Bevissthet og beredskap

Atea sikkerhetsrapport 2023

INNHOLD

INTRODUKSJON

Thomas Tømmernes
Leder IT-sikkerhet
Atea Norge

Denne rapporten bygger på en undersøkelse gjort tidlig i 2023, blant et representativt utvalg av daglige ledere og IT-ansvarlige i virksomheter godt spredt både geografisk, bransjemessig og i størrelse.

Vi planlegger at dette skal bli en årlig affære, en slags «State of the Union» for å kartlegge hvordan det ligger an med IT-sikkerheten i det ganske land. Beklageligvis er funnene i undersøkelsen omtrent som forventet. Det står ikke bra til, og dette må vi agere på før det er for sent.

Jeg liker ikke å drive med skremselspropaganda, men her er tallenes tale klar:
Norske virksomheter, og dermed samfunnet som helhet, er for dårlig forberedt. Vi trenger handling, og ikke minst samhandling, på tvers av privat og offentlig sektor for at Norge skal kunne gå det fremtidige trusselbildet i møte.

#SammenSikrerViNorge

UTVALG

- **Intervjumetode:** Telefon- og webintervju
- **Antall intervju:** 610
- **Periode datainnsamling:** Januar-mars 2023
- **Målgruppe:** Daglig leder/ansvarlig for IT/IT-sikkerhet i norske bedrifter med 10-350 ansatte
- **Populasjon:** Det er omtrent 63 500 virksomheter i Norge med 10-350 ansatte

I årets Bevissthet og beredskap hadde vi totalt 610 respondenter. Dette fordelte seg som 334 daglige ledere og 276 ansvarlige for IT-sikkerhet i offentlige og private virksomheter. Vi fordelte oss godt utover det langstrakte land, der 100 Oslo-baserte virksomheter, 208 fra østlandet, 136 fra sør- og vestland, 100 fra midt-Norge og 66 fra Nord-Norge besvarte årets undersøkelse. Det var også jevnt fordelt mellom små-, mellomstore og store virksomheter, både i omsetning og antall ansatte.

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

TRUSSELBILDET

“Vi har sett en tydelig økning i trusselnivået de siste årene. Det kan være alt fra phishingforsøk via e-post eller sms og passord som er på avveie, til større hendelser som faktiske løsepengeangrep der uvedkommende har vært på innsiden i dages- eller ukesvis før angrepet oppdages.

Vi som jobber med kritisk hendelseshåndtering etter f.eks hackerangrep (IRT), kan faktisk melde om en tredobling av antall hendelser i år, sammenlignet med i fjor.”

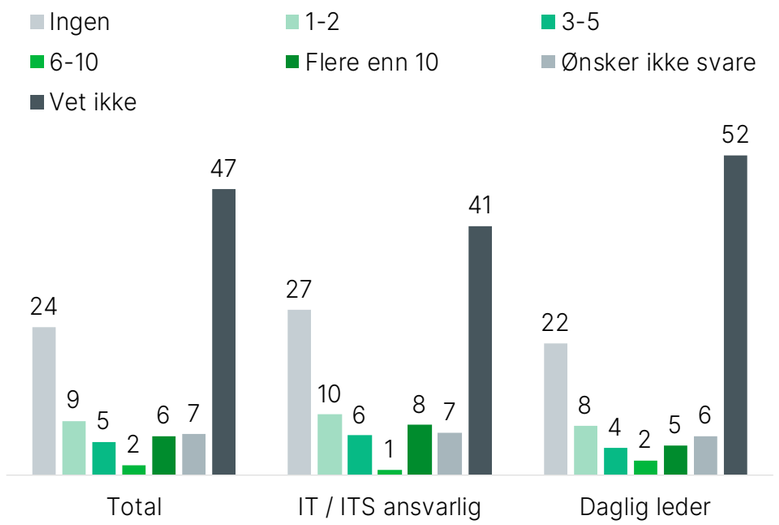
Vegard Kjerstad
Leder Incident Response Team (IRT)
Atea Norge

VI ER LYKKELIGE UVITENDE

Verden opplever stadig et svært komplisert trusselbilde. På tross av dette melder flere norske virksomheter om få eller ingen sikkerhetsbrudd de siste tolv månedene.

Potensielle sikkerhetsbrudd

Hvor mange kritiske hendelser har systemene fanget opp i løpet av de siste 12 månedene?



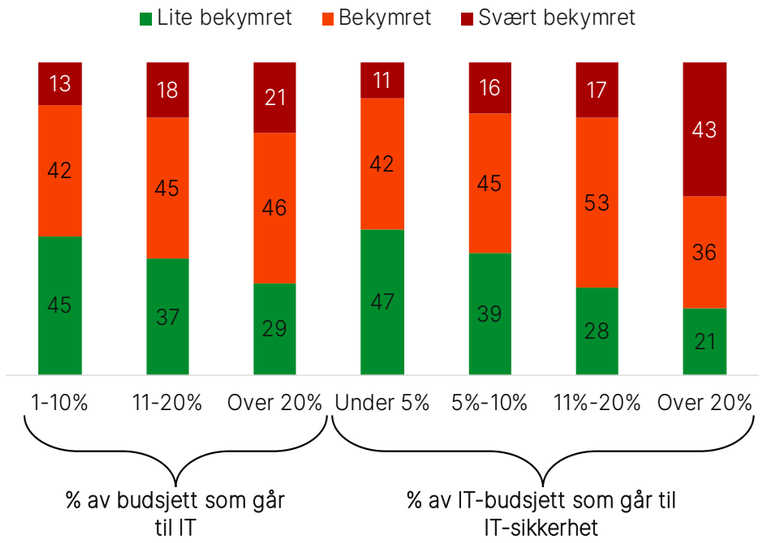
Et alarmerende høyt antall vet ikke om de har vært utsatt for et sikkerhetsbrudd.

