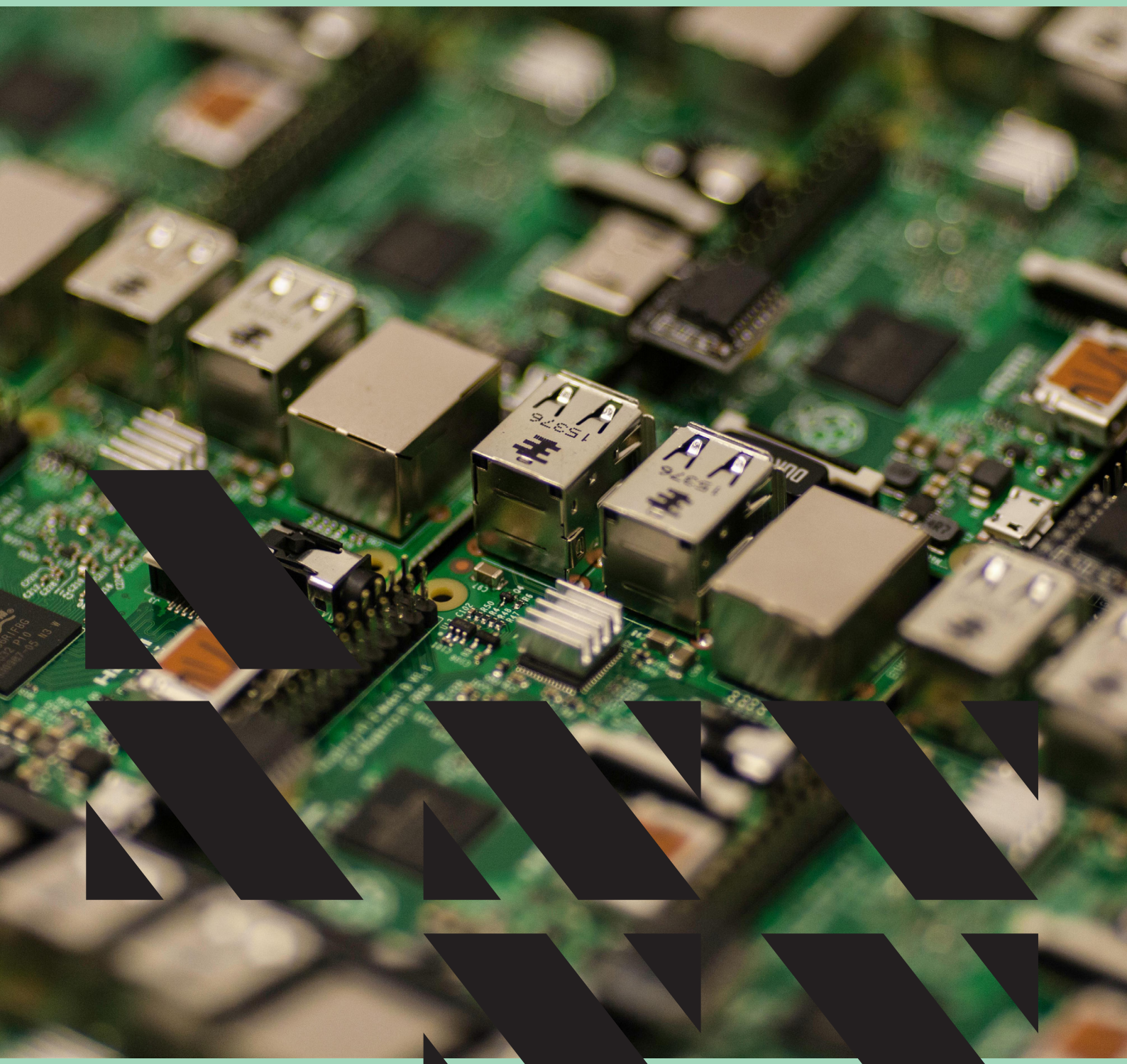
Næringslivets sikkerhets-råd

Mørketalls-undersøkelsen 2024



INNHOLD

FORORD

Det er en glede å presentere Mørketallsundersøkelsen 2024. Dette er 14. gang undersøkelsen gjennomføres. Det er ikke mange slike undersøkelser som kan skilte med en slik rekke av undersøkelser knyttet til digital sikkerhet i Næringslivet. Vi har denne gang gjort noen endringer knyttet til undersøkelsen. Endringer som har hatt som formål å gjøre produktet du nå har i hendene mer relevant i forhold til dagens trusselbilde.

Siden forrige Mørketallsundersøkelse har kunstig intelligens (KI) kommet inn som en ny faktor av betydning. 2024 ble det året da KI for alvor ble allemannseie. Gjennom apper på telefoner, nettbrett og PC gir teknologien oss tilgang til et univers av kunnskap, kompetanse og muligheter. Men som alltid ellers – det som gir nye muligheter, bringer også ny risiko. De som lykkes med å ta teknologien i bruk, vil ha et fortrinn overfor de som ikke gjør det. Det er ingen vei utenom. Men å ta i bruk disse digitale verktøy må gjøres med klokhet og omtanke.

Når vi analyserer resultatene fra denne undersøkelsen, vil nok flere kjenne igjen svarene fra tidligere undersøkelser. Noen kan da hevde at dette ikke er nytt, og at undersøkelsen ikke er særlig spennende eller relevant. Vi hevder det motsatte. For å forstå hva vi utsettes for, spesielt i en tid der ny teknologi (KI) er på vei inn, og få kjenner både muligheter og risiko knyttet til dette, er beskrivelsen av et normalbilde viktig. NSR har med serien av mørketallsundersøkelser bidratt til dette viktige arbeidet.

I lys av dette vil jeg fremheve kapitlene 6, 7 og 8. Her deler viktige cybersikkerhets virksomheter sine analyser og erfaringer, og bidrar med det til å styrke det digitale sikkerhetsarbeidet. Takk til Nasjonalt Cyberkrimsenter, Kripos og Økokrim, mnemonic, Telenor, Abelia, Netsecurity og Coop for deres støtte til arbeidet med Mørketallsundersøkelsen 2024.

Takk også til Spekter, NHO, Telnor, Abelia, Coop, Norges Bank, Advansia, Kongsberg, Visma, F24, mnemonic, Netsecurity og DNB som gjennom økonomiske bidrag har gjort arbeidet med denne rapporten mulig.

Oslo 4. mars 2025

Odin Johannessen
Direktør


ARBEIDSGIVERFORENINGEN
SPEKTER


NHO


telenor


abelia


coop


NORGES BANK


ADVANSIA
PART OF AFRY


KONGSBERG


VISMA


F24


mnemonic


Netsecurity


DNB

SAMMENDRAG

Seks av ti virksomheter (62 prosent) har et rammeverk og/eller styringssystem for informasjonssikkerhet. Det er på nivå med 2020 (63 prosent) og en oppgang fra 2022 (51 prosent). Det er i størst grad virksomheter som leverer samfunnskritiske tjenester som har et slikt rammeverk, og store virksomheter har det i større grad enn andre. 13 prosent av de som har et rammeverk har lagt NSM grunnprinsipper for IT-sikkerhet til grunn, 25 prosent bruker andre standarder, mens hele 61 prosent ikke vet hvilke standarder som ligger til grunn for rammeverket for informasjonssikkerhet.

Det er spurt om virksomhetene har opplevd noen av seks ulike informasjonssikkerhetshendelser: bedrageri, hacktivisme, digitalt skadeverk, tjenesteangrep, datainnbrudd og datatyveri. Av disse er det mest utbredt med bedrageri som 3,5 prosent av virksomhetene har opplevd i 2024. Totalt er det 8 prosent av virksomhetene som har opplevd en eller flere av de seks hendelsene det er spurt om. Blant bedrifter med 5-19 ansatte er det 7 prosent som har opplevd sikkerhetshendelser. Tilsvarende tall for virksomheter med 20 til 99 ansatte er 11 prosent, mens 18 prosent av virksomheter med 100 ansatte eller flere har opplevd det.

De som har opplevd datainnbrudd/datatyveri og bedrageri har fått oppfølgingsspørsmål om disse hendelsene. 24 prosent av de som opplevde datainnbrudd/datatyveri anmeldte forholdet til politiet, mens 26 prosent av de som opplevede bedrageri gjorde det samme. Her skal vi imidlertid merke oss at det er små baser og store feilmarginer.

De som har opplevd sikkerhetsbrudd tror i størst grad sikkerhetsbruddet oppsto på grunn av tilfeldigheter eller uflaks. 63 prosent av de som er utsatt for et sikkerhetsbrudd mener det var årsaken. Den nest mest vanlige årsaken er menneskelige feil (38 prosent) og deretter mangel på sikker-

hetsbevissthet hos de ansatte (31 prosent). Samtidig er det like store andeler som mener hendelsen ble oppdaget ved en tilfeldighet som at den ble oppdaget ved rutinemessig intern sikkerhetsmonitorering.

E-læring er den vanligste aktiviteten virksomheter utfører for å øke ansattes bevissthet rundt sikkerhet. 37 prosent av virksomhetene gjør dette tiltaket. Samtidig ser vi at 28 prosent av virksomheter med 5 ansatte eller flere ikke gjennomfører noen tiltak for å øke ansattes sikkerhetsbevissthet.

INNLEDNING

Bakgrunn

På oppdrag fra Næringslivets Sikkerhetsråd har Opinion gjennomført Mørketallsundersøkelsen 2024. Dette er 14. gangen Mørketallsundersøkelsen gjennomføres av NSR. Det er i 2024 gjort noen endringer i spørreskjema. Muligheten for å sammenligne med tidligere år er derfor begrenset, men gjøres der det er grunnlag for slik sammenligninger.

Populasjon

Populasjonen for denne undersøkelsen er norske virksomheter i privat og offentlig sektor med 5 ansatte eller flere. Undersøkelsens utvalg er trukket fra Datafactory sin database som henter informasjon fra Enhetsregisteret. Det er gjennomført 2500 intervju i undersøkelsen.

