du bør følge ved anskaffelser

1. Det er ikke lett å differensiere leverandører og tilbydere fra hverandre. Fokuser først og fremst på behovet for å få en oversikt over dagens nå-situasjon, før man utarbeider en bestilling eller et anbudsdokument. En ROS-analyse (risiko- og sårbarhetsanalyse) i kombinasjon med en sårbarhetsskanning og penetrasjonstest av virksomhetens IT-systemer, er en anbefalt start. Resultatene herfra vil gi et godt bilde på dagens utfordringer, status og sikkerhetsnivå. Samtidig vil det avdekke hvilket behov man trenger å fokusere på i en bestilling.

2. Mange anskaffelser har problematikk rundt personvern, og da også informasjonssikkerhet. Det er ingen som kommer utenom å overholde GDPR, og da er det også mange krav som må oppfylles.

3. Rent konkret krever nå mange kommuner at tilbydere må godta KiNS-malen for databehandleravtale (DBA), med vedlegg 1 og 2. Her vil IT-sjefer og andre også finne en ny «lissepasning» i vedlegg 1. Der det ramses opp en mengde gode sikkerhetskrav, utledet fra GDPR og normen, som tilbydere må svare på.

4. Det er Bærum kommune som har utviklet malen, men den kan fritt brukes av alle - også leverandører. Så jobber du i offentlig sektor, eller bidrar på en eller annen måte inn i anbud fra stat, kommune osv., er disse dokumentetene noe du kan bruke som din brekkstang for å få øket kvaliteten og sikkerhetsfokuset i alle anskaffelser fremover.

Dagens trusselbilde

I Nasjonal Sikkerhetsmyndighets (NSM) rapport «Risiko 2024», skriver de at Norges sikkerhetsutfordringer påvirker hele samfunnet. Nasjonal sikkerhet angår staten, offentlige virksomheter, privat næringsliv, enkelt-personer og alt imellom - og at IT-sikkerhet dermed er et samfunnsansvar.

Økning på 400 prosent

I løpet av 2023 håndterte hendelseshåndtererne i Atea Incident Response Team (IRT) i underkant av 400 sikkerhetshendelser for våre kunder. Dette er en økning på 400 prosent, sammenlignet med året før.

Over halvparten av de suksessfulle hendelsene var relatert til e-post. Noen eksempler på konsekvenser av disse angrepene har vært tap i multimillionklassen, data-dumping, kompromitterte kontoer og ytterligere spredning av angrepet til offerets kontakter. I «Risiko 2024» skriver NSM at kvaliteten på såkalt «spearfishing» har nådd et urovekkende høyt nivå og at alle mennesker kan bli lurt i et svakt øyeblikk, selv den mest årvåkne.

Ransomware

Gjennom året ble det også håndtert flere ransomwareangrep. Denne typen angrep setter alle systemer og løsninger på prøve, og alle mangler og feil i oppsettet blir over natten større og tydeligere. For IT-organisasjoner er nok dette den mest krevende situasjonen å havne i.

Å komme tilbake til operasjonell drift etter en ransomwarehendelse tar tid. Erfaringene til IRT viser at det tok gjennomsnittlig 4-5 dager før kritiske produksjonssystemer ble operative, mens det tok flere måneder før alle systemer er oppe og gå hos noen virksomheter.

Våre erfaringer tilsier at hovedkostnaden ved ransomwarehendelser er produksjonstap. I følge IBM og deres rapport «Cost of a Data Breach Report 2023» blir kostnadene høyere for hvert år som går.

Utnyttelse av kjente sårbarheter og feilkonfigurering har vært startpunkt på samtlige ransomwarehendelser håndtert i 2023, til forskjell fra tidligere år hvor skadevare fra sluttbruker har vært hovedårsak. IRT tror at dette henger sammen med gjennomføringsevne på prosjekter og konfigurering, samt en mangel på kontinuerlig sikkerhetsfokus. Mange virksomheter vet at de burde ha gjort noe før hendelsen oppsto, men har ikke kapasitet til å prioritere IT-sikkerhetsarbeidet eller til å holde seg oppdatert på dagens trusselbilde.

I angrepene som ikke resulterte i kryptering var årvåkenhet, tilfeldigheter og flaks årsaken til at hendelsen ble oppdaget. I hendelsene hvor trusselaktør hadde fullført kryptering var det tilfeller av alarmer, men da utenfor normal arbeidstid og virksomhetens ansatte kunne dermed ikke agere raskt nok.

Enkle tiltak kan hjelpe

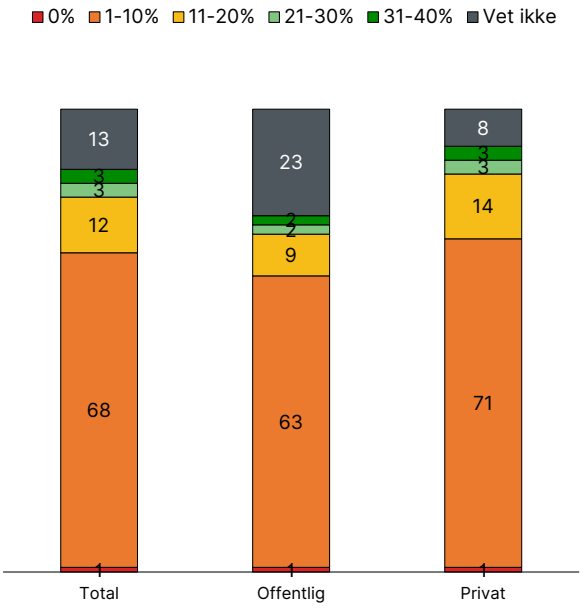
Ransomwarehendelser fra 2023 viser at det ikke nødvendigvis er dyrt eller avansert å beskytte seg, men det kreves grunnleggende sikkerhetshygiene. Dette bekreftes også av Nasjonal Sikkerhetsmyndighet (NSM) som tidligere har uttalt at omlag 80 prosent av hendelsene de håndterer kunne vært unngått hvis grunnleggende sikkerhetstiltak var blitt fulgt.

NSM har uttalt at omlag 80% av hendelsene de håndterer kunne vært unngått hvis grunnleggende sikkerhetstiltak var blitt fulgt. Det er derfor viktig å øke bevisstgjøringen og styrke det forebyggende arbeidet. Samtidig må virksomheter og myndigheter ha kompetanse og kapasitet til å avdekke og håndtere uønskede hendelser.
Meld. St. 9 (2022-2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig.

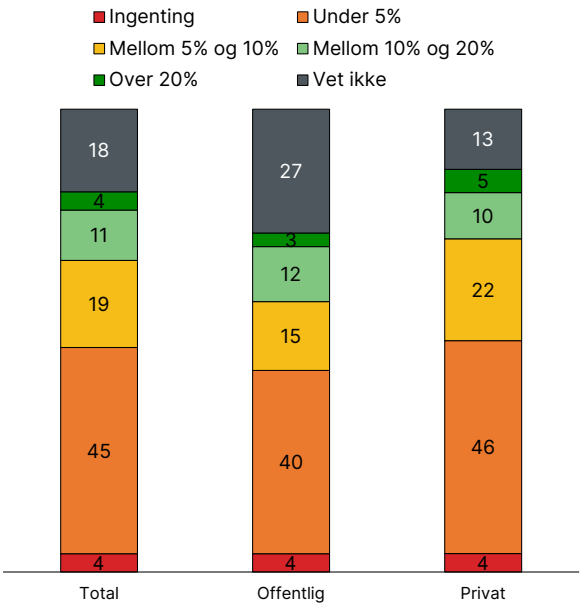
Investeringer

Fortsatt ser vi at majoriteten av norske virksomheter setter av mindre enn 10 % av sitt totale budsjett til IT. Her er det ikke store utslag sammenliknet med 2023. Det er også bare mindre utslag på spørsmålet om hvor stor andel av IT budsjettet som går til IT-sikkerhet.