ØKT INVESTERING GIR ØKT BEKYMRING

Kunnskap er makt, så også i norske virksomheter. Jo større investeringene i sikkerhet er, jo større er bekymringen for sikkerhetsbrudd. Lav kompetanse fører til at for få skjønner hvor utsatt de er for cyberangrep.

Bekymret for IT-sikkerhetsbrudd – avh. av investeringer

I hvilken grad er du bekymret for at virksomheten skal bli utsatt for et IT-sikkerhetsbrudd?



Bekymring for sikkerhetsbrudd og andelen av budsjett som går til IT/IT-sikkerhet henger sammen – jo større budsjett, jo større bekymring.

VI STOLER PÅ VÅRE EGNE, ELLER?

Over halvparten av de spurte virksomhetene opplever verden utenfor som trusselen. De ansatte er ofrene. Imidlertid er det også en stor gruppe som bekymrer seg for brukerfeil (41 %). Her ser vi en markant forskjell mellom privat og offentlig sektor, der privat faller inn under første gruppe, mens det offentlige ligger i andre gruppe.

Det er også stor forskjell på hva daglig leder og IT-ansvarlig ser på som den største trusselen. Daglig leder virker å ha større tillit til sine ansatte, mens 49 % av IT-ansvarlige svarer at brukerfeil er den største risikoen. Men hva legger virksomhetene egentlig i «brukerfeil»? Her kan det være store forskjeller fra virksomhet til virksomhet, og respondent til respondent.

Ateas Incident Responce Team (IRT) har sett en tredobling av antall hendelser i år, sammenlignet med i fjor.

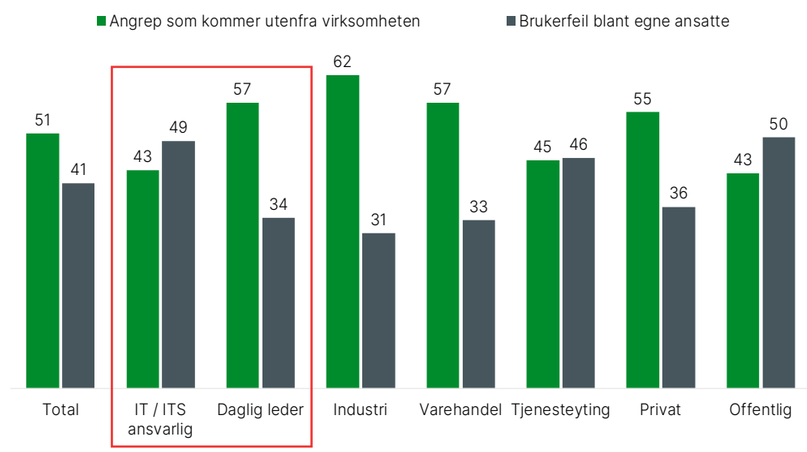
Hvilke hendelser har virksomheten vært utsatt for?

Har virksomheten vært utsatt for følgende IT-sikkerhetsbrudd de siste 12 månedene?

Phishing og brukerfeil er fortsatt hovedandelen av hendelser.

Hvor er det størst risiko?

På hvilke av følgende områder anser virksomheten at det er størst risiko for at det kan skje en IT-sikkerhetshendelse?



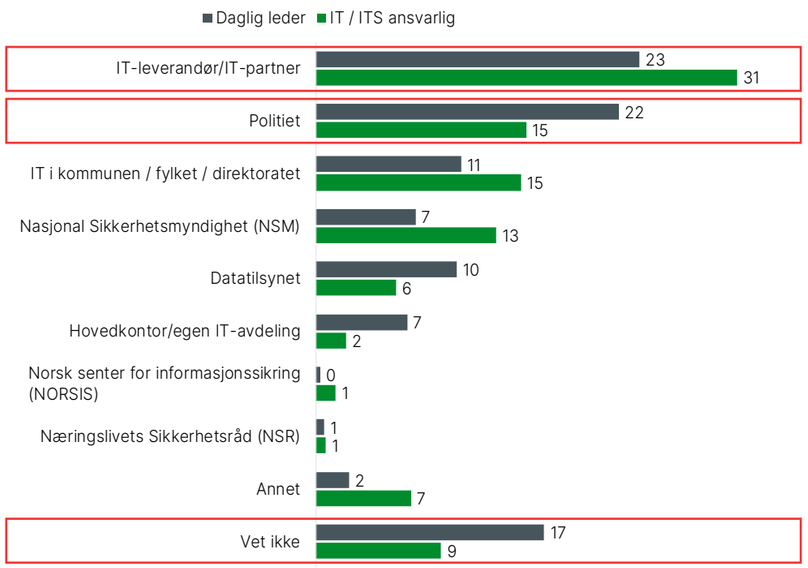
Daglige ledere har større tillit til egen ansatte, og frykter angrep utenfra i større grad. IT-ansvarlige mener risikoen for brukerfeil blant egne ansatte er den største faren.