Datainnsamling og vekting

Datainnsamling er gjennomført ved hjelp av telefonintervjuer (CATI), i perioden 24. september til 30. oktober 2024. Data er vektet på størrelse (antall ansatte) og bransje (RIM-vektet). Data for tidligere undersøkelser er vektet etter samme metode.

Feilmarginer

Opinion gjør oppmerksom på at enhver undersøkelse vil være beheftet med feilmarginer. Feilmarginene knytter seg i hovedsak til statistisk usikkerhet. Dette er utvalgsskjevheter, som medfører at utvalget ikke er identisk med universet eller målgruppen. Ulikheter kan knytte seg til bestemte kjennetegn eller atferd.

Ved 2500 respondenter eller intervjuer (n=2500) kan vi med 95 % sannsynlighet si at det riktige resultatet ligger innenfor ± 0,9 og ± 2,0 prosentpoeng, avhengig av prosentresultatets størrelse. Usikkerheten er størst ved et prosentresultat på 50 % og minst ved prosentresultater på 5%/95%.

Sektor

Respondentene i undersøkelsen har følgende fordeling mellom privat og offentlig sektor:

Sektor	Antall (n)	Andel intervju
Privat	1776	71 %
Offentlig	724	29 %
Totalt	2500	100 %

Virksomhetsstørrelse

Undersøkelsen omfatter virksomheter i følgende størrelsesgrupper:

Virksomhetsstørrelse	Antall intervju	Andel intervju
5 til 19 ansatte	1407	56 %
20 til 99 ansatte	899	36 %
100 ansatte eller flere	194	8 %
Totalt	2500	100 %

Geografi

Under er en oversikt over respondentenes fylkesvise tilhørighet:

Regioner	Antall	Andel intervju
Nord-Norge	292	12 %
Midt-Norge	306	12 %
Vestlandet	541	22 %
Østlandet	695	28 %
Sørlandet, Telemark og Vestfold	350	14 %
Oslo	316	13 %
Totalt	2500	100 %

Bransje

Undersøkelsen omfatter virksomheter i følgende bransjer:

Bransje	Antall	Andel intervju
Industri etc.	267	11 %
Bygg- og anleggsvirksomhet	170	7 %
Varehandel etc.	382	15 %
Transport og lagring	71	3 %
Overnattings- og serverings-virksomhet	85	3 %
Tjenesteytende næringer	561	22 %
Offentlig administrasjon	71	3 %
Undervisning	322	13 %
Helse og sosial	439	16 %
Kulturell virksomhet	132	5 %
Totalt	2500	100 %

Stilling

I undersøkelsen er det hovedsakelig leder for virksomheten som har svart:

Stilling	Antall	Andel intervju
Adm.dir/daglig leder/skoleleder	1879	75 %
Avdelingsleder/annen leder	287	11 %
IT-/sikkerhetsansvarlig	170	7 %
Annet	164	7 %
Totalt	2500	100 %

1.

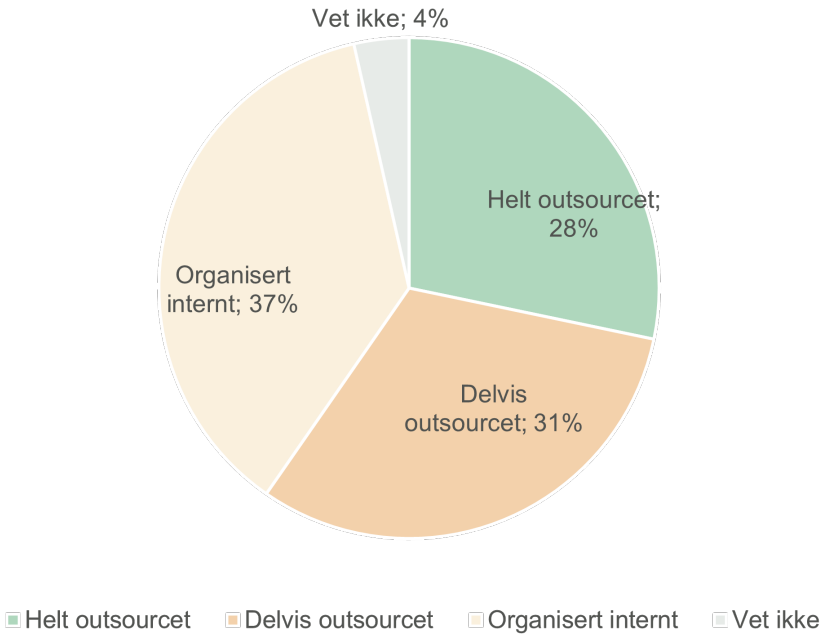
Organisering av IT-driften

Dette kapittelet dekker spørsmål knyttet til hvordan virksomhetene har organisert IT-driften, samt styringssystem eller rammeverk for informasjonssikkerhet.

1.1 Outsourcing

28 prosent har helt outsourcet it-driften, mens 31 prosent har delvis gjort det. I 39 prosent av virksomheter med 5 ansatte eller flere er it-driften organisert internt. Det er noe høyere andel som har helt outsourcet sammenlignet med tidligere undersøkelser. I forrige undersøkelse var det 22 prosent som svarte dette. Bedrifter med 100 ansatte eller flere har i mindre grad enn andre bedrifter helt outsourcet it-driften.

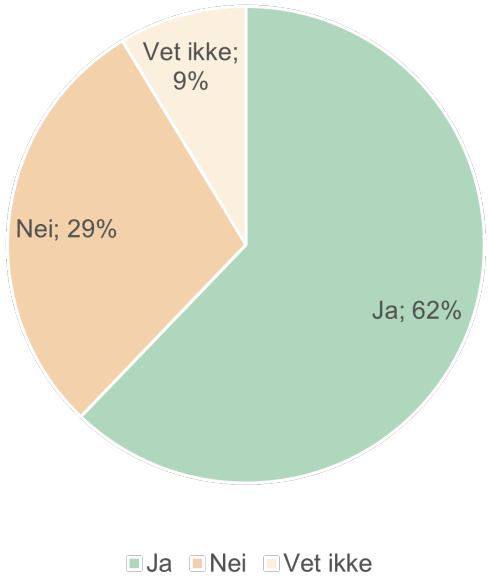
Figur 1. Er virksomhetens it-drift organisert ved at den er helt outsourcet, delvis outsourcet eller er all drift organisert internt? base n = 2500



1.2 Styringssystem og rammeverk

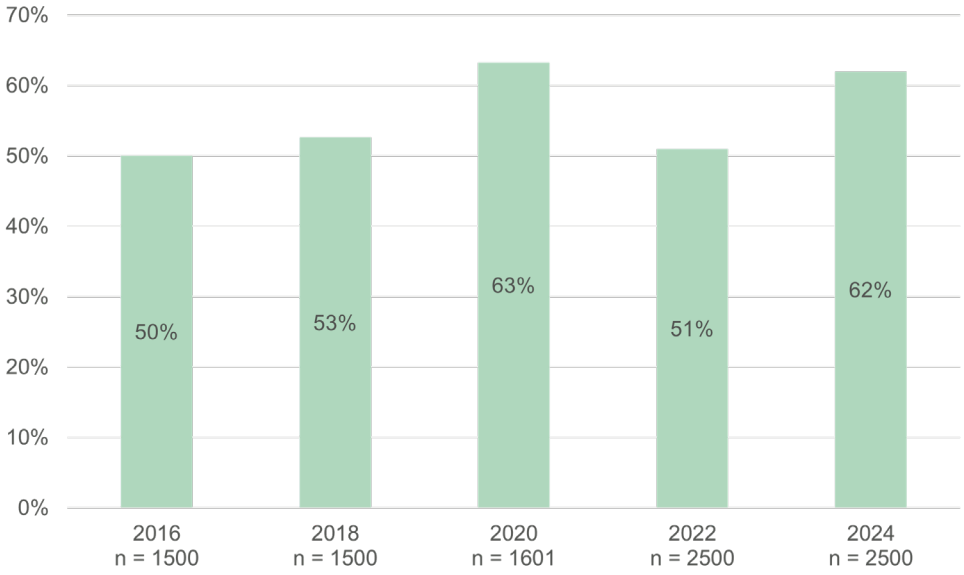
Seks av ti virksomheter oppgir at de har et rammeverk eller et styringssystem for informasjonssikkerhet.

Figur 2. Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerhet? base n = 2500



Sammenlignet med de foregående undersøkelsene er dette på nivå med 2020 og en oppgang fra 2022.