Fremdeles kan vi konkludere med at majoriteten av norske virksomheter bruker mindre enn 5 % av IT-budsjettet på sikkerhet. Sagt på en annen måter, **norske virksomheter budsjetterer med å bruke 0.5 % av virksomhetens budsjett på IT-sikkerhet.**



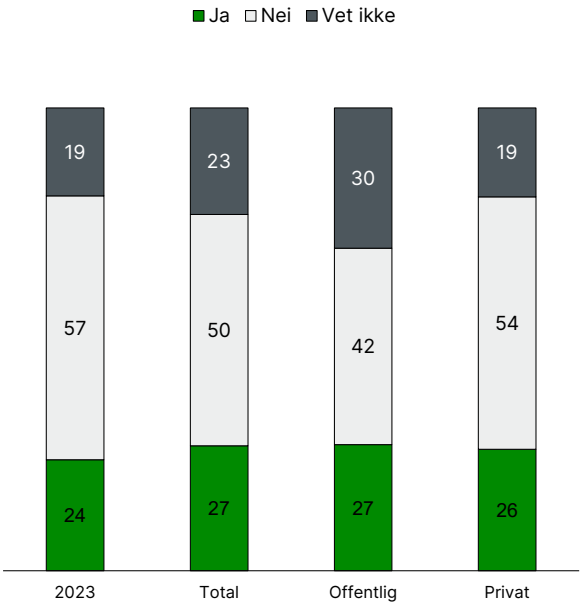
Budsjett IT. *Omtrent 7 av 10 norske virksomheter setter av mindre enn 10 % av sitt totale budsjett til IT. Kun 6 % setter av mer enn 20 %.*



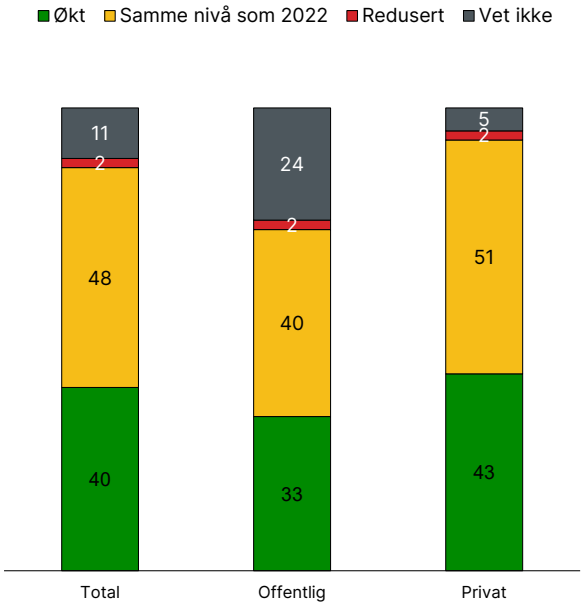
Budsjett IT-sikkerhet. *Nesten halvparten av norske virksomheter bruker mindre enn 5 % av IT budsjettet til IT-sikkerhet. Kun 15 % bruker mer enn 10 % av IT budsjettet til IT-sikkerhet. Nesten 1 av 4 i offentlige virksomheter oppgir at de ikke vet hvor mye av IT budsjettet som brukes til IT-sikkheret.*

Vi i Atea mener dette er for lavt. Vi spør derfor også om det foreligger planer for å øke dette budsjettet i løpet av det kommende året. Her svarer ca. ¼ av virksomhetene at, ja det skal vi. Dette kan peke på den økonomiske nedgangstiden vi har vært i, og at det er forventninger til økte budsjetter i den kommende perioden. Men, det kan også være at virksomhetene er klar over at et IT-sikkerhetsbudsjett som tilsvarer 0.5 % totalbudsjettet antakelig er for snaut. Vi fulgte derfor opp med et spørsmål rundt hvordan dette faktisk så ut i året som gikk. Ble investeringene større eller lavere enn det budsjetterte? Kun 2 % oppga at investeringene ble lavere enn forventet, men hele 4 av 10 oppga at investeringene ble høyere enn budsjettet. Det er også verdt å merke seg at 24 % oppgir at de skal øke budsjettene det kommende året, mens hele 40 % endte med å øke investeringene i året som gikk.

Vi tror dette handler om en gradvis modning i forståelsen av sikkerhetsfaget og at viktigheten av god kontroll stadig blir tydeligere. Vi vil også trekke frem bransjens evne til å gjøre seg bedre forstått i styrerommene og måten IT-sikkerhetsutfordringen legges frem på til virksomhetsledere. Et annet viktig poeng handler om en økende bevissthet og tydeligere kravstilling fra myndigheter, samarbeidspartnere, leverandører og kunder. Dette har vært med på å øke investeringen på IT-sikkerhet hos virksomhetene.



Skal virksomheten øke investeringene i IT-sikkerhet de neste 12 månedene. *Til tross for en marginal økning fra 2023, så har neten 1 av 4 norske virksomheter planer om å øke invetseringene i IT-sikkerhet de neste 12 månedene. 23 % oppgir at de ikke vet.*



Investeringer i IT-sikkerhet i 2023 sammenlignet med 2022. *4 av 10 norske virksomheter økte investeringene i IT-sikkerhet i fjor sammenlignet med året før. Kun 2 % reduserte investeringene.*

Flaks som IT-sikkerhetsstrategi

Vi legger bak oss et år med der vi i Atea har hatt rekordmange utrykninger til større og mindre angrep og hendelser.

Thomas Tømmernes
Leder IT-sikkerhet
Atea Norge

I løpet av 2023 har våre hendelseshåndterere (Atea Incident Response Team), de som rykker ut når IT-angrepet skjer, håndtert i underkant av 400 sikkerhetshendelser. Tallet dreier seg i hovedsak om henvendelser fra norske kunder, men vi jobber også med hendelser fra våre nordiske naboland. Ser vi tilbake til antallet hendelser i 2021-22, så er dette en økning på 400 prosent, og det er ingen indikasjoner på at trusselbildet blir mindre alvorlig i 2024.

Mange e-postangrep

Over halvparten av antallet hendelser relaterer seg til e-post. Dominerende innen dette feltet er såkalte «Adversary-in-the-Middle», eller AiTM-angrep. Denne typen angrep er ganske lik vanlige phishing-angrep – som er angrep der noen prøver å lure deg til å trykke på en falsk lenke i en epost.

«AiTM-angrep kan banalt sammenlignes med at en kriminell setter en papirlapp i låsen på din ytterdør før den smekker igjen, og kan åpne døren når vedkommende selv har lyst.»

Mer teknisk fungerer det slik at de IT-kriminelle bruker en proxy-server til å sitte mellom deg og tjenesten du logger på. Proxy-serveren kan for eksempel vise innlogging til Microsoft 365, eller andre internett-tjenester du bruker i hverdagen. Den brukes så til å fange opp påloggingsinformasjonen din inklusivt session cookie.

Denne cookien brukes av angriperen for å autentisere seg, selv om du bruker to-faktor autentisering. Angriperen kan deretter bruke denne innloggingen til å nå dine tjenester fra en annen nettleser – for eksempel din epostkonto.

De første tilfellene av AiTM fanget vi opp sommeren 2022, men frem til 2023 var de relativt sjeldne. Denne angrepsmetoden økte utover året og nådde toppen samtidig som sommermånedene kom, derifra og ut året var det jevnt høyt.

Men om du nå sitter med følelsen av «maktesløshet» for at til og med tofaktorautentisering kan misbrukes, kan vi fortelle at det er fult mulig å beskytte seg mot AiTM, og vi anbefaler alle bedrifter å vurdere tiltak

tilpasset sitt behov. Vi anbefaler også på det sterkeste å fortsatt benytte tofaktorautentisering, da dette stopper det aller meste av «enkle» forsøk.

Økning i antall ransomware-angrep

I løpet av året som har gått har vi også håndtert en mengde ransomware-angrep. Dette er angrep som krypterer all data og hackeren krever løsepenger for å dekryptere. Det er nok den typen situasjon som er mest krevende for it-organisasjoner å havne i, for de er så effektive og som regel lammer hele organisasjonen.

Vi har håndtert både pre-ransomwarehendelser hvor angrepet er oppdaget og håndtert før kryptering, og fulle ransomwarehendelser som har resultert i delvis eller fullstendig infrastrukturkryptering. I begge disse tilfellene må miljøet gjennomgås fullstendig, for å avdekke om data er på avveie og finne inngangsportene de kriminelle har brukt.