STORE SPRIK I HVEM VIRKSOMHETENE KONTAKTER

Det er stor variasjon i sikkerhetsbruddene, derfor er det store forskjeller i hvem virksomhetene kontakter.
For få virksomheter vet hvor de skal ringe. Her har samfunnet en stor informasjonsjobb foran seg, og større samarbeid mellom det offentlige og private er essensielt for økt kompetanse.

Hvem ringes når en opplever et IT-sikkerhetsbrudd?

Dersom virksomheten skulle oppleve et alvorlig IT-sikkerhetsbrudd - hvilken aktør/instans ville dere kontaktet først for å få hjelp?



Én av fire sier de vil ringe sin IT-leverandør dersom de opplever et alvorlig IT-sikkerhetsbrudd. Nesten én av fire sier de ville ringt politiet, mens 13 % svarer at de ikke vet hvem de hadde ringt.

SIKKERHETSKULTUR

“De fleste virksomheter ville hatt stor nytte av en modenhetsanalyse for å få kartlagt IT-sikkerheten. Dette for å tenke mer helhetlig rundt informasjonssikkerhet, og for å finne ut hvilke tiltak de skal prioritere først.”

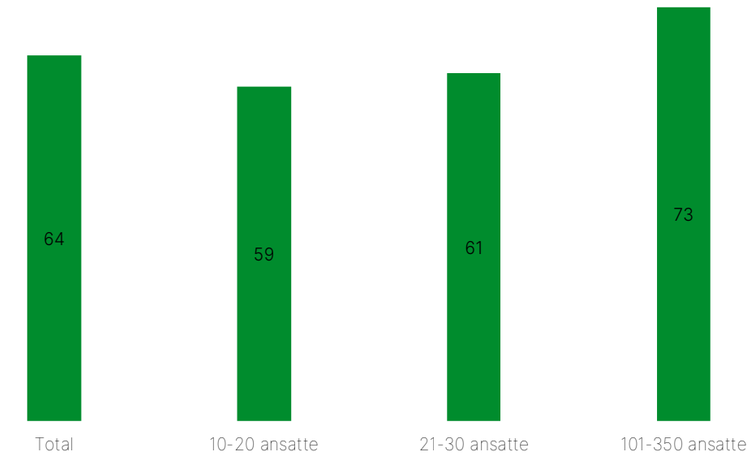
Vegard Kjerstad
Leder Incident Response Team (IRT)
Atea Norge

ALLTID BEREDT?

De store virksomhetene og det offentlige går foran med størst fokus på IT-sikkerhet. Det er derimot verdt å merke seg at norsk industri skiller seg negativt ut. Norske industrivirksomheter sitter ofte på viktig kunnskap og teknologi som kan være interessant for aktører som ikke skal ha tilgang på informasjonen.

Fokus på IT-sikkerhet

I hvilken grad vil du si at virksomheten har fokus på IT-sikkerhet?



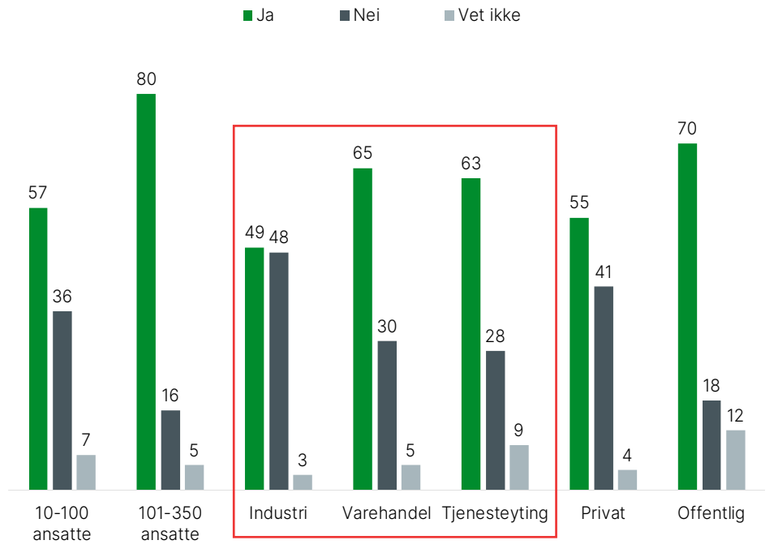
De små virksomhetene fokuserer i mindre grad på IT-sikkerhet.

STORE FORSKJELLER

Én av tre virksomheter har ikke beredskapsplaner. Dette er helt grunnleggende å ha på plass. Særlig bekymringsfullt er det at industrien og de minste virksomhetene skiller seg negativt ut.