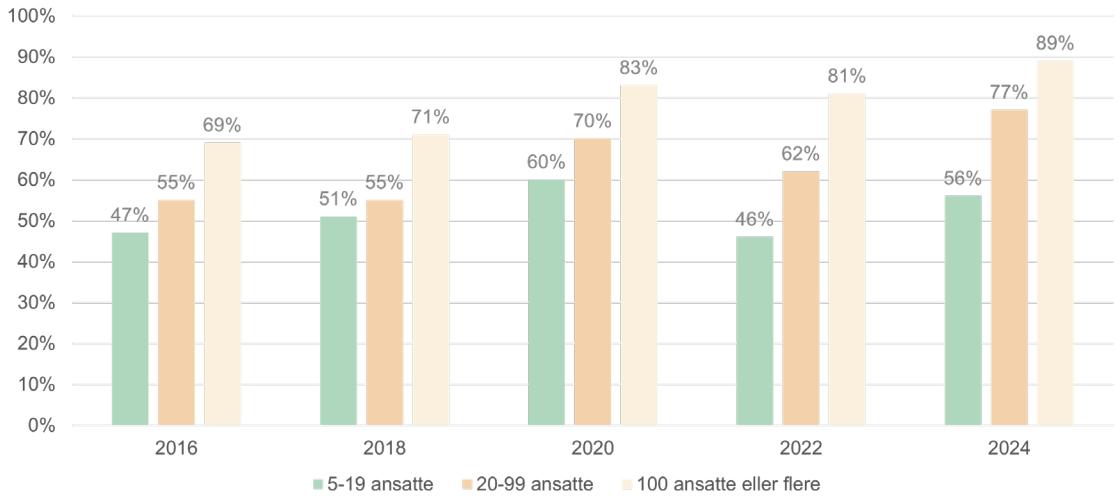
Figur 3. Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerhet? (andel som svarer ja) base n = 9601



Det er forskjell på offentlig og privat sektor der 88 prosent av offentlige virksomheter har et rammeverk, mot 57 prosent av private. Innen offentlig administrasjon er det 98 prosent som har et rammeverk, innen helse og sosial er det 87 prosent og i undervisning er det 84 prosent. I den andre enden med lavest andel med et rammeverk finner vi overnatting og servering med 35 prosent. 74 prosent av virksomheter som leverer samfunnskritiske tjenester har et rammeverk, mot 53 prosent av de som ikke leverer samfunnskritiske tjenester. På dette spørsmålet ligner store virksomheter i privat og offentlig sektor på hverandre, der store bedrifter i begge sektorer i stor grad har rammeverk, mens private mellomstore og små i mindre grad enn offentlige mellomstore og små har det.

Store virksomheter har rammeverk i større grad enn små bedrifter. 56 prosent av virksomheter med 5 til 19 ansatte har det, 77 prosent av de med 20 til 99 ansatte og 89 prosent av de med 100 ansatte eller flere har rammeverk eller styringssystem for informasjonssikkerhet. Tilsvarende mønstre har vi funnet i tidligere undersøkelser.

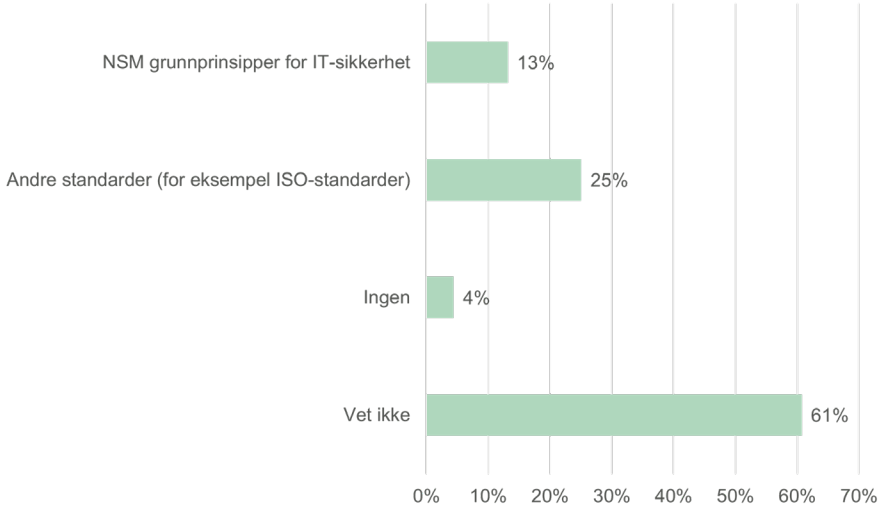
Figur 4. Rammeverk eller styringssystem for informasjonssikkerhet over tid. base n = 9601



Som påpekt i tidligere rapporter ligger det i spørsmålet et tolkningsrom for respondenten. Det er ikke usannsynlig at definisjonen av hva et rammeverk eller styringssystem er, hvor omfattende det er og hvor godt implementert det er kan variere fra respondent til respondent. Likevel skal vi se at de bedriftene som sier de har et rammeverk eller styringssystem på en flere områder er forskjellig fra virksomheter som ikke har det. Med andre ord er det slik at uansett hvordan bedriftene definerer begrepene, så er det forskjell på de som svarer at de har slike system og de som svarer at de ikke har det.

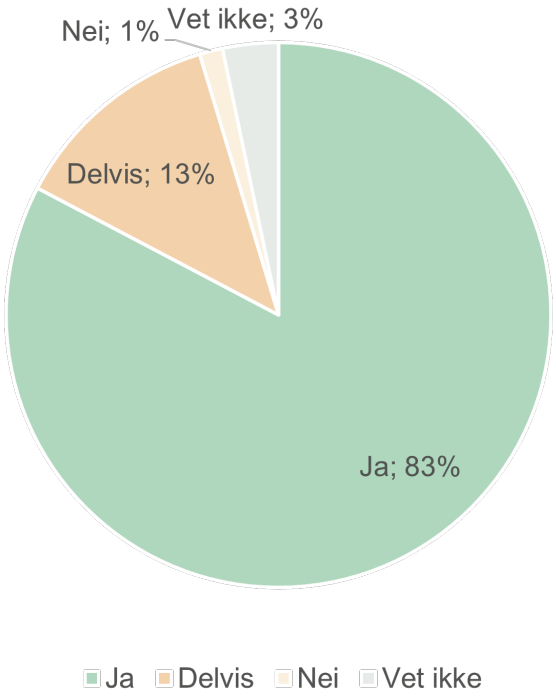
I 2024 har vi med spørsmål om hvilket rammeverk som ligger til grunn for styringssystemet (det har ikke vært stilt tidligere). 13 prosent svarer at det er NSM grunnprinsipper for IT-sikkerhet, 25 prosent svarer andre standarder, for eksempel ISO-standarder, 4 prosent at det ikke ligger noen standard til grunn, mens hele 61 prosent ikke vet hvilke standarder som ligger til grunn for styringssystemet.

Figur 5. Hvilke standarder ligger til grunn for rammeverket / styringssystemet? base n = 1739; total n = 2500; 761 missing



De som har et rammeverk eller styringssystem mener i stor grad at det etterleves i organisasjonen. 83 prosent svarer at det blir etterlevd, 13 prosent svarer at det delvis etterleves og kun 1 prosent svarer nei. Dette spørsmålet er tidligere stilt uten svaralternativet «delvis» så det er ikke sammenlignbart med tidligere. Andeler som svarte ja var 92 prosent i 2022, 91 prosent i 2020 og 90 prosent i 2018.

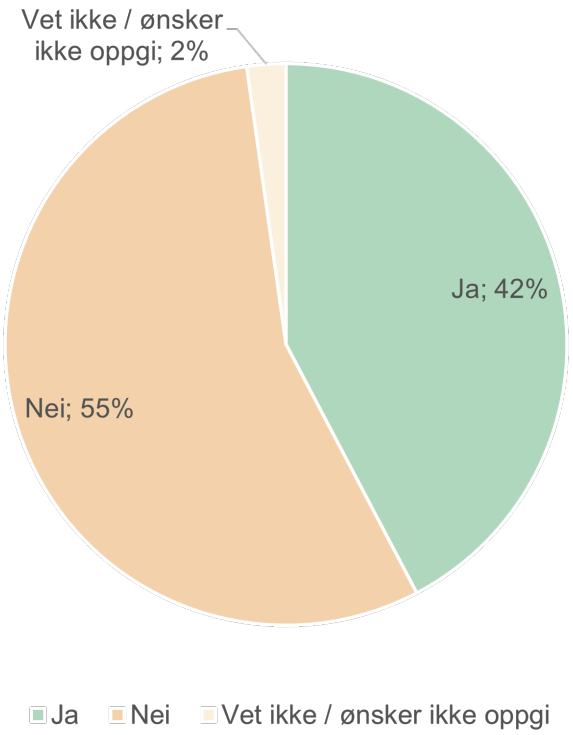
Figur 6. Opplever du at rammeverket / styringssystem for sikkerhet blir etterlevd i organisasjonen? base n = 1739; total n = 2500; 761 missing



1.3 Samfunnskritiske tjenester

42 prosent av virksomhetene opplever at de leverer samfunnskritiske tjenester. Dette spørsmålet er stilt for første gang i 2024.

Figur 7. Leverer din virksomhet, slik du ser det, samfunnskritiske tjenester? base n = 2500



Å levere samfunnskritiske tjenester er mer vanlig i store enn små bedrifter. I de tre størrelsesgruppene 5-19, 20 til 99 og 100 eller flere ansatte er det 38, 52 og 68 prosent av virksomhetene som leverer samfunnskritiske tjenstester. I offentlig sektor er det 78 prosent som leverer samfunnskritiske tjenester, mens det er 36 prosent i privat sektor som gjør det samme. I størst grad er det virksomheter innen offentlig administrasjon som leverer samfunnskritiske tjenester med 86 prosent, og i minst grad overnatting og servering med 13 prosent. Videre er det 51 prosent av virksomheter med rammeverk for informasjonssikkerhet som leverer samfunnskritiske tjenester, mot 27 prosent av de som ikke har et rammeverk. Blant virksomhetene som leverer samfunnskritiske tjenester er det 74 prosent som har et rammeverk for informasjonssikkerhet.

2.

Hendelser

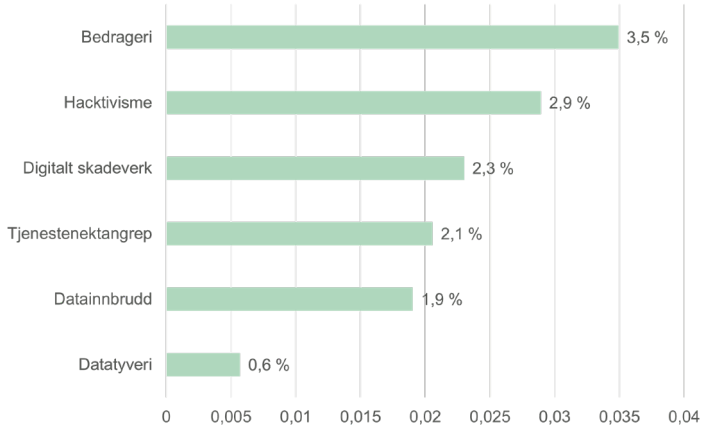
Dette tema handler om hvilke informasjonssikkerhets-hendelser virksomhetene er utsatt for, og hva som ble følgene av disse hendelsene.