Fellesnevnere

For de av hendelsene som ikke resulterte i kryptering, var fellesnevneren at virksomheten hadde implementert gode løsninger for logg og overvåking, som alarmerer når it-kriminelle er på vei inn i virksomhetens nettverk. Har man ikke gode overvåkingssystemer på plass, må man stole på årvåkenhet, tilfeldigheter og ofte flaks.

I de tilfellene der hendelsen resulterte i kryptering var det også likhetstrekk. Noe av det som går igjen er manglende oversikt over systemer og tjenester eksponert mot internett, samt mangel på en fullverdig beredskapsplan. Disse funnene bekreftes også av vår undersøkelse fra fjoråret, « Bevissthet og beredskap 2023».

Ikke nødvendigvis dyrt å beskytte seg

Innfallsvinkelen på samtlige av ransomwarehendelsene vi håndterte i 2023 var utnyttelse av sårbarheter og feilkonfigurering. Ransomwarehendelser fra 2023 viser også at det ikke nødvendigvis er dyrt eller avansert å beskytte seg. Men det krever at man har kontroll på egen infrastruktur, sørger for kontinuerlig oppdateringer, har flerfaktorautentisering (MFA multifaktor) og begrenser VPN-tilgangen.

Skulle ulykken likevel være ute, er vi som hendelseshåndterere avhengig av at virksomheten har gode «backup»-rutiner og et tidsriktig «backup»-system. Vi opplever for ofte at virksomheter har trodd de har fungerende «backup», men det ikke viser seg å stå til forventningene. Har du ikke «backup» når din virksomhet blir kompromittert og all data krypteres, tvinges virksomheten din til å måtte velge mellom å starte på nytt eller å betale for å få tilbake tilgangen til dataene dine.

Vi anbefaler ingen å betale løsepenger, dette er som politiet sier å støtte oppunder kriminell aktivitet og fører bare til at angriperne fortsetter. Vårt beste råd er derfor å ta utgangspunktet i grunnprinsippene til Nasjonal sikkerhetsmyndighet, utføre den grunnleggende sikkerhetshygienen og jobbe proaktivt.

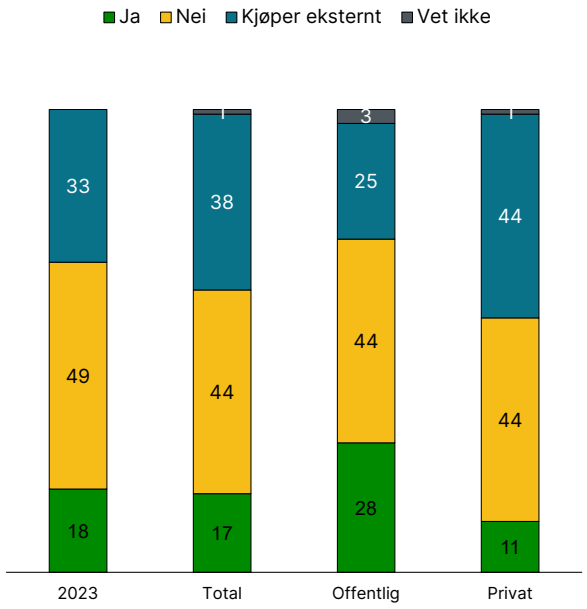
Vet du ikke helt hvor du skal begynne, er det aller enkleste å utføre en modenhetsanalyse basert på NSM grunnprinsipper. Etter gjennomført aktivitet sitter med en konkret liste over hva man bør gjøre både organisatorisk og teknisk.

Jobb proaktivt, ikke la sikkerhetsstrategien og virksomhetens fremtid basere seg på flaks.

Fokus på IT-sikkerhet

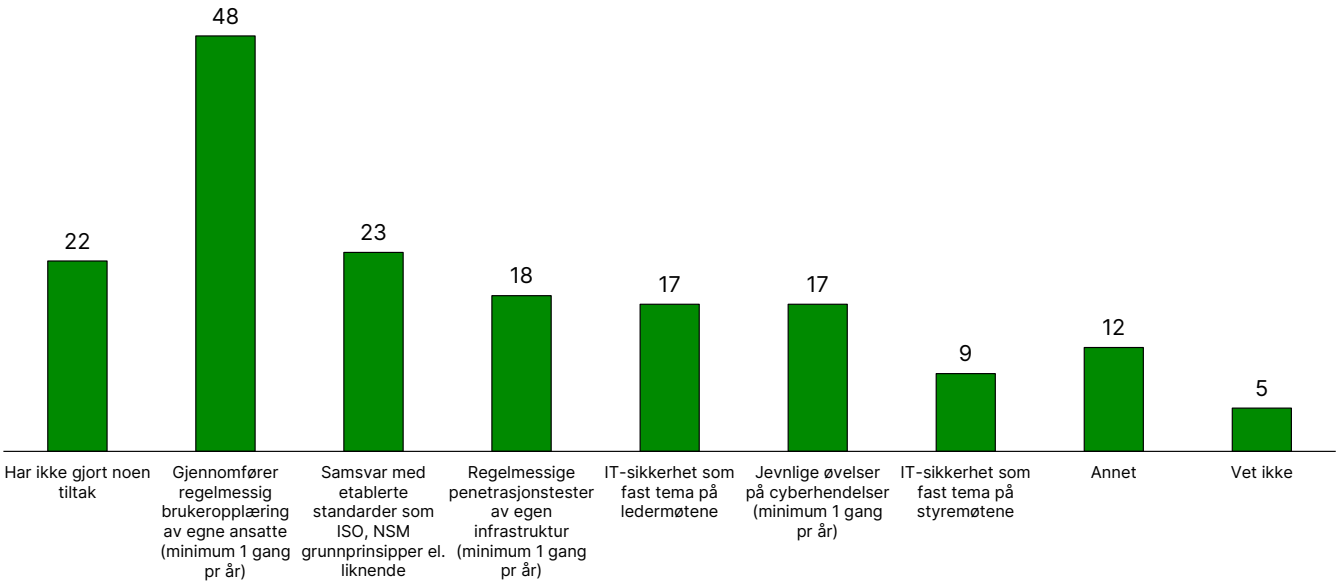
Det har lenge vært belyst en knapphet på IT-sikkerhetsressurser i Norge. Selv om høyskoler og universiteter nå har gode utdanningsløp for denne typen kompetanse, vokser behovet raskere enn den totale kapasiteten. Nye teknologiske fremskritt tillater oss å bruke kunstig intelligens for økt efektivitet, bygge inn automatiserte rutiner og bedre utnyttelse av systemer. Samtidig er og blir kompetanse en knapphet som man enten selv må investere i (ansettelser) eller som man kjøper av en spesialist (outsorcing).

Når vi spør virksomhetene om hvordan de forholder seg til dette, er det bare 17 % som sier at de har egne ansatte som jobber med IT-sikkerhet som hovedoppgave. Tallene totalt sett er ikke så ulike i år i forhold til hvordan det så ut i fjor. Men i svarene ligger det likevel et interessant poeng. Andelen av offentlige virksomheter som har egne ansatte er nesten tre ganger så høy som hos de private virksomhetene. På samme måte har de private virksomhetene nesten dobbelt så stor andel som kjøper denne kompetansen eksternt. Sammenliknet med sist år er forskjellene på begge sider økende. Det er altså en tydelig trend at det offentlige ansetter IT-sikkerhetskompetanse mens de private heller kjøper dette fra aktører som foreksempel Atea.