Beredskapsplan

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



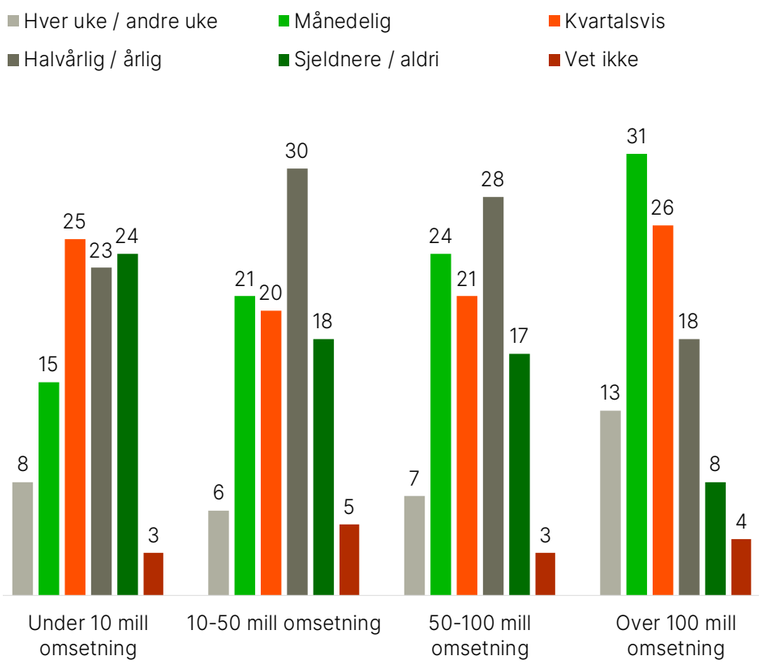
På tvers av bransjene så har industri langt større andel som ikke har en beredskapsplan enn i varehandel og tjenesteyting. I virksomheter som har en beredskapsplan, svarer nesten én av tre at ansatte kun i liten/svært liten grad er kjent med beredskapsplanen.

VI DISKUTERER!

Vi har fortsatt et komplisert trussebilde, og det er store forskjeller i hvor ofte ledergrupper diskuterer sikkerhet i norske virksomheter. De største virksomhetene har de største økonomiske musklene og skiller seg kraftig fra de mindre hva gjelder hyppighet. Men hva diskuteres?

Diskutere IT-sikkerhet i ledelsen

Hvor ofte diskuterer ledelsen IT-sikkerheten til virksomheten?



Generelt viser svarene at jo høyere omsetning virksomhetene har, jo oftere diskuteres IT-sikkerhet i ledelsen

KUNNSKAP

“Vi står i en kompetansekrise. Mange virksomheter har manglende bevissthet rundt helt grunnleggende tiltak. Kompetanse er selve grunnsteinen for å redusere risiko og håndtere sikkerhetsbrudd.”

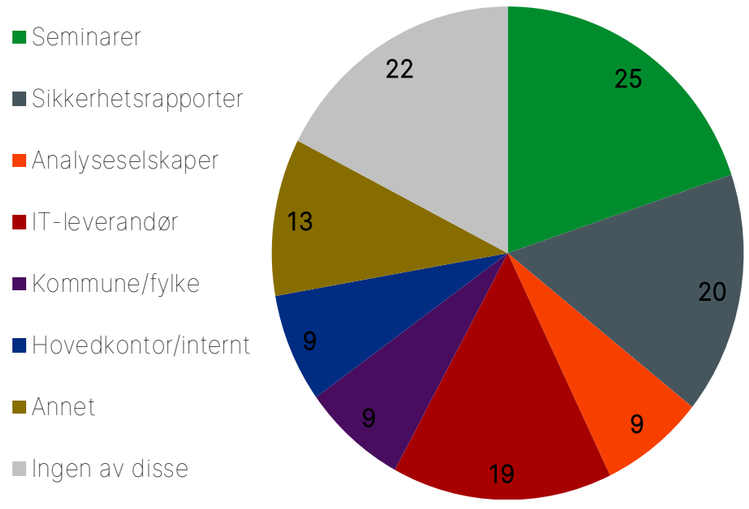
Thomas Tømmernes
Leder IT-sikkerhet
Atea Norge

KOMPETANSEKRISE

Vi vet i dag at det mangler 1900 fagspesialister innen IT-sikkerhet. I 2030 har dette antallet steget til 4200, og norske virksomheter står overfor en kompetansekrise. På grunn av dette anbefaler Nasjonal sikkerhetsmyndighet (NSM) og norske myndigheter at virksomheter kjøper inn denne kompetansen fra leverandører som kan faget. Dette gjenspeiler seg i resultatene i denne undersøkelsen, der hele 19 % svarer IT-leverandør på spørsmål om hvor de henter kunnskap fra.

Søke kunnskap

Hvor søker du kunnskap til eget sikkerhetsarbeid?

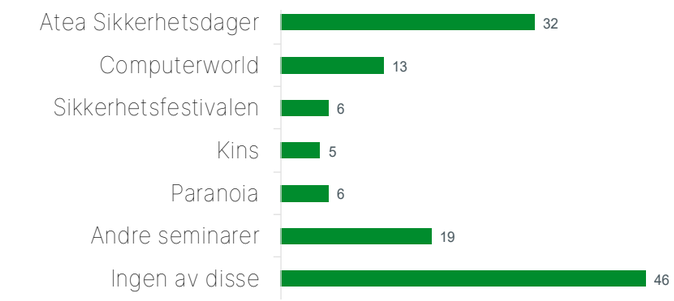


25 % henter kunnskap fra seminarer, 20 % fra sikkerhetsrapporter som denne og 19 % fra IT-leverandør.