Denne delen av undersøkelsen er endret fra tidligere år og resultatene er ikke sammenlignbare. Vi vil derfor i denne delen kun fokusere på 2024-resultater.

2.1 Informasjonssikkerhetshendelser

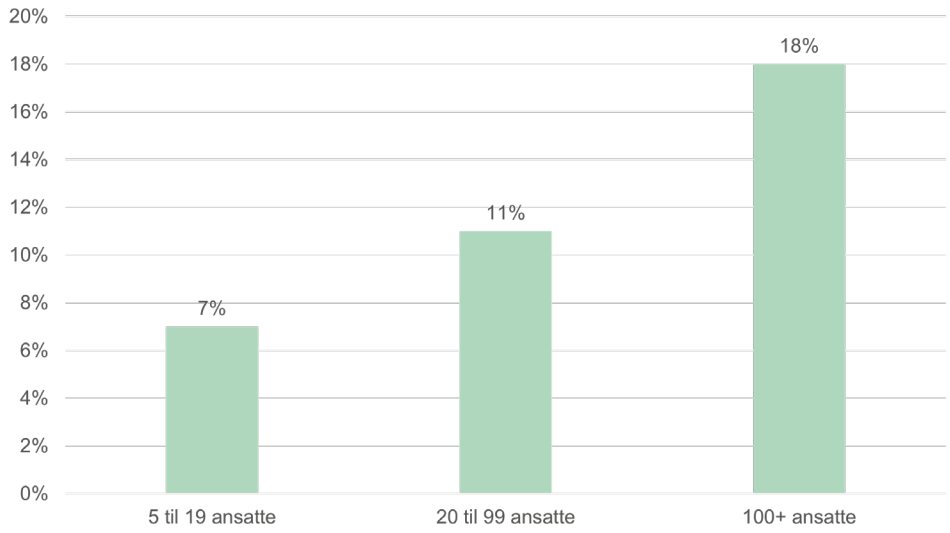
Det er spurt om seks ulike hendelser der virksomhetene har svart ja eller nei på om de har opplevd disse i løpet av kalenderåret 2024. De mest vanlige hendelsene er bedrageri og hacktivisme som 3,5 og 2,9 prosent av virksomhetene har opplevd i løpet av 2024. Datatyveri er den hendelsen virksomhetene er minst utsatt for (0,6 prosent av virksomhetene). Figuren under viser andel av virksomheter som har opplevd de ulike hendelsene i løpet av 2024.

Figur 8. Jeg vil nå lese opp noen mulige informasjonssikkerhetshendelser og ber deg svare ja eller nei på om virksomheten har vært utsatt for disse i kalenderåret 2024? base n = 2500



Totalt er det 8 prosent av virksomhetene som har opplevd en eller flere hendelser. 17 prosent av virksomheter innen transport har opplevd hendelser, signifikant høyere enn andre bransjer (alle andre bransjer samlet). Det er større andel store bedrifter som har opplevd hendelser enn små. Mens 7 prosent av de minste bedriftene har opplevd hendelser er det 18 prosent av de store virksomhetene som har opplevd det.

Figur 9. Jeg vil nå lese opp noen mulige informasjonssikkerhetshendelser og ber deg svare ja eller nei på om virksomheten har vært utsatt for disse i kalenderåret 2024? Total sample; base n = 2500

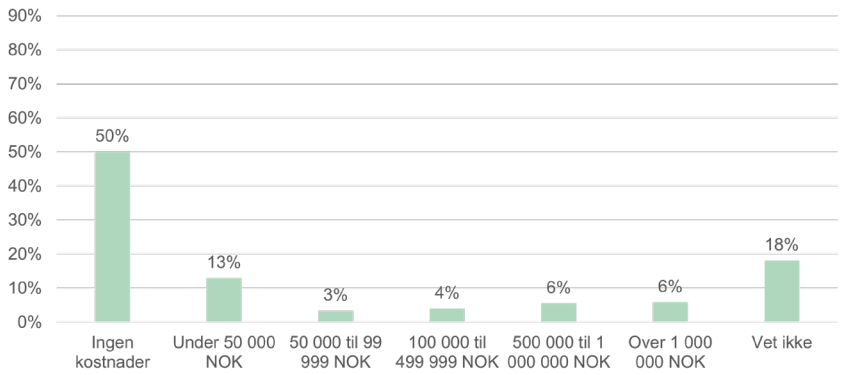


2.2 Følger av datainnbrudd/datatyveri

De som har opplevd datainnbrudd og/eller datatyveri har fått oppfølgingsspørsmål om hvilke følger disse hendelsene har medført. I og med at det kun er de som har opplevd datainnbrudd/datatyveri som får denne oppfølgingen, er det en liten base som ligger til grunn (n=50).

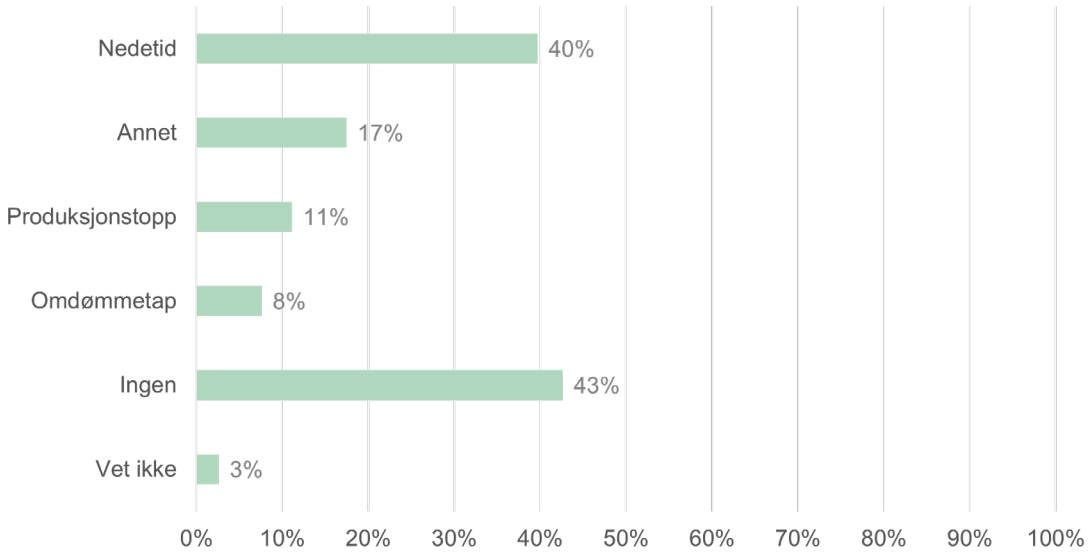
For det første er det spurt om hvilke tap man eventuelt opplevde. Halvparten opplevde ingen økonomiske tap (svarer at det ikke hadde noen kostnader).

Figur 10. I forbindelse med datainnbruddet/datatyveriet, hva var deres tap? base n = 50; total n = 2500; 2450 missing



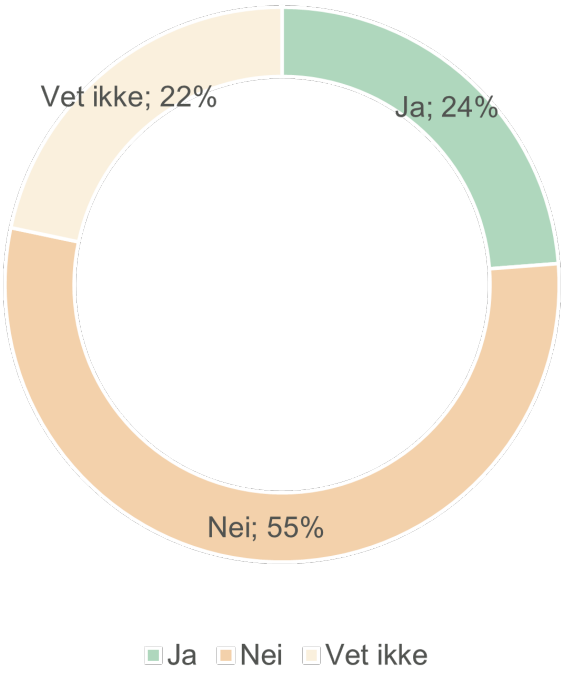
Utover økonomiske tap, er det nedetid som er den mest vanlige ikke-økonomiske følgen av hendelsen.

Figur 11. Var det andre konsekvenser i forbindelse med datainnbruddet/datatyveriet? base n = 50; total n = 2500; 2450 missing



24 prosent av de som opplevde datainnbrudd/datatyveri anmeldte forholdet til politiet.

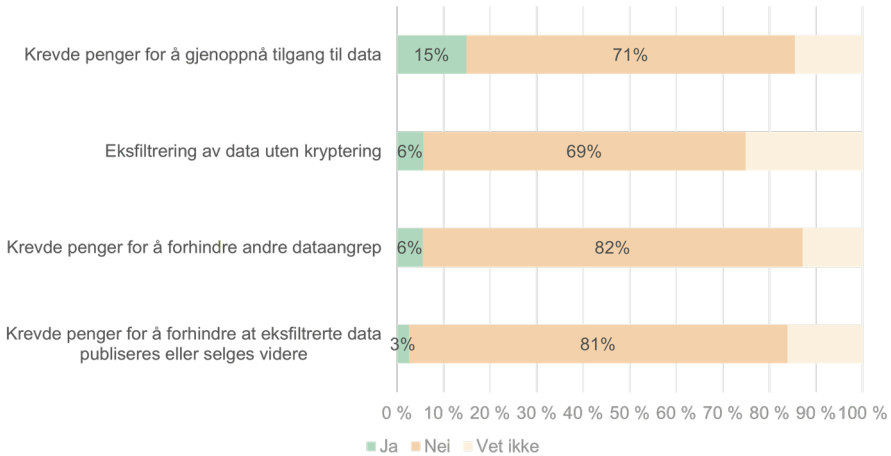
Figur 12. Anmeldte dere datainnbruddet/datatyveriet til politiet? base n = 50; total n = 2500; 2450 missing



Blant de som ikke anmeldte forholdet oppgis i størst grad at det var en ubetydelig hendelse/lite tap som årsak til at de ikke anmeldte. At årsaken er at de har liten tillit til politiet oppgis av kun 4 prosent.