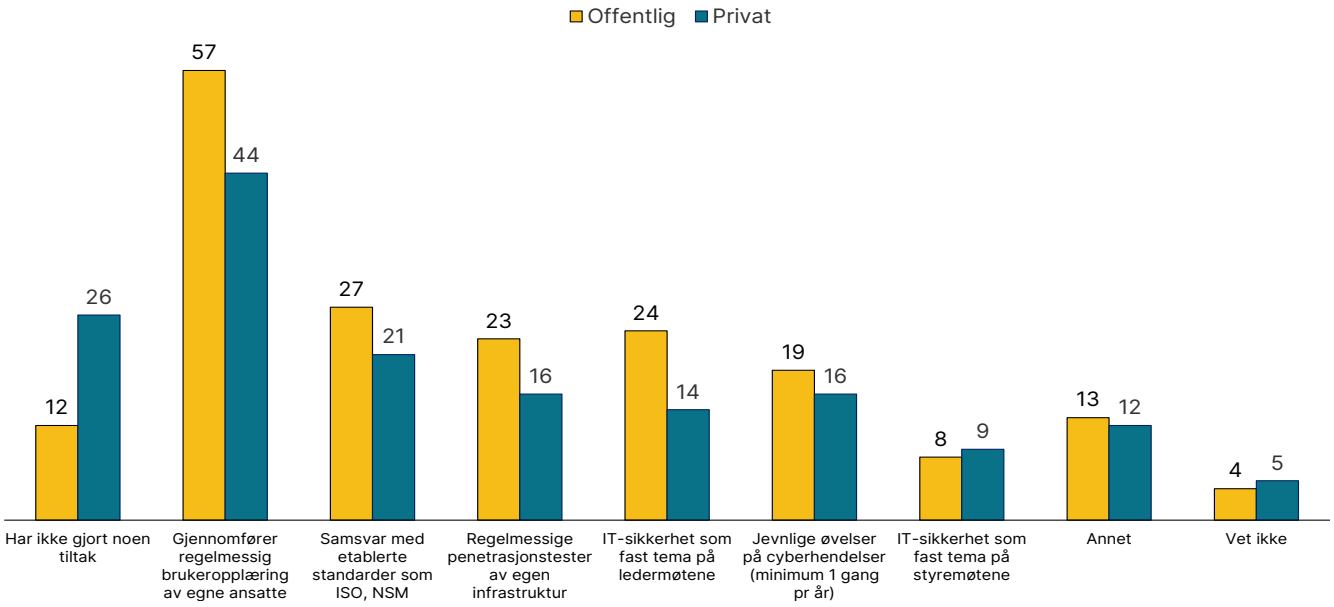


Egne ansatte som jobber med IT-sikkerhet i virksomheten.

Trekker vi dette videre, og ser på hvilke faktiske tiltak som gjøres for å sette fokus på IT-sikkerhet i virksomhetene, ser vi en generell høyere score hos de offentlige virksomhetene. Dette kan indikere en potensiell gevinst av å ha egne ansatte som jobber dedikert med sikkerhet internt i virksomheten. Det er også urovekkende at over 30 % av de private virksomhetene ikke gjør noen tiltak, eller ikke vet om de gjør noen tiltak.

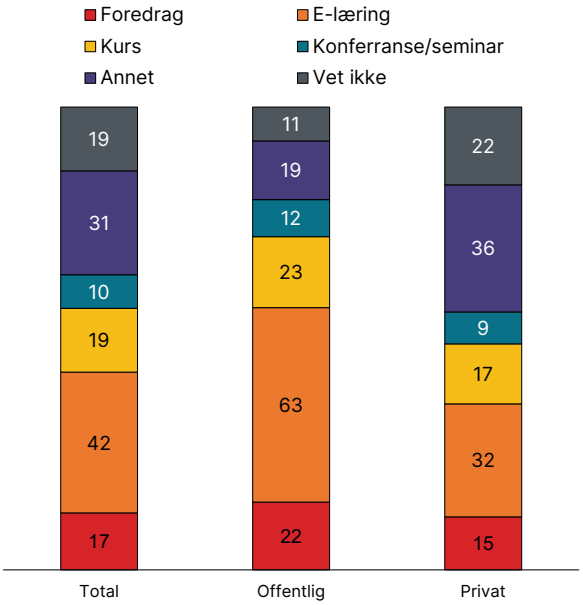


Tiltak virksomheten har gjort for å ha fokus på IT-sikkerhet.



Tiltak virksomheten har gjort for å ha fokus på IT-sikkerhet - offentlig og privat sektor.

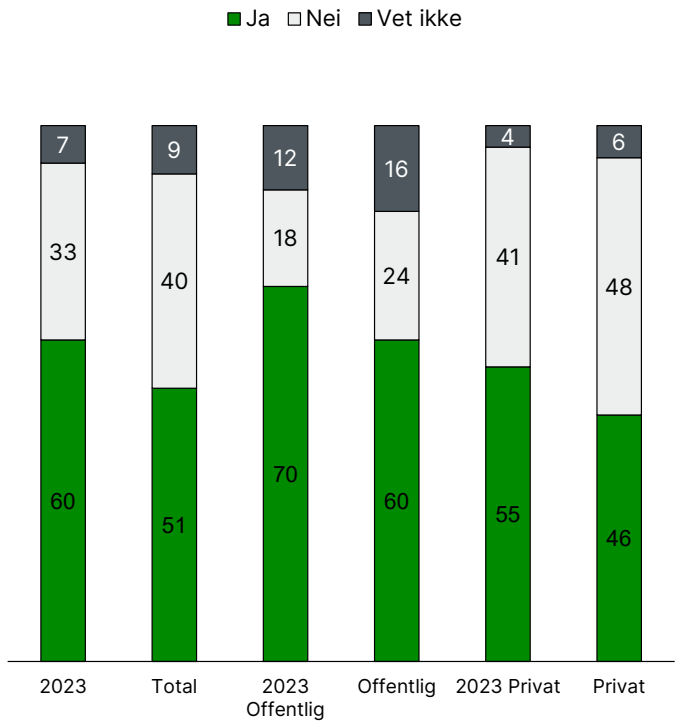
Innenfor bevistgjøring av egne ansatte på IT-sikkerhetsområdet, er trenden den samme, selv om en stor andel av de private svarer at de gjør andre tiltak enn det som ligger i alternativene. E-læring er fortsatt den mest benyttede aktiviteten for bevistgjøring.



Kursing. *Aktiviteter virksomhetene har gjennomført i løpet av de siste 122 månedene for å øke de ansattes bevissthet rundt IT-sikkerhet.*

Forberedelse på krise

I årets undersøkelse oppgir 51 % av de spurte virksomhetene at de har en beredskapsplan dersom de skulle bli utsatt for en sikkerhetshendelse. Basert på fjoråret, ser vi en synkende trend. Erfaringene fra hendelseshåndtererne i Atea Incident Response Team (IRT) tilsier at fjorårets tall nok var noe høyt. Vi spør oss selv om virksomhetene som har svart på undersøkelsen egentlig vet hva som ligger i en beredskapsplan og hva den bør inneholde?



Har virksomheten en beredskapsplan.

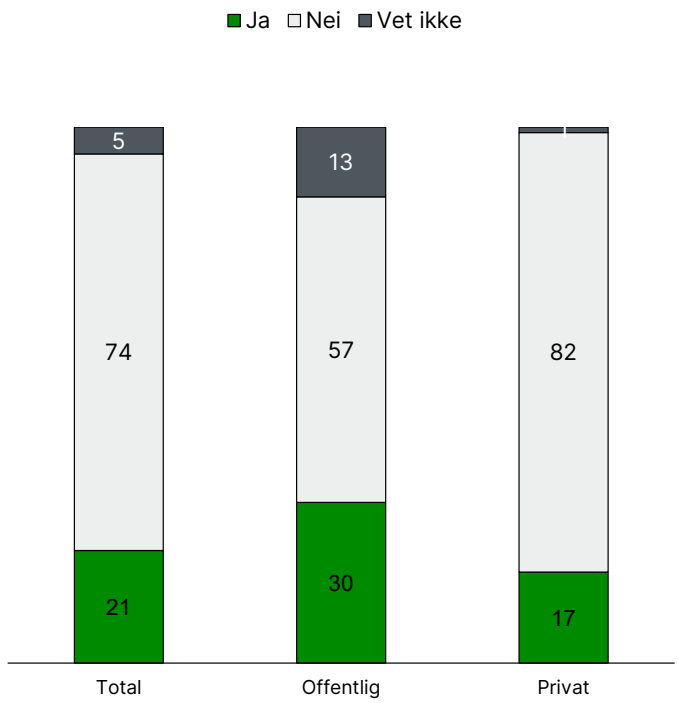
Hva er en beredskapsplan?