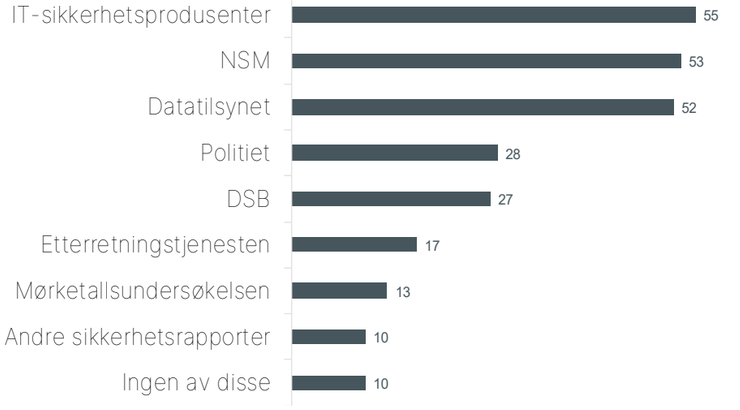
VI MÅ TILGJENGELIGGJØRE KUNNSKAP

IT-sikkerhetsleverandører har topp-kompetanse på det dynamiske trusselbildet, trusselaktører, risiko og tekniske løsninger. Det må vi kunne for å levere det norske virksomheter trenger i kampen mot hackerne. Dette ser vi norske virksomheter er klar over i årets resultater fra undersøkelsen. Atea sikkerhetsdager og rapporter fra IT-leverandører er, sammen med rapporter fra NSM og Datatilsynet, der flest henter kunnskap. Vi har derfor et stort ansvar for å tilgjengeliggjøre kunnskap for norske virksomheter.

Seminarer:



Sikkerhetsrapporter:



Analyseselskaper:

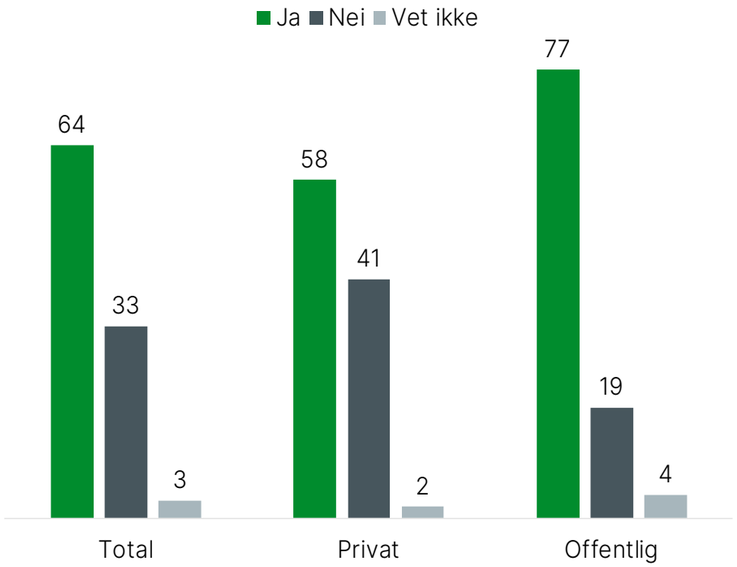
Det er til IT-leverandørene eller det offentlige norske virksomheter ser for å skaffe kompetanse.

BEHOV FOR ØKT BEVISSTHET

Det er lav grad av investering for å øke ansattes kunnskap. Spesielt flere private virksomheter bør tilby kurs og kompetanseheving for å møte et digitalt trusselbilde med økende grad av profesjonalisering og større omfang enn noen gang.

Kursing

Har virksomheten i løpet av de siste 12 månedene gjennomført aktiviteter som øker de ansattes bevissthet rundt IT-sikkerhet?



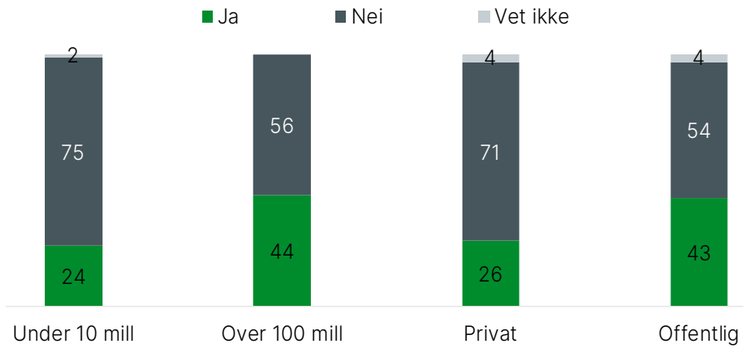
Én av tre virksomheter har ikke gjennomført aktiviteter som øker de ansattes bevissthet rundt IT-sikkerhet i løpet av de siste tolv månedene. Det er større fokus på slike aktiviteter i offentlige virksomheter enn i private.

FOR LAV KJENNSKAP TIL NASJONAL SIKKERHETSMYNDIGHET (NSM) SINE GRUNNPRINSIPPER

To av tre melder at de har liten eller ingen kjennskap til Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IT-sikkerhet. Dette er skremmende da disse burde være pensum både hos ledelsen, og ikke minst, hos IT-ansvarlige i alle landets virksomheter.