15 prosent av de som ble utsatt for datainnbrudd/datatyveri svarer at det ble krevd penger for å gjenoppnå tilgang til dataene.

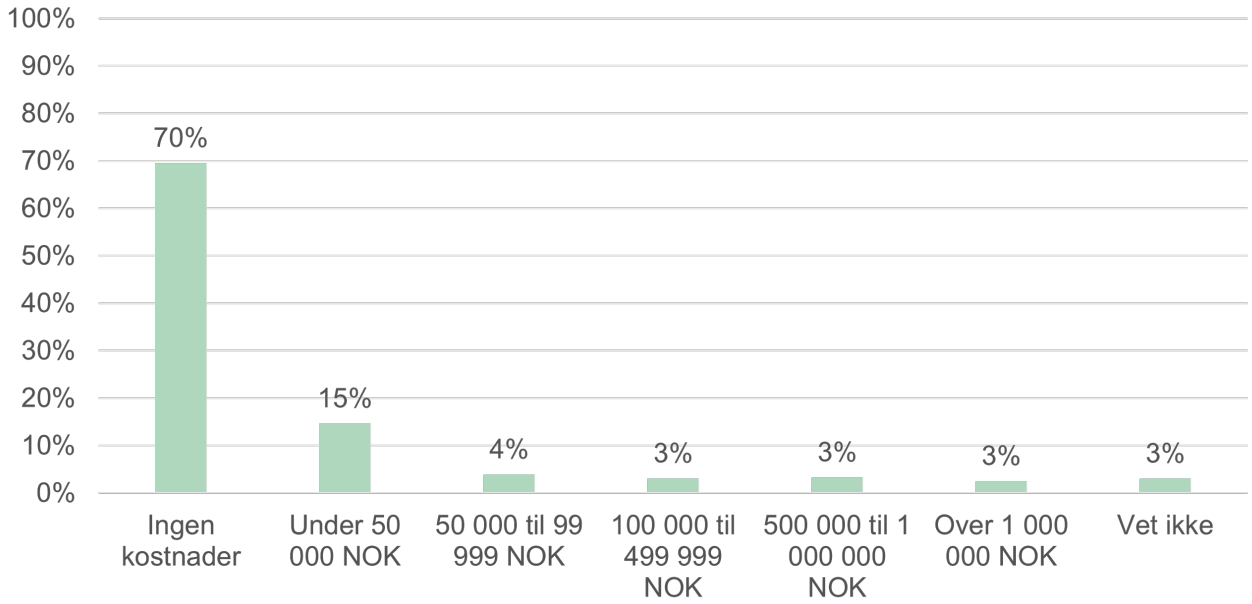
Figur 13. Krevde de som utførte datainnbruddet/datatyveriet noe av følgende? base n = 50; total n = 2500; 2450 missing



2.3 Følger av bedrageri

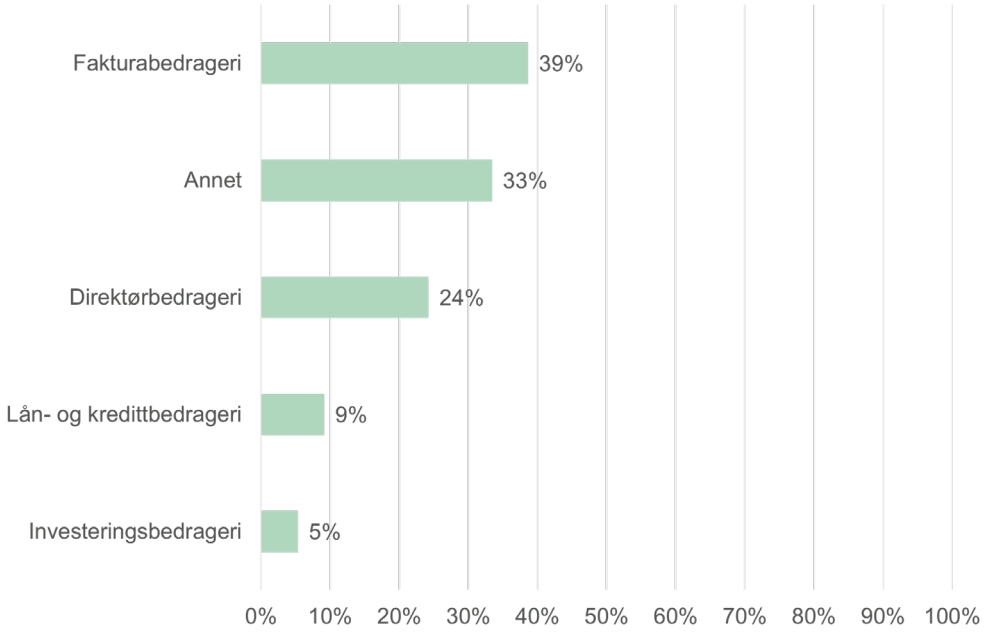
De som har opplevd bedrageri har fått oppfølgingsspørsmål om hvilke følger disse hendelsene har medført. For det første er det spurt om hvilke tap man eventuelt opplevde. Blant de som er utsatt for bedrageri er det 70 prosent som svarer at det ikke hadde noen kostnader.

Figur 14. I forbindelse med bedrageriet, hva var deres tap? base n = 102; total n = 2500; 2398 missing



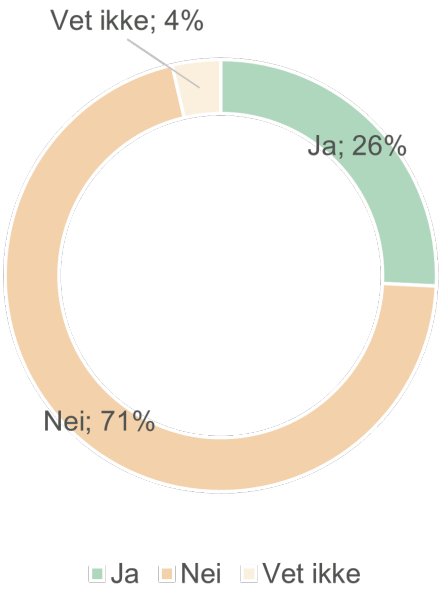
Det er fakturabedrageri som er den vanligste formen for bedrageri. I gruppen som svarer annet, finner vi flere som noterer phishing og ID-tyveri.

Figur 15. Hvilke metoder ble brukt av de som utførte bedrageriet? base n = 102; total n = 2500; 2398 missing

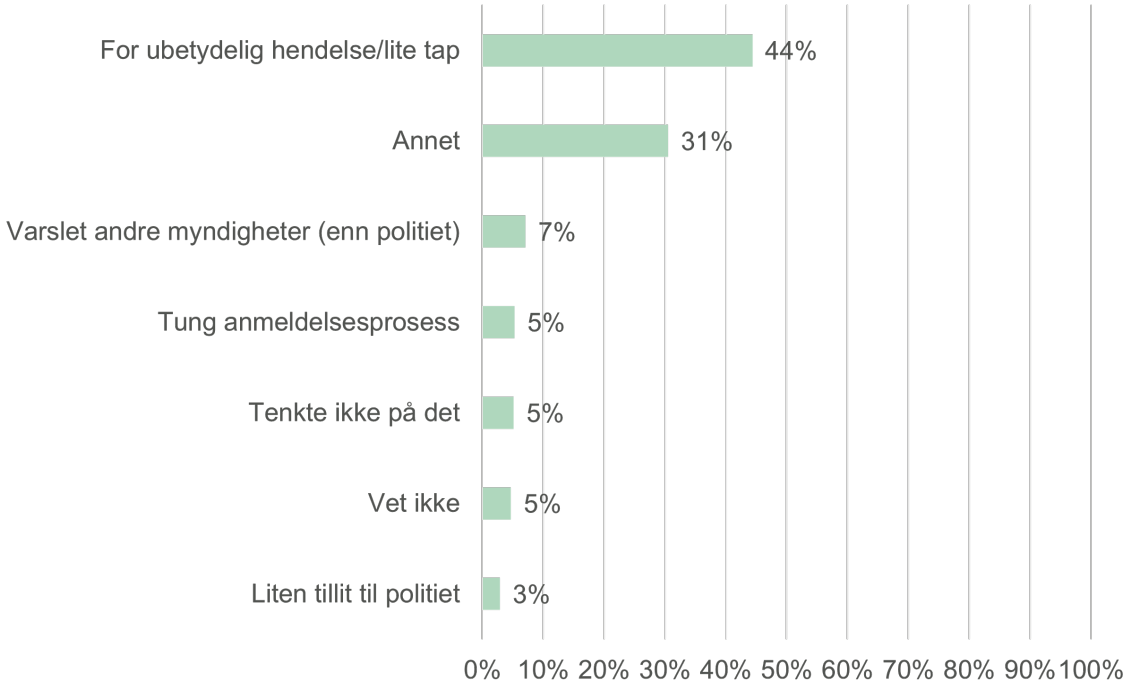


26 prosent av de som opplevde bedrageri anmeldte forholdet til politiet. I privat sektor er det 39 prosent som anmeldte, mens det i offentlig sektor er 9 prosent. Det er signifikant forskjell, men vi må likevel tolke dette med forsiktighet på grunn av små baser.