Helt konkret er beredskapsplanen en beskrivelse av prosesser og rutiner som skal følges om en hendelse skulle oppstå. Den bør derfor inneholde en totaloversikt over hvem som gjør hva, hvem som skal kontaktes og rutiner for håndtering. Stikkord for en beredskapsplan bør være: Varsling, roller, kommunikasjon og organisering. Husk også å sette av tid og ressurser til å gå gjennom planen for å være kjent med prosessen og sørg for at de som inngår i planen er kjent med sin rolle og hva som forventes av dem.

Om en hendelse skulle oppstå, er det beredskapsplanen som er det styrende dokumentet. Derfor er det viktig at de ansatte i virksomheten har kjennskap til beredskapsplanen og er informert om hva som forventes av dem.

Beredskapsplanen bør gjelde systemene, tjenestene og infrastrukturen som behandler elektronisk informasjon og systemene bør klassifiseres. Detaljeringsgraden i beredskapsplanen bør gjenspeile de ulike systemenes beskyttelsesbehov.

Om en hendelse skulle oppstå, er det beredskapsplanen som er det styrende dokumentet. Derfor er det viktig at de ansatte i virksomheten har kjennskap til beredskapsplanen og er informert om hva som forventes av dem.



Kjøres det øvelser/trenes det på hva man skal gjøre i virksomheten dersom man blir utsatt for en IT-sikkerhetshendelse.

Du må øve

Men selv om man har en beredskapsplan, må man øve/trene på hva man skal gjøre dersom man blir utsatt for en IT-sikkerhetshendelse. I årets undersøkelse oppgir kun 21 % av virksomhetene at de øver på dette. I det private er det 82 % av virksomhetene som ikke øver. Dette kan lett sammenlignes med brannøvelser. Andelen virksomheter som kjører brannøvelser vil vi tippe er mye høyere, men hva kommer det av?

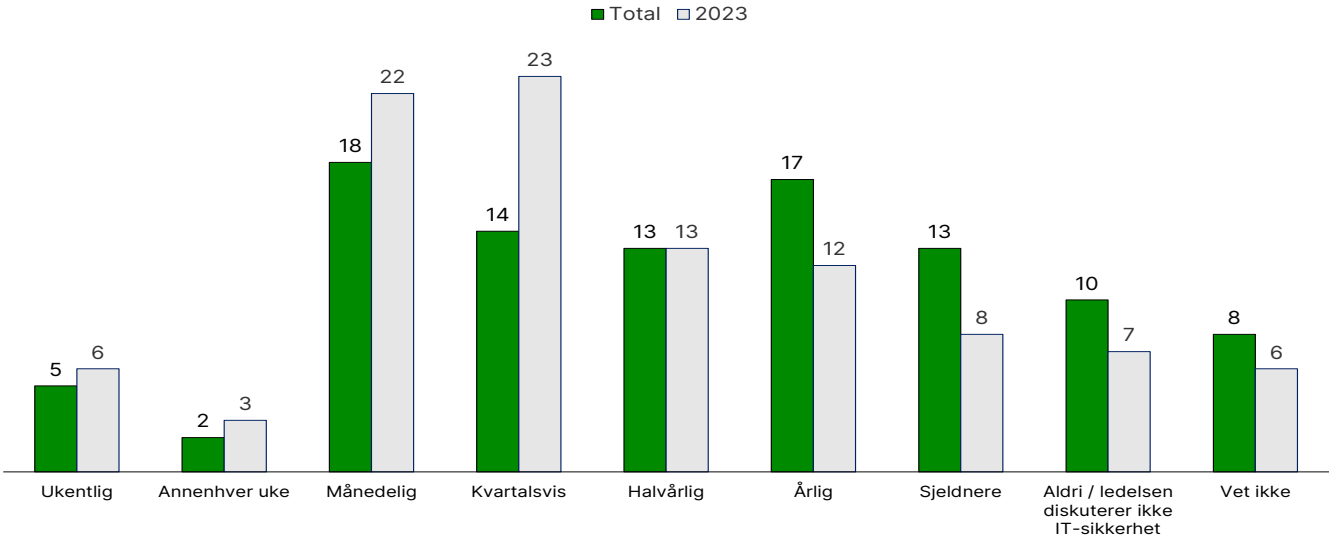
En øvelse kan gjennomføres på ulike måter, men fellestrekkene er at man øver på hva som faktisk skjer ved en hendelse, som for eksempel et ransomwareangrep. En typisk øvelse kan foregå ved at det lages et sett med hendelser og scenarioer som pågår over tid, skreddersydd for virksomheten, som virksomheten med hjelp av beredskapsplanen skal håndtere.

Se for deg følgende scenario

Du oppdager at alt av filer på serverne er kryptert og ingen får tilgang til dem. Temperaturen stiger, og alle kontakter IT-avdelingen. Frykten sprer seg og alle skjønner at dette vil få betydelig innvirkning på hvordan virksomheten skal fungere fremover. Vil du da vite hvor du skal starte? Hvor skal du ringe? Hvem er det som kan ditt system og kan hjelpe til ved en akutt hendelse? Hvem skal gjøre hva? Hvem tar de krevende beslutningene?

Uansett fremgangsmåte, oppfordrer vi at man øver sammen med de personene og/eller leverandørene som typisk blir involvert i en skarp hendelse hos din virksomhet. Det gir et mye bedre samspill når en hendelse oppdages.

Hvor mange ledermøter med IT-sikkerhet som tema gjennomføres i 2024?



Hvor ofte diskuterer ledelsen IT-sikkerheten til virksomheten. *Ledelsen diskuterer IT-sikkerhet betydelig sjeldnere enn i fjor.*

En viktig suksessfaktor for å lykkes med IT-sikkerhetsarbeidet, er å ha et tydelig eierskap i ledelsen. Det er derfor interessant å analysere hvordan dette ansvaret overføres til faktiske agendapunkter i ledelsens møter.

Undersøkelsen viser en tydelig tilbakegang i frekvensen på slike diskusjoner i ledelsen, noe som potensielt kan være en fremtidig sikkerhetsrisiko. Mindre eierskap til sikkerhetsarbeidet i ledelsen fører ofte til manglende kontinuitet i sikkerhetsarbeidet, lavere investeringer og mindre kontroll.

Brekker vi ned tallene og sammenlikner med 2023, tyder det på at det i år blir hele 30 000 ledelsesmøter hvor IT-sikkerhet ikke er på agendaen. Dette vil få konsekvenser for den totale motstandsdyktigheten i Norge. Uten en tydelig sikkerhetsstrategi med forankring i ledelsen, vil arbeidet med IT-sikkerhet hemmes kraftig og utsette virksomhetene for en unødvendig økt risiko.

Med introduksjonen av tydeligere og kraftigere sikkerhetskrav fra EU i form av NIS2, vil vi antakelig se en stor bedring på dette spørsmålet i neste åers undersøkelse.

30 000

30 000 færre ledelsesmøter hvor IT-sikkerhet er på agendaen.