Nasjonal sikkerhetsmyndighets (NSM) Prinsipper

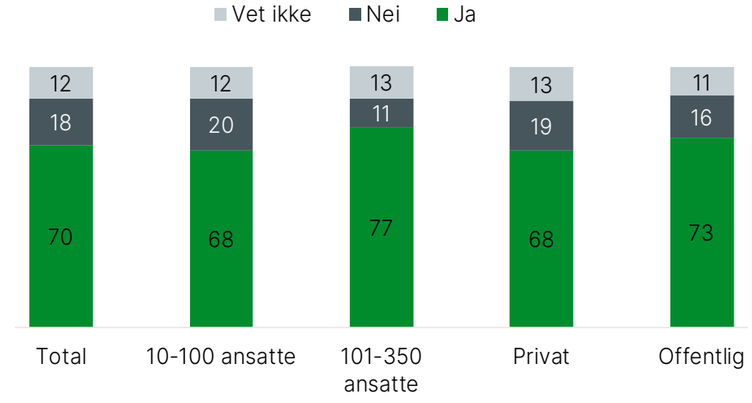
Kjenner du til grunnprinsippene til Nasjonal sikkerhetsmyndighet (NSM) for IT-sikkerhet?



Andelen er høyere i offentlig sektor enn i privat, og i privat sektor er andelen høyere jo flere ansatte eller høyere omsetning virksomheten har. Jo større virksomhet, jo større kjennskap til grunnprinsippene.

Implementering av Nasjonal sikkerhetsmyndighets (NSM) prinsipper

Har dere implementert grunnprinsippene til Nasjonal sikkerhetsmyndighet (NSM) i deres drift?



Når de først kjenner grunnprinsippene implementeres de i driften.

INVESTERING

“Skal virksomhetene henge med i den komplekse sikkerhetssituasjonen, må det gjøres investeringer, både i mennesker, opplæring og IT-systemer.”

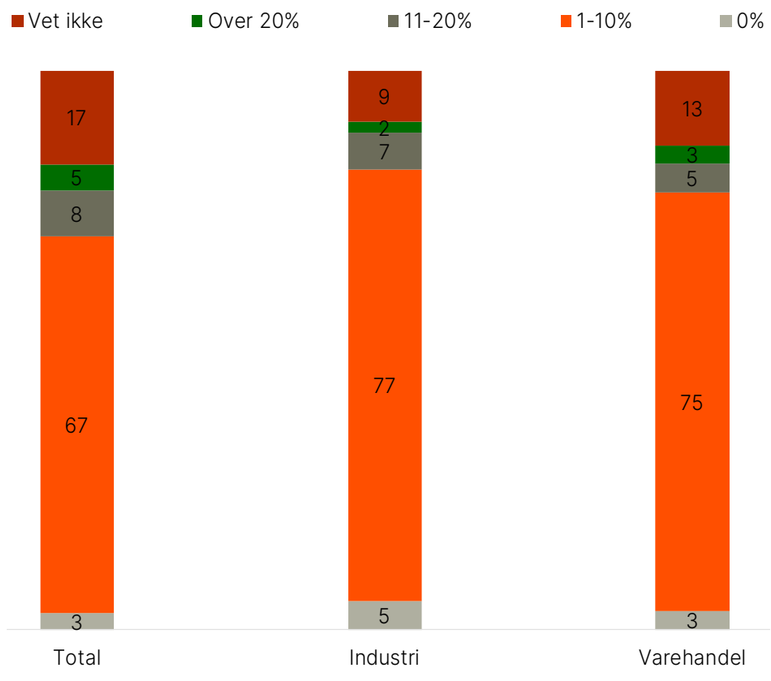
Thomas Tømmernes
Leder IT-sikkerhet
Atea Norge

INVESTERINGER I IT-SIKKERHET

De aller fleste virksomhetene melder at de har fokus på sikkerhet, men hvordan tas dette videre uten investering? Det kan se ut til at sikkerhet må prioriteres innen allerede eksisterende budsjett. Virksomheter som bruker større del av totalt budsjett på IT, bruker også mer på IT-sikkerhet.

IT-budsjett

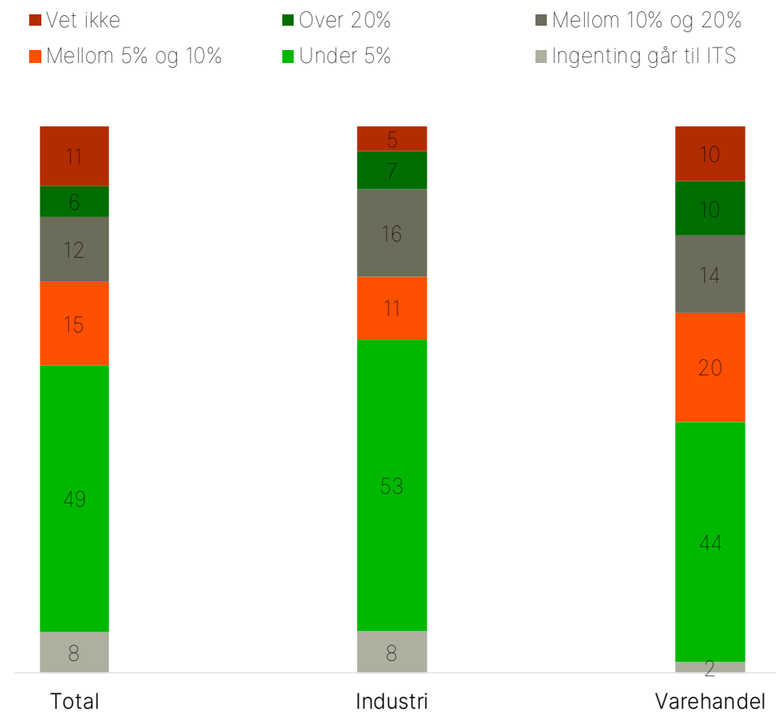
Omtrent hvor stor andel av virksomhetens budsjett går til IT?