Figur 16. Anmeldte dere bedrageriet til politiet? base n = 102; total n = 2500; 2398 missing



Figur 17. Hvorfor ble bedrageriet ikke anmeldt? base n = 73; total n = 2500; 2427 missing



3.

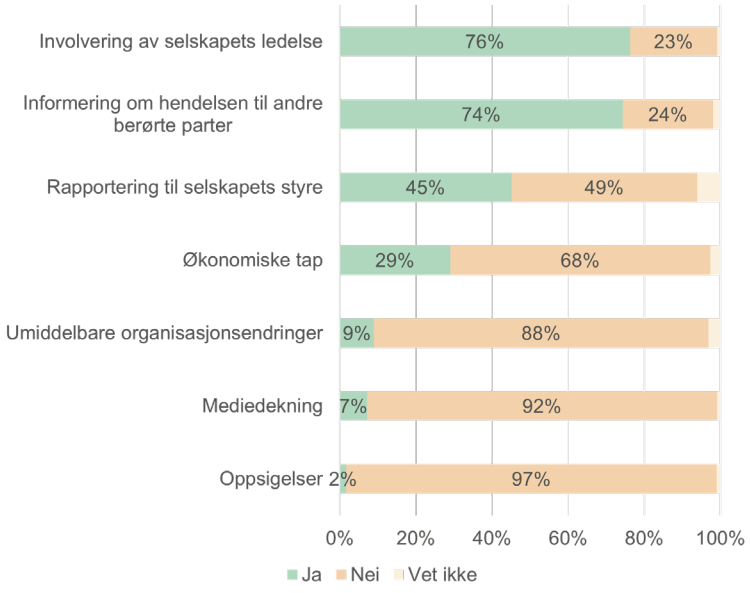
Følger av hendelsen

Dette kapittelet handler om hva som ble følgene av hendelsene.

3.1 Hva førte hendelsen til

De som har opplevd uønskede hendelser har fått oppfølgingsspørsmål om hva hendelsen førte til. I størst grad er det involvering av virksomhetens ledelse og informering av andre berørte parter som var følgene. Endringer i organisasjonen eller mediedekning er i liten grad følger av de uønskede hendelsene virksomhetene har opplevd. Det er ikke klare mønstre når det gjelder virksomheter i ulike undergrupper. Vi finner at private virksomheter i større grad enn offentlige har hatt økonomiske tap (34 vs. 11 prosent), men ellers er det små forskjeller.

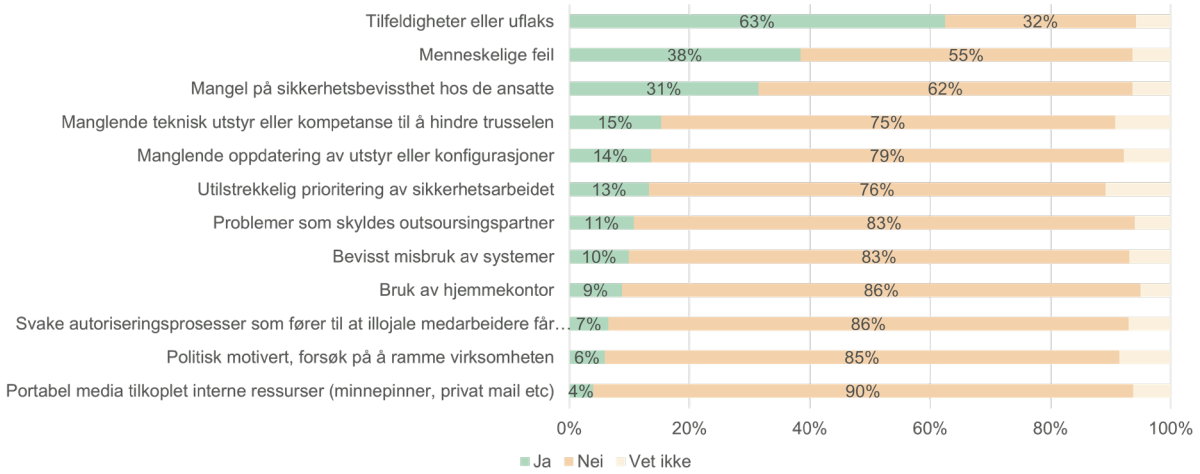
Figur 18. Førte denne spesifikke hendelsen til følgende? base n = 224; total n = 2500; 2276 missing



3.2 Årsak til sikkerhetsbruddet

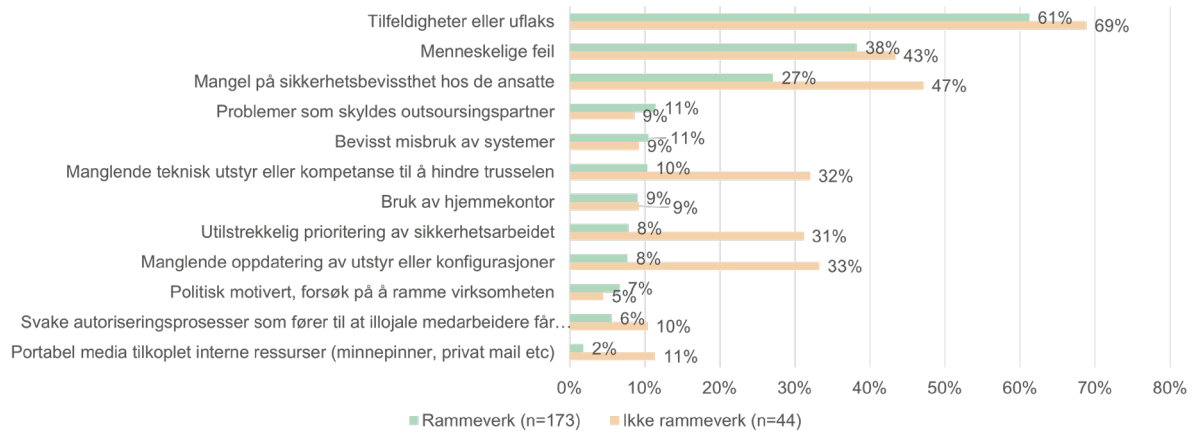
De som har opplevd sikkerhetsbrudd tror i størst grad sikkerhetsbruddet oppsto på grunn av tilfeldigheter eller uflaks. 63 prosent av de som er utsatt for et sikkerhetsbrudd mener det var årsaken. Den nest mest vanlige årsaken er menneskelige feil.

Figur 19. Var noen av følgende faktorer medvirkende til at sikkerhetsbruddet oppsto? base n = 224; total n = 2500; 2276 missing



Virksomheter i privat sektor skiller seg noe fra virksomheter i offentlig sektor ved at de i større grad oppgir utilstrekkelig prioritering av sikkerhetsarbeidet, svake autoriseringsprosesser som fører til at illojale medarbeidere får tilgang til informasjon og manglende oppdatering av utstyr eller konfigurasjoner. Virksomheter som ikke har rammeverk for informasjonssikkerhet har i større grad enn de som har rammeverk sikkerhetsbrudd på grunn av utilstrekkelig prioritering av sikkerhetsarbeidet, mangel på sikkerhetsbevissthet hos de ansatte, manglende oppdatering av utstyr eller konfigurasjoner, manglende teknisk utstyr eller kompetanse til å hindre trusselen og portabel media tilkoblet interne ressurser (minnepinner, privat e-post etc.).

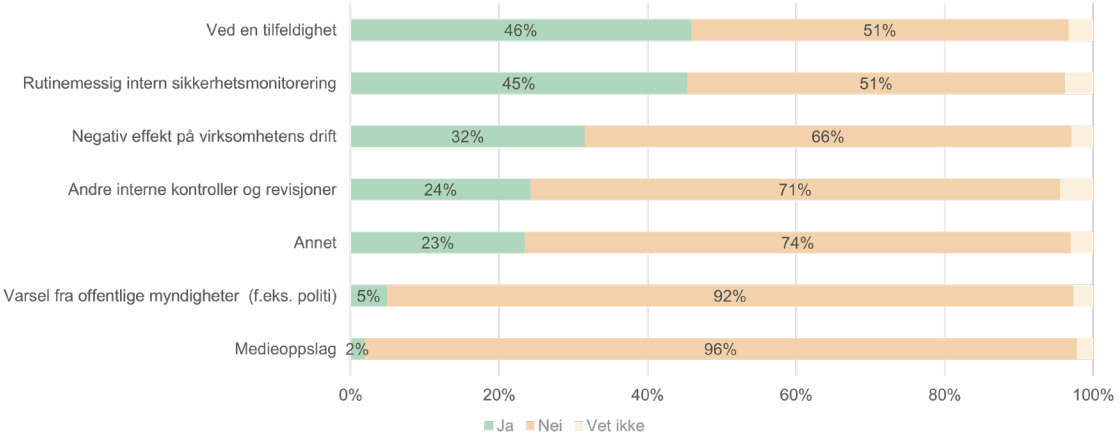
Figur 20. Var noen av følgende faktorer medvirkende til at sikkerhetsbruddet oppsto? base n = 224; total n = 2500; 2276 missing



3.3 Årsak til at hendelsen ble oppdaget

Det er like store andeler som mener hendelsen ble oppdaget ved en tilfeldighet som oppdaget det ved rutinemessig intern sikkerhetsmonitorering.

Figur 21. Var noe av følgende årsak til at hendelsen ble oppdaget? base n = 224; total n = 2500; 2276 missing



Virksomheter som leverer samfunnskritiske tjenester og har rammeverk for informasjonssikkerhet har i mindre grad enn andre oppdaget hendelsen ved en tilfeldighet. Store virksomheter (100+ ansatte) blir i større grad enn mindre varslet av myndigheter. Det er ikke forskjell på virksomheter i privat og offentlig sektor.

4.