LOCAL TIME
11:34:34
ATTACKS TODAY
357231
TAIWAN
THAILAND
INDONESIA
Solutions
Services
Partners
Support
Resources
ATTACKERS
VIEW FULL

Flere har kjennskap til grunnprinsippene, men færre iverksetter

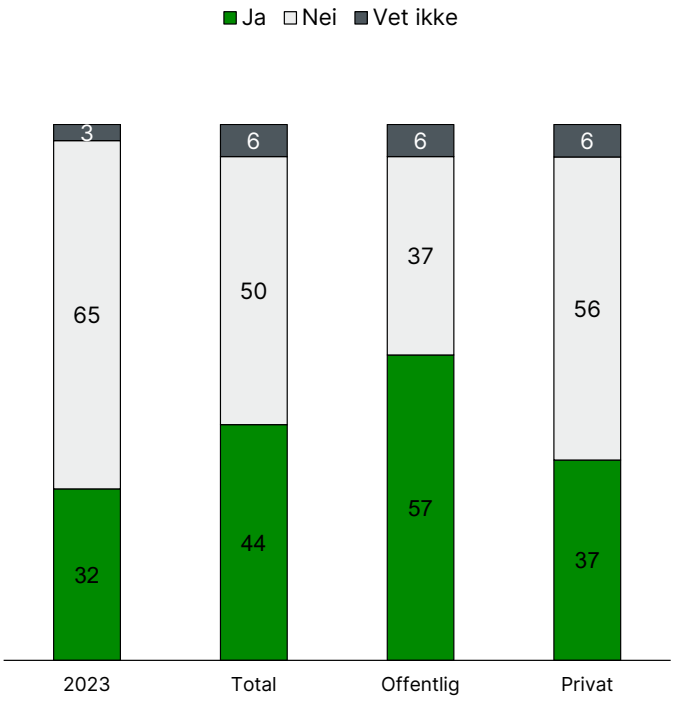
Etter at Nasjonal sikkerhetsmyndighet (NSM) relanserte sine grunnprinsipper i versjon 2.0 tilbake i 2020, har både den kommersielle IT-sikkerhetsbransjen, samt offentlige og private virksomheter, fått en ny renessanse der mange bruker prinsippene som rettesnor i sitt daglige sikkerhetsarbeid. I Atea bruker vi NSMs grunnprinsipper som grunnmuren i alt vi leverer - fra sikkerhetstjenester og løsninger, konsulentoppdrag til intern opplæring av våre medarbeidere.

«NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. De er relevante for alle norske virksomheter».

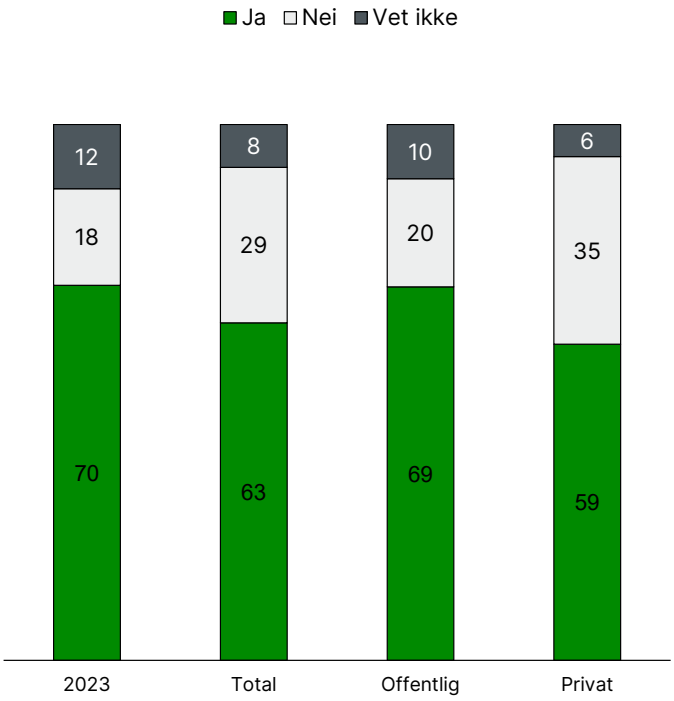
Kjenner til grunnprinsippene

Det er en stor glede for oss å se at flere og flere virksomheter får øynene opp for grunnprinsippene. Undersøkelsen viser at 12 % flere i 2023 har fått øynene opp for grunnprinnsippene sammenlignet med året før. Samtidig er det 7 % færre som har iverksatt tiltak for å implementere grunnprinsippene i egen organisasjon i 2023. Det er vanskelig å si hvorfor tallet stiger på den ene siden, samtidig som det synker på den andre. Svarene viser at det er de små virksomhetene som trekker ned snittet, og at de større virksomhetene har relativt likt resultat som i 2022.

Vi ser også at fokuset offentlig sektor har hatt på IT-sikkerhet, kanskje basert på flere større hendelser omtalt i mediene, også reflekteres i at det er 20 % flere (totalt 57 %) innenfor offentlig sektor kjenner til Grunnprinsippene. Hele 69 % av disse har implementert prinsippene mot 57 % i det private.



Kjennskap til NSM sine grunnprinsipper for IKT-sikkerhet.

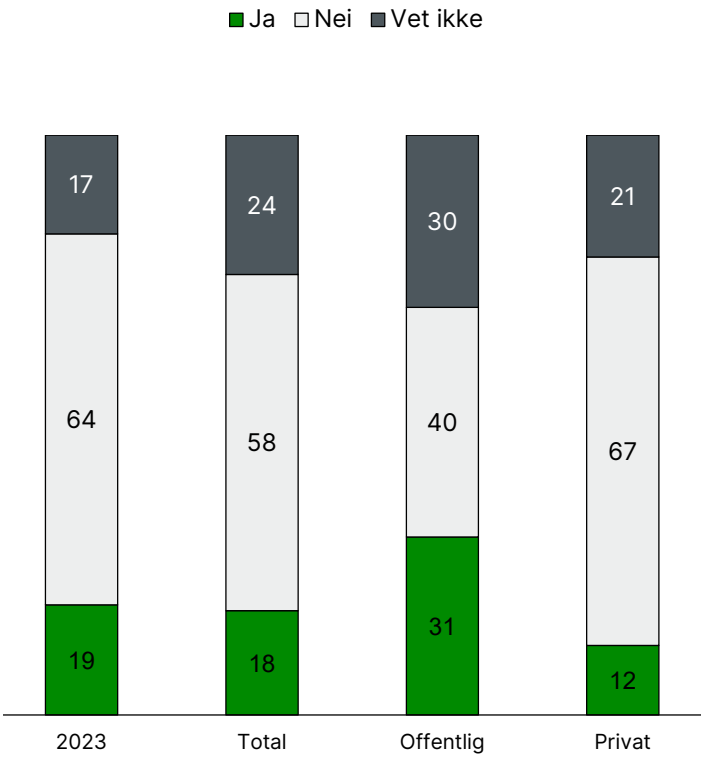


Implementering av NSM sine grunnprinsipper for IKT-sikkerhet.

Støtte fra myndighetene

På spørsmål om virksomhetene opplever at myndighetene har bidratt til å styrke virksomhetens IT-sikkerhet, er tallet fortsatt svært lavt. Totalen for 2022 var 19 %, mot 2023 hvor det nå er 31 % innenfor offentlig som svarer ja. I privat sektor er det ikke mer enn 12 % som sitter med samme opplevelsen. Kanskje det er urettferdig å stille dette spørsmålet. Det lave tallet kan skyldes at myndighetenes ansvar er å ivareta alle virksomheter som går under kritisk nasjonal infrastruktur, mens det er den kommersielle IT-sikkerhetsbransjen som ivaretar alle andre. Vi snakker om en fordeling på 2 % vs 98 % av det totale antallet virksomheter i Norge.

Vår konklusjon på disse resultatene går tilbake på diskusjonen om viktigheten av offentlig/privat samarbeid. Under parolen **#SammenSikrerViNorge** vil vi i den kommersielle IT-sikkerhetsbransjen fortsette med både sikkerhetsfremmende dialoger med alle norske virksomheter og opplysningskampanjer om både samtidstrusselbilde, grunnprinsipper og regulativer.



Har myndighetene bidratt til å styrke virksomhetens IT-sikkerhet.

Hvor mange investerer i cyberforsikring?

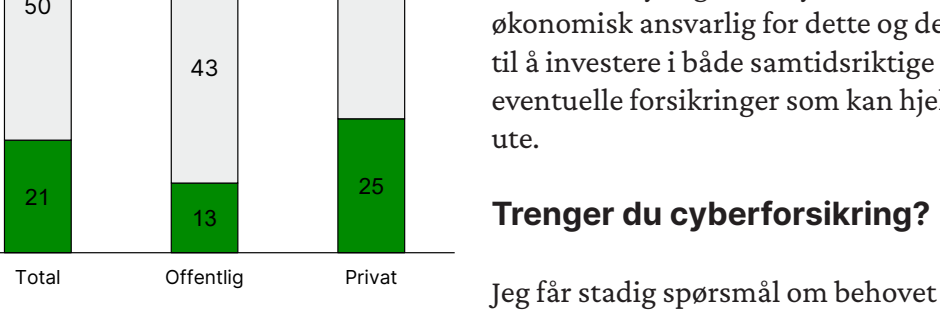
Tallene på virksomheter som invisterer i cyberforsikring stiger, nå har hver fjerde privat virksomhet cyberforsikring. Det er opp 6 prosentpoeng sammenlignet med fjoråret. Håpet er at flere også bruker forsikringen når uhellet er ute, og ikke bare kjøper den.