Seks av ti norske virksomheter bruker under 10% av investering på IT til IT-sikkerhet. Virksomheter som bruker større del av budsjettet på IT som helhet, prioriterer også IT-sikkerhet i større grad.

IT-sikkerhetbudsjett

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



Norske virksomheter legger generelt sett en lav andel av IT-budsjettet på IT-sikkerhet.

FÅ PLANER OM Å RUSTE OPP

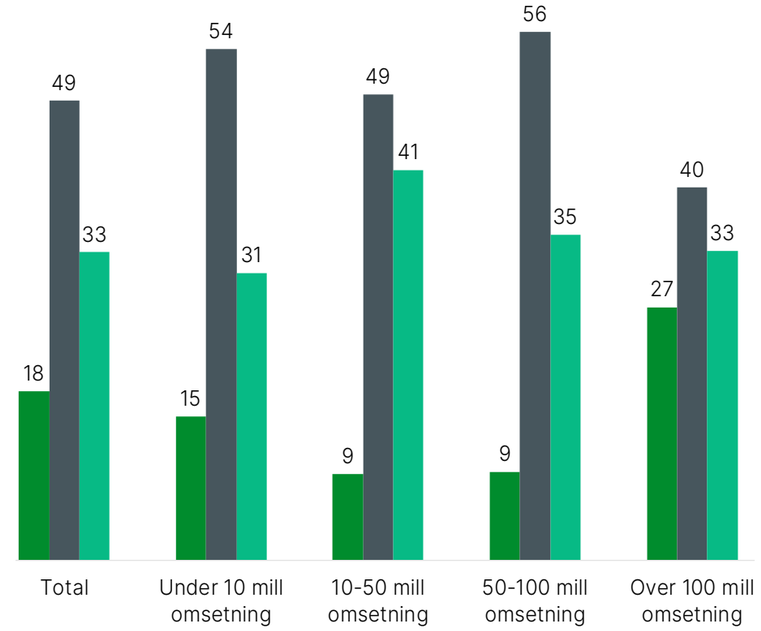
Når viljen til investering er lav, og kompetansen mangler - hvordan skal vi vite hva vi ikke vet? Kompetanse er helt grunnleggende for å redusere risiko og håndtere sikkerhetsbrudd.

Tallene viser at norske virksomheter er lite forberedt på det komplekse trusselbildet. Tre av fire sier de ikke vet om de vil, eller ikke vil øke investeringene i IT-sikkerhet de neste tolv månedene.

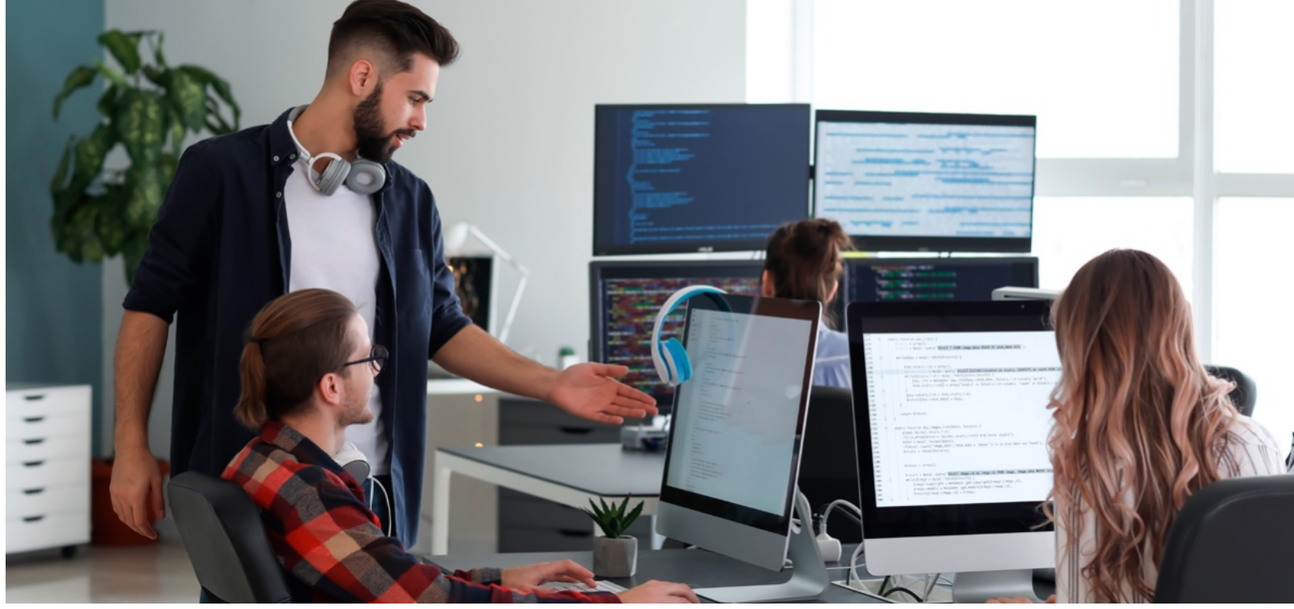
Det er et alarmerende høyt antall, faktisk over halvparten av norske virksomheter, som ikke har egne ansatte som jobber med IT-sikkerhet.