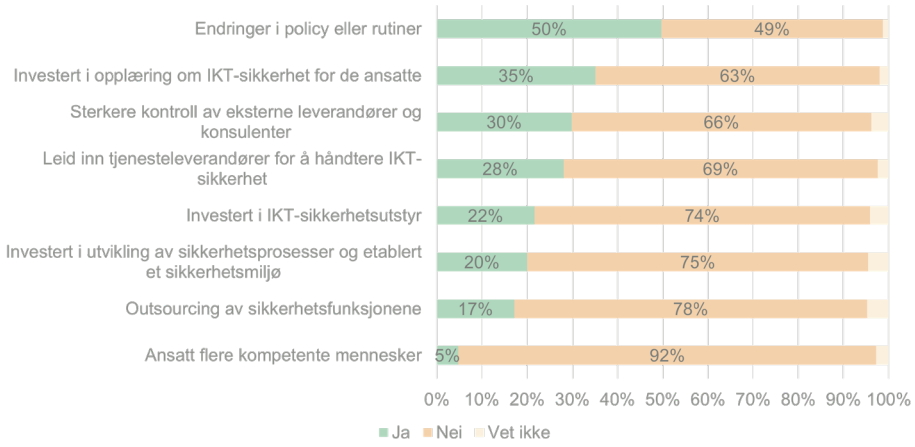
Håndtering av hendelser

Dette tema handler om hvordan hendelsene ble håndtert.

4.1 Håndtering av hendelser

Den vanligste endringen blant virksomheter som har opplevd uønskede hendelser er endring av policy eller rutiner. Halvparten av virksomhetene som har opplevd sikkerhetsbrudd har endret policy eller rutiner.

Figur 22. : Som et resultat av hendelsen, ble noen av følgende endringer gjort i organisasjonen? base n = 224; total n = 2500; 2276 missing



Utover endring av policy er det investering i opplæring som er den nest mest vanlige endringen. De som har et rammeverk for informasjonssikkerhet har i større grad enn andre investert i opplæring som følge av sikkerhetsbruddet. På dette spørsmålet er det generelt liten forskjell på virksomheter i ulike grupper.

Vi skal være forsiktige med sammenligning med tidligere undersøkelser i og med at spørsmålet som filtrerer hvilke respondenter som får dette spørsmålet er endret. Det er derfor rimelig å anta at det ikke er helt sammenlignbare virksomheter som får oppfølgingsspørsmålet.

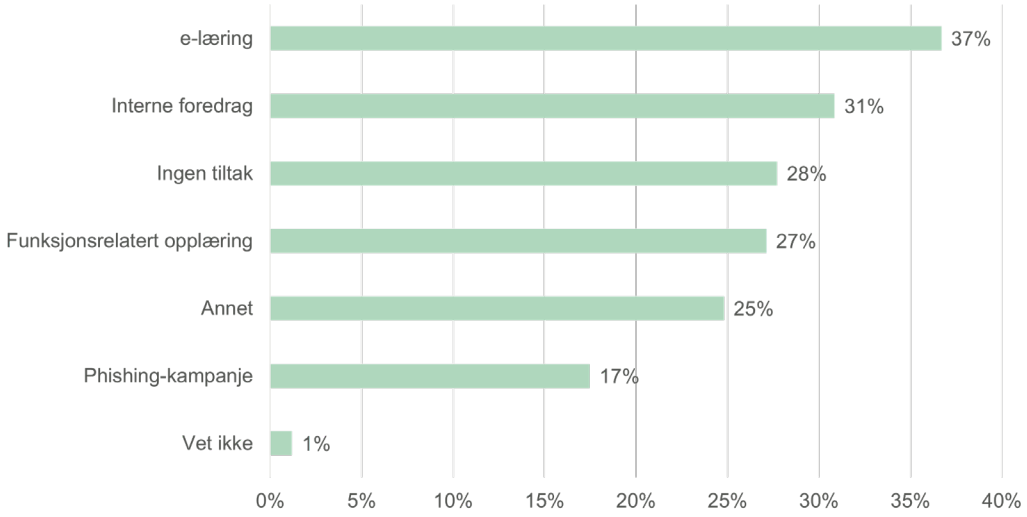
5.

Tiltak for økt sikkerhet

5.1 Økt bevissthet rundt sikkerhet blant ansatte

E-læring er den vanligste aktiviteten virksomheter utfører for å øke ansattes bevissthet rundt sikkerhet. Samtidig ser vi at 28 prosent av virksomheter med 5 ansatte eller flere ikke gjennomfører noen tiltak for å øke ansattes sikkerhetsbevissthet.

Figur 23. Hvilken type aktiviteter som øker ansattes bevissthet rundt sikkerhet er gjennomført i løpet av det siste året? base n = 2500; total n = 2500



Det er klare forskjeller når det gjelder bedriftsstørrelse der 33 prosent av virksomheter med 5-19 ansatte ikke har noen tiltak for å øke sikkerhetsbevisstheten blant ansatte. Blant de med 20 til 99 ansatte er tilsvarende tall 16 prosent, mens blant de største virksomhetene med 100 ansatte eller mer er det 5 prosent som ikke har noen aktiviteter for å øke sikkerhetsbevisstheten til de ansatte. Når det gjelder bransje er det industri, bygg og anlegg og overnatting/servering der høyest andel svarer ingen tiltak (henholdsvis 40, 35 og 51 prosent har ingen tiltak). I privat sektor er det 31 prosent som har ingen tiltak, mot 9 prosent i offentlig sektor. Blant virksomheter som ikke har et rammeverk for informasjonssikkerhet er det 54 prosent som sier de ikke har noen aktiviteter for å øke ansattes bevissthet om informasjonssikkerhet. Tilsvarende for de som har et rammeverk er 14 prosent. Det samme mønsteret finner vi blant virksomheter som leverer samfunnskritiske tjenester, der 35 prosent av de som ikke leverer samfunnskritiske tjenester ikke har noen aktiviteter for økt informasjonssikkerhet, mot 18 prosent av de som leverer samfunnskritiske tjenester. Med unntak av funksjonsrelatert opplæring, er alle aktiviteter mer vanlig blant de som har opplevd sikkerhetshendelser enn blant de som ikke har opplevd hendelser.

6.

Risiko og trender

Dette kapittelet er skrevet av Nasjonalt Cyberkrimsenter, Kripos og Økokrim.

6.1 Trekk ved den digitale kriminaliteten

Digital kriminalitet eller cyberkriminalitet rammer bredt, har stor geografisk spredning og omfatter mange ulike typer lovbrudd. Kripos bruker begrepene cyberrettet kriminalitet og cyberstøttet kriminalitet til å skille ulike områder innenfor digital kriminalitet. Den cyberrettede kriminaliteten rammer IKT-systemer direkte, mens cyberstøttet kriminalitet bruker det digitale for å understøtte eller forenkle gjennomføringen av lovbruddene. Datainnbrudd, datatyveri og digitalt skadeverk er cyberrettet kriminalitet, mens seksuallovbrudd, økonomisk kriminalitet og organisert kriminalitet er cyberstøttet. For nær sagt alle former for cyberkriminalitet øker det registrerte omfanget, og de kriminelle utvikler seg ved å tilpasse teknikker, metoder, verktøy og strategier.

For å drifte den ulovlige virksomheten har aktørene behov for anonymitet, operasjonssikkerhet og i noen tilfeller sensitiv informasjon. Dette skaper et marked innenfor den kriminelle sfæren hvor teknologiske tjenester, verktøy og infrastruktur selges eller leies ut. Denne kommersialiseringen omtales som kriminalitet som handelsvare (KSH) og er en av driverne bak cyberkriminalitet. Flere tilbydere innenfor dette markedet tilbyr opplæring og ekspertise sammen med verktøyene de selger. Terskelen for å bedrive kriminaliteten blir dermed senket og mulig å utføre uten at den teknologiske kompetansen nødvendigvis er høy.

Særlig kriminelle som utfører cyberrettet kriminalitet er tjent med KSH pga. kompleksitet og kompetansekrav. For eksempel vil et datatyveri være avhengig av tilgang til et datasystem. I neste omgang kan stjålet data være brukt til utpressing eller bedrageri. Også aktører innenfor løsepengevirus kan nyttiggjøre seg KSH, hvor enkelte kan stå for krypteringen av virksomheters systemer, mens andre utvikler selve skadevaren.

Denne gjensidige avhengigheten som det kriminelle økosystemet skaper gjør at det dannes grupperinger som driver med digital kriminalitet. Kripos deler aktørene i ulike kategorier: uerfarne, spesialiserte og organiserte kriminelle. De uerfarne kan benytte programvare som ikke krever store forkunnskaper, mens de spesialiserte gjerne tilbyr tjenestene sine gjennom KSH. Ofte annonseres dette gjennom lukkede kanaler på ende-til-ende-krypterte meldingstjenester, som for eksempel Telegram. De organiserte kriminelle er profesjonelle aktører og fremstår som en hierarkisk organisasjon hvor ulike personer har sine funksjoner og fullmakter. Både teknisk og språklig kompetanse er ettertraktet, det samme med mellommenneskelige ferdigheter.

Den teknologiske utviklingen og tilpasningen går raskt, og bruken av generativ kunstig intelligens (KI) har blitt dagligdags for store deler av befolkningen etter at tjenester som ChatGPT ble lansert. Også dette har senket kompetansekravet og kostnadene til de kriminelle. Eksempelvis er det lettere å tilpasse bedragerikampanjer og vanskeligere å skille ekte fra falskt innhold. Deepfake, som benyttes til å lage realistiske bilde-, video- og lydopptak, har blitt observert i bedragerivirksomhet i flere land.

6.2 Bedrageri

Det er registrert en økning innen alle områder for både cyberrettet og cyberstøttet kriminalitet, med unntak av digitalt skadeverk, som har holdt seg stabilt. Et av områdene innenfor cyberstøttet kriminalitet med flest forsøk og fullbyrdede handlinger er bedrageri. Det er rettet mot et bredt spekter av personer, bedrifter og etater, og de kriminelle kan både operere individuelt eller som en del av et nettverk. Halvparten av de største kriminelle nettverkene i Europa spesialiserer seg på digitale bedrageri. Selv om bedrageri kan ramme alle ser vi også at det begås svindel der gjerningspersonene velger seg ut ofre mer målrettet. Dette kan for eksempel skje ved at de innhenter person- og selskapsinformasjon fra offentlige registre eller kjøpe stjålne datapakker.