Vi applauderer alle virksomheter som investerer i cyberforsikring, men stiller samtidig spørsmålet om hvor enkelt det egentlig er å bruke cyberforsikringen når det skjer noe? Vår erfaring er at mange ikke bruker forsikringen fordi de er usikre på hva forsikringen dekker og har manglende logg- og rapporteringsverktøy. I tillegg er det nok mange virksomheter, som i kampens hete, er mer opptatt av å håndtere krisen enn å sjekke forsikringen. Uansett, det er viktig å sette seg inn i hva det er man kjøper, hva det dekker og hvordan man bør agere når uhellet er ute og hackerne inne.

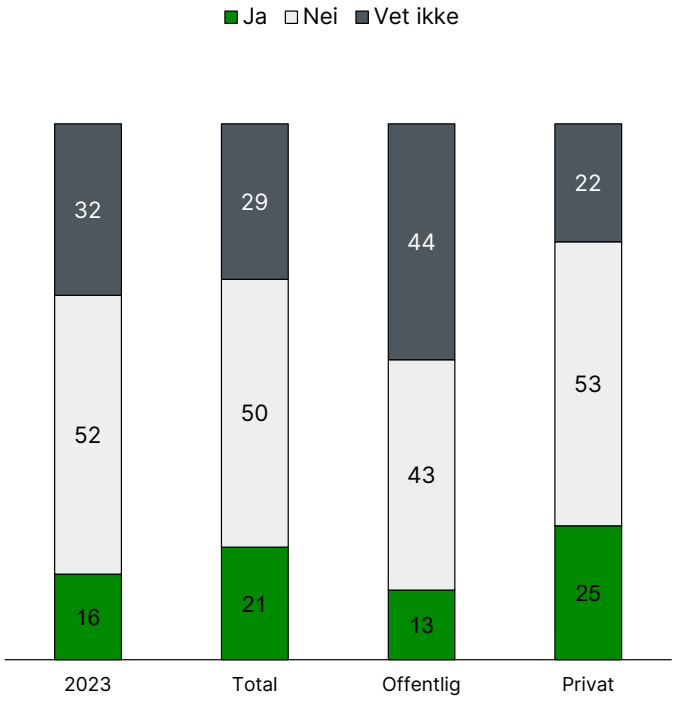
Du blir ikke en bedre sjåfør av å ha trafikkforsikring

Trafikkforsikring er en av få forsikringer som faktisk er påbudt. Ansvarsforsikring, også kalt trafikkforsikring, er en grunnleggende forsikring som alle registrerte biler i Norge er pålagt å ha. Dette er selvfølgelig et pålegg som alle skjønner nytten av, og ikke minst danner grunnlaget for en «kollektiv ansvarsdeling». Der skadelidende får ivaretatt sine rettigheter, og ansvarlige for hendelser blir gjort økonomisk erstatningspliktig i henhold til gjeldende lover og regler.

Ansvarsforsikring er pålagt og en akseptert del av det å ha bil. Selv om du kan velge mellom rimelige varianter som kun dekker ansvar, er det gjerne prisen på bilen, alder, og bruksmønster i kombinasjon med eiers risikoappetitt, som avgjør hva du betaler for forsikringen.



Thomas Tømmernes
Leder IT-sikkerhet
Atea Norge



Har virksomheten cyberforsikring.

Når NSM to år på rad løfter frem underleverandører og verdikjeder som den største digitale trusselen for samfunnet i sine rapporter, bør vi kansje løfte blikket og si at vi som nasjon burde innføre en eller annen form for kollektive kjøreregler for at det skal finnes midler til å løse tvister og dekke skadeomfang på lik linje som pålegget med trafikkforsikring. Virksomheter som blir økonomisk ansvarlige når de bevist eller ubevisst ikke har gjort gode nok tiltak for å være motstandsdyktige mot cyberkriminelle, bør stilles økonomisk ansvarlig for dette og dermed motiveres til å investere i både samtidsriktige løsninger og eventuelle forsikringer som kan hjelpe når uhellet er ute.

Trenger du cyberforsikring?

Jeg får stadig spørsmål om behovet for cyberforsikringer. Ofte om hvilke som er best, erfaringer med bruken, og eksempler på

virksomheter som har hatt eller ikke hatt det. Jeg har vært interessert i cyberforsikringer siden 2015, da Atea sammen med samarbeidspartnere tok cyberforsikringen til Norge. Den gang var det en omstendelig prosess å tegne en cyberforsikring. Virksomheter måtte utføre en «modenhetsanalyse» gjennomført av eksperter på IT-sikkerhet, som avdekket status og gjorde det mulig å kalkulere prisen for forsikringen.

Ønsket virksomhetene en lavere pris, var det bare å utbedre eventuelle feil og mangler. Ønsket de ikke det, ble prisen for forsikringen tilsvarende høy, eller de fikk beskjed om at de ikke var ønsket som kunde. Med andre ord: Høye krav til både kunde og forsikringsselskap. Men mye har endret seg siden den gangen.

Automatiserte løsninger

I dag finnes det et bredt spekter av cyberforsikringer å velge i. Trenden har gått fra eksklusive forsikringer satt sammen av markedets beste leverandører, til mest mulig automatiserte løsninger. Der forsikringssekapene gjør en enklere vurdering av virksomhetene kombinert med at de som vil tegne en cyberforsikring, selv krysser av for hvilke tiltak de har gjort for å være motstandsdyktige mot samtidstrusselbilde. Dette gjør selvfølgelig forsikringene mye rimeligere. Samtidig leter forsikringsselskapene etter enklere tjenester for å kunne levere hjelp om en forsikret virksomhet blir kompromittert.

Det med liten skrift

Om man kolliderer med bil, er det relativt enkelt å bruke lovverket i kombinasjon med vei og føreforhold for å avgjøre både skyld og utbetaling. Alle skjønner det vil bli en avkortning i utbetaling om man kjører med sommerdekk på vinterføre.

Slik er det ikke i det digitale landskapet. Her er trusselbildet langt mer uklart. Selv om en løsning er sikker i dag, kan det være så enkelt at noen glemmer å oppdatere en brannmur - og vipps, så er IT-kriminelle på innsiden.

Så hvor enkelt er det å bruke cyberforsikringen når det skjer noe? Vår erfaring er at mange ikke bruker forsikringen fordi de er usikre på hva forsikringen dekker og har manglende logg- og rapporteringsverktøy. I tillegg er det nok mange virksomheter, som i kampens hete, er mer opptatt av å håndtere krisen enn å sjekke forsikringen. Uansett, det er viktig å ha sette seg inn i hva det er man kjøper.

Hva hadde jeg gjort selv?

Det er litt avhengig av hvilken type virksomhet jeg hadde ledet. Hadde jeg hatt en virksomhet med kontroll på egen IT-sikkerhet, med tydelige beredskapsplaner, logg og rapporteringsverktøy, så ville jeg investert i en cyberforsikring. Den burde dekket hendelseshåndtering, jurist og kommunikasjon. Samt opprydding og tilbakestilling av egen IT-løsning og eventuelle skader min løsning kunne ha påført samarbeidspartnere.

Hadde jeg hatt en liten eller middels virksomhet, ville jeg heller ha investert i en god styreromsforsikring. Den burde dekket hendelser og tap. Resten av pengene ville jeg ha lagt i en full driftet sikkerhetsløsning, som inkluderer logginnsamling, overvåking og respons på hendelser om uhellet skulle være ute. Det finnes flere dyktige leverandører av dette i det norske markedet.