Egne IT-ansatte

Har virksomheten egne ansatte hvor hoveddelen av arbeidsoppgavene omhandler IT-sikkerhet?

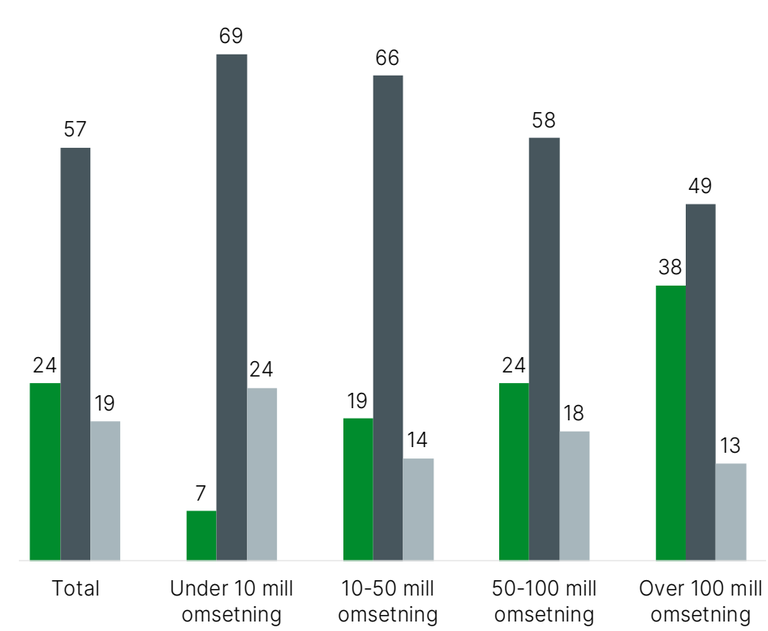


Halvparten av norske virksomheter har ingen dedikerte ansatte som jobber med IT-sikkerhet.



Investering i IT

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



Tre av fire virksomheter vil ikke, eller vet ikke om de vil øke investeringene i IT-sikkerhet de neste tolv månedene.

SAMARBEID

“Myndighetene har nylig fått sterk kritikk fra Riksrevisjonen. Virksomhetene opplever at de er overlatt til seg selv.”

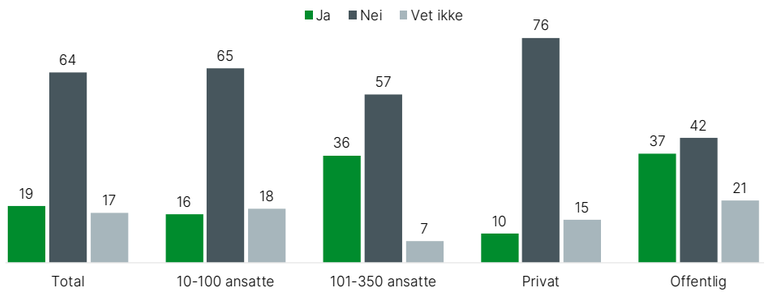
Thomas Tømmernes
Leder IT-sikkerhet
Atea Norge

#SAMMENSIKRERVINORGE

Vi mangler helhetlig styring og koordinering av IT-sikkerhet på tvers av offentlig og privat sektor, for best mulig å ruste Norge til å møte fremtidens digitale trusselbilde. Her må myndighetene på banen, og oppnevnelsen av en digitaliseringsminister er en god begynnelse. Ved å jobbe sammen kan vi skape et mer sikkert digitalt samfunn. Vi kan redusere risikoen for IT-angrep, beskytte data og informasjon, og sikre at samfunnets digitale systemer er robuste. I vår undersøkelse svarte nesten to av tre at de ikke følte at myndighetene hadde bidratt til å styrke virksomhetens IT-sikkerhet.

Støtte fra myndigheter

Opplever du at myndighetene har bidratt til å styrke virksomhetens IT-sikkerhet?



64 % svarer at de ikke opplever at myndighetene har bidratt til å styrke virksomhetens it-sikkerhet.

FELLES FRONT

Vi i Atea ønsker å tette gapet mellom fokus og investering med kompetanse. Denne kompetansen sitter vi og en rekke andre aktører på. Med denne rapporten setter vi søkelyset på tingenes tilstand i AS Norge, og vi skal bidra til å tilgjengeliggjøre kunnskapen virksomhetene etterspør.

Temaer en vil vite mer om

Er det temaer/områder innenfor IT-sikkerhet du/dere i virksomheten ønsker å lære mer om?

Steg én er å øke kunnskapen i norske virksomheter til et nivå der de vet hva de ikke kan og hvilken kompetanse de skal se etter.


ATEA