Kunstig intelligens og sikkerhet

Petter Moe
Chief Technology Officer
Atea Norge

Kunstig Intelligens (AI) er den sterkeste IT-trenden akkurat nå siden generativ AI dukket opp i media i november 2022. Det er ingen ting som tyder på at det kommer til å gå over snart. Mange trender kommer og går; det er veldig vanskelig å forutse hvilke som har kraft og timing til å medføre varig endring. AI har vært på banen flere ganger før – kanskje er denne gangen annerledes, slik at vi kommer til å jobbe og leve på andre vis enn vi gjorde før?

Så hva ville det medføre? Når vi ser på hva AI gir oss av muligheter er det et kaotisk villnis. Eller er det egentlig slik? La oss bryte ned:

Type: Mye av oppmerksomheten akkurat nå kommer fra generativ AI (GenAI). Det er det gode grunner for, siden det er så spektakulært. Men fremskrittene her bygger på underliggende maskinlæring (ML) i mange tilfeller, som har vokst frem over mange år. Dette begynner å bli et modent fagfelt, brukes bredt i mange bransjer, og forutsetter datakvalitet.

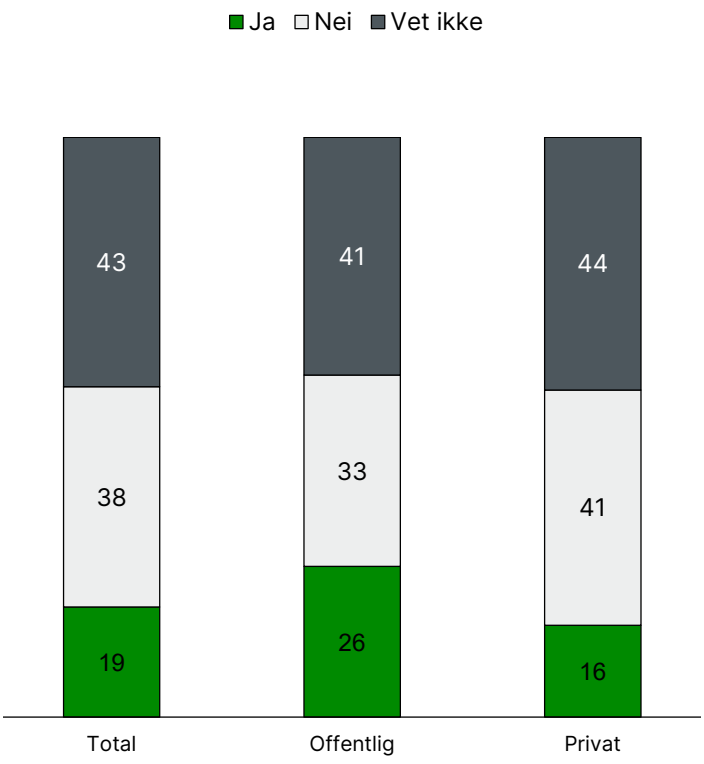
Finansinstitusjoner har brukt ML i mange år, kanskje har de kunnet innta en ledende posisjon fordi den bransjen alltid har hatt fokus på datakvalitet. De er allikevel forsiktige med GenAI, siden konsekvensene ved feil er vanskelige å overskue.

Bruk: Gartner skiller mellom «everyday AI» og «gamechanging AI», og sier at rundt 80 % av investeringene i dag er i området «everyday AI». Definisjonen er at dette er tilpasninger av hvordan vi løser oppgaver vi allerede har, som resulterer i mindre endringer heller enn revolusjoner. Ikke undervurder dette – om konkurrentene dine henter noen prosenter effektivitet i året som du ikke tar ut gjør det vondt over tid. Men «gamechanging AI» er den andre kategorien, hvor man skaper nye produkter eller markeder, eller gjør ting fundamentalt annerledes.

Like før jul annonserte Channel1.ai en ny tilnærming til nyheter, hvor presentasjonen av nyhetene skulle gjøres av AI-generert personell – avatarer. Dette ville øke deres evne til å generere relevante, personlig tilpassede nyheter, og samtidig redusere produksjonskostnaden til noen få prosent av tidligere. Dette ville være en«gamechanger». Samtidig er det viktig å påpeke at siden denne lanseringen har det vært helt stille om initiativet, så det er vanskelig å vite om det skjer, og ikke minst om det ville lykkes.

Kompetansenivå: Er AI flink, eller er det bare praktisk ikke å måtte gjøre jobben selv? Her ser vi begge deler – på spissede fagdomener kan AI allerede gå i dybde på en måte som mennesker ikke kan, eller ikke har tid til. En menneskelig lege kjenner ikke til alle mulige diagnoser – AI har ikke slike begrensninger. En menneskelig revisor kan vanskelig gå gjennom alle regnskaper for alle deler av en stor virksomhet i detalj, AI har nærmest uendelig kapasitet. Men samtidig ser vi at menneskelig evne til skjønn eller sunn fornuft gir en håndtering av usikkerhet som maskiner ikke har.

En av de første som ble påkjørt og drept av en selvkjørende bil var Elaine Herzberg. Hun dyttet en sykkel full av handleposer over en firefelts motorvei, og et testkjøretøy fra Uber skjønte intet av denne situasjonen, siden den ikke var observert tidligere. Et menneske ville trolig ha reagert annerledes.



Utgjør kunstig intelligens en IT-sikkerhetsrisiko for virksomheten.

AI har flere konsekvenser for sikkerhet

Angrepssystemene blir raskere og mer presise. Når all verdens sårbarheter er tilgjengelig for angripende AI, og den samtidig ser alle mulige angrepsflater i sann tid, kan du ikke lenger regne med å ha flaks, og ikke bli angrepet. Patching må være automatisk, flerfaktor må være implementert over alt, og du må ha forsvar i dybde. Virksomheter som ikke tar dette på alvor kommer til å slite veldig snart. Denne rapporten viser at mange har sett behovet for å investere mer i sikkerhet i 2023 enn de hadde budsjettert med – det vil være billigere å investere i forkant enn å reparere i etterkant.

Sosial engineering via AI vil bli umulig å kjenne igjen. NSM sier også dette i sin siste rapport «Risiko 2024». Angrepene vil bli så troverdige at opplæring ikke er nok. Du må ha mekanismer i bakkant som gjør at katastrofen unngås selv om du tror det var sjefen din som ringte, eller du klikker på feil lenke – for det kommer til å skje.

Noen angrep vil lykkes! Alle virksomheter må anta at noen angrep lykkes, og planlegge og trene på å komme tilbake etter at det har skjedd. Beredskapsplaner, øvelser, risikoanalyser – tiltakene er kjente, men koster tid og penger.

Samtidig gir AI også noen fordeler innen sikkerhet

Generering av konfigurasjon. Mange sikkerhetsmekanismer er komplekse, med sterke avhengigheter mellom forskjellige komponenter. Etter hvert som AI integreres i produktene ser vi allerede at mer av konfigurasjon og oppsett gjøres generativt, med bedre granulering og mindre feil.

Bedre automatisert testing. Det kommer nå produkter som i større grad ser hele infrastrukturen, og kan simulere angrep. Mye av dette var før manuelt arbeid, begrenset av kost og tid, og kan nå skalere bedre. (Samtidig er det viktig å påpeke at cyberkriminelle også automatiserer, så angrepene blir også mer effektive.)

Prediksjon. I et kanadisk sykehus var man i stand til å redusere sykehusinfeksjoner med 74 % ved å predikere hvor det var mest sannsynlig at det oppsto. På samme måte kan man nå bruke GenAI prediksjon til å forutsi angrep, og derved forbygge.

Så hva er konklusjonen? Muligheter og utfordringer med AI innen sikkerhet ligner mye på muligheter og utfordringer med AI generelt:

- Det går fort, den som ikke engasjerer seg blir fort hengende etter.
- Det er store muligheter, men de er ikke modne og ferdige, så det er ikke gitt hvilke som lykkes.
- Du vil ikke gå glipp av «everyday» muligheter og forbedringer.
- Ingen vet hvor «gamechanging AI» endrer markedet totalt, så vær forberedt på store og raske endringer!

ATEA

atea.no/it-sikkerhet/

sikkerhet@atea.no