En type svindel mot næringslivet er BEC-bedrageri. Det er en forkortelse for Business email compromise og betegner blant annet direktør- og fakturabedrageri. I Sverige er det estimert at dette genererte 329 millioner svenske kroner til kriminelle aktører i 2023. Vi ser også flere eksempler på at norske bedrifter er blitt svindlet for beløp på flere titalls millioner kroner i slike bedrageri.

En annen trussel mot næringslivet er lånebedrageri ved utnyttelse av samtykkebasert lånesøknad (SBL). Her opprettes det fiktive ansettelsesforhold som genererer uriktige opplysninger om lønn til myndighetene. Dette brukes deretter til å søke lån på feilaktig grunnlag. Noe av det samme sees ved manipulerte foretaksregnskap som benyttes til å kjøpe varer på kreditt, fordi økonomien ser bedre ut enn den reelt er.

6.3 Sårbarheter

Et viktig ledd i bekjempelsen av cyberkriminalitet ligger i å avdekke og håndtere sårbarheter. Økokrim peker på at gapet mellom de kriminelle og politiets bruk av teknologi øker. Illegale aktører tar raskt i bruk ny teknologi, mens politiet må forholde seg til lover, regler og retningslinjer før de kan benytte den, noe som gjør at de kriminelle får økt handlingsrom på bekostning av politiet og samfunnet for øvrig.
Selv om åpenhet og tillit er viktige verdier i det norske samfunnet gjør det at mye informasjon om både privatpersoner og foretak ligger offentlig tilgjengelig. Denne informasjonen gir også kriminelle innsyn i hendelser, som for eksempel kjøp, salg og endringer i registerinformasjon og kan utnyttes til å fremstå troverdige i kriminalitetsutøvelsen.

Mange virksomheter benytter skyløsninger. Det innebærer en sentralisering av verdier og kriminelle kan bruke infrastrukturen til å ramme aktører som har data, applikasjoner og systemer hos disse leverandørene. Anonymiseringsteknologier som proxy- og VPN-løsninger gjør at cyberkriminelle kan skjule egne IP-adresser og kryptere datatrafikk. Dette vanskeliggjør etterforskningen av denne type kriminalitet. Også fremveksten av desentraliserte betalingsløsninger og kryptovaluta gjør at pengestrømmene til kriminelle aktører kan bli vanskeligere å spore enn ved tradisjonelle pengetjenester.

7.

Erfaringer


43
44
45
46
47
2
2/2

7.1 Erfaringer fra mnemonic

Denne artikkelen bygger på våre erfaringer fra tjenesteleveranser til kunder i perioden 2023 og 2024 - omtalt som rapporteringsperioden. Våre leveranser har omfattet granskning og håndtering av alvorlige datainnbrudd, analyse av trusseletterretning, samt døgnkontinuerlig sikkerhetsmonitorering fra vårt operasjonssenter. Basert på dette har vi identifisert sentrale utviklingstrekk i trussellandskapet, kartlagt sårbarheter og utformet anbefalinger som reflekterer dagens sikkerhetsutfordringer.

Trusselbildet

Statlige aktører

Basert på våre erfaringer er «det store bildet» at avanserte trusselaktører (APT), inkludert Russland, Kina, Nord-Korea og Iran, i økende grad utfører målrettede angrep mot vestlige land som en del av sine hybride operasjoner. Disse operasjonene finner sted både i det fysiske og digitale domenet og preges av stor variasjon i motivasjon, frekvens og metodebruk. Typiske mål inkluderer spionasje, påvirkningsoperasjoner, økonomisk vinning, og destabilisering av samfunn, kritisk infrastruktur og institusjoner.

Den pågående geopolitiske ustabiliteten, med økende stormaktskonkurranse og intensiverte konflikter, har ført til en tydelig økning i trusselaktørers vilje til å ta risiko. Dette innebærer hyppigere bruk av det digitale domenet som en arena for å nå strategiske mål, hvor kombinasjonen av datatyveri, sabotasje og desinformasjonskampanjer brukes for å påvirke politiske og økonomiske forhold i vestlige land.

Vi observerer også at trusselaktørene i større grad kombinerer tradisjonelle digitale angrep med andre metoder som økonomisk press og sosial manipulering. Dette muliggjøres av sofistikerte teknikker, som utnyttelse av sårbarheter i forsyningskjeder, bruk av spesialtilpasset skadevare, og målrettet phishing som rettes mot spesifikke nøkkelpersoner eller viktige samfunnsvirksomheter.

Denne utviklingen er i tråd med åpne trusselvurderinger fra norske EOS-tjenester, som fremhever behovet for økt årvåkenhet og samarbeid mellom aktører . En raskere tilpasningsevne blant avanserte trusselaktører gjør det også helt nødvendig å investere i mer robuste sikkerhetsmekanismer, forbedret trusseletterretning og en helhetlig tilnærming til digital sikkerhet.

Kriminelle grupperinger

Det kriminelle økosystemet har utviklet seg til å bli mer effektivt, organisert og spesialisert. Mange aktører fokuserer på smale deler av angrepskjeden, som å identifisere sårbare tjenester, skaffe brukernavn og passord, og etablere et innledende fotfeste. Disse tilgangene eller informasjonspakkene selges videre på skjulte nettforum til andre aktører med ulike formål, inkludert økonomisk vinning, sabotasje eller spionasje.

På de samme forumene omsettes også tjenester som Ransomware as a Service (RaaS), hvor erfarne grupperinger med høyere teknisk kapabilitet tilbyr ferdigutviklede verktøy og løsninger til andre kriminelle. Disse tjenestene er ofte pakket som kommersielle produkter, der betaling skjer som et fast beløp eller gjennom en prosentandel av utbyttet. Dette senker terskelen for andre kriminelle aktører som mangler teknisk ekspertise, men som ønsker å gjennomføre målrettede angrep.

Det kriminelle økosystemet er preget av et åpent «marked» hvor tjenester og kapasiteter, som utvikling av skadevare, utnyttelse av sårbarheter og automatiserte angrepsverktøy, kan kjøpes og brukes uten behov for betydelig egenkompetanse. Dette har gjort det mulig for aktører å gjennomføre avanserte operasjoner, ved å sette sammen ulike kjøpte komponenter, fremfor å utvikle dem selv.

Basert på dagens trusselbilde vurderer vi at dette økosystemet stadig blir mer sofistikert og kraftfullt. Vi forventer en økning i angrep fra både økonomisk motiverte kriminelle, og kriminelle proxy-aktører som opererer på vegne av statlige aktører. Samtidig ser vi en økt profesjonalitet i metodene som benyttes, og en utbredt bruk av kommersialiserte tjenester som effektiviserer angrepsprosesser. Dette forsterker behovet for robuste sikkerhetstiltak og tettere samarbeid mellom offentlige og private aktører for å imøtekomme et trusselbilde i utvikling.

Bruk av kunstig intelligens (KI)

Vi er sannsynligvis noen år unna å se bruk av KI i helautomatiserte angrep, men vi observerer allerede en økende bruk av «KI-assisterte» angrep. Dette inkluderer automatisering av phishing-kampanjer, oppdagelse av sårbarheter, og generering av unike skadevaremoduler, samt kodesegmenter. I denne sammenhengen har ondsinnede generative KI-modeller som eksempelvis FraudGPT og WormGPT begynt å dukke opp som verktøy for kriminelle aktører. Disse modellene tilbys på det mørke nettet og senker terskelen for mindre erfarne aktører til å gjennomføre mer sofistikerte angrep.

I tillegg ser vi økt bruk av generativ KI [1], som store språkmodeller (LLM), eksempelvis ChatGPT, i desinformasjonskampanjer og påvirkningsoperasjoner. Disse modellene brukes til å generere store mengder troverdig tekstinnhold for å manipulere opinion, plante falsk informasjon, eller skape misnøye og opprør i samfunnsstrukturer. Selv om «deepfakes» foreløpig ikke har hatt den gjennomslagskraften som mange forutså, har det blitt brukt målrettet i spesifikke kampanjer, særlig for sosial manipulering, bedrageri og påvirkningsoperasjoner rettet mot beslutningstakere eller virksomheter.

KI er fortsatt i en tidlig fase når det gjelder anvendelse i digital sikkerhet, men potensialet er stort. mnemonic oppfatter imidlertid at det kommersielle markedet er i dag preget av «hype» og urealistiske forventninger til hva KI kan oppnå. Mange løsninger som lover revolusjonerende funksjonalitet leverer begrensede resultater, spesielt der de ikke har tilgang til data av høy kvalitet for å trene modellene, eller ikke er tilstrekkelig integrert med eksisterende sikkerhetsløsninger.

Kombinasjonen av kommersielt tilgjengelige modeller og ondsinnede KI-plattformer, som FraudGPT og WormGPT, gjør det tydelig at vi går inn i en ny fase i trusselbildet, der kampen om KI-kapasiteter kan bli avgjørende for sikkerhetslandskapet.

1 Generativ kunstig intelligens er teknikker innen maskinlæring der målet er å etterligne et datamateriale, jf. Store norske leksikon

7.2 Erfaringer fra Coop

Effektivt samarbeid med politiet – en suksesshistorie fra Coop

En virksomhet står aldri alene når det gjelder å håndtere svindel og økonomisk kriminalitet. Dette ble tydelig for Coop Norge da vi tidlig i 2024 oppdaget et større forsøk på svindel rettet mot vår e-handelsplattform. Saken viser hvordan et godt samarbeid med politiet, kombinert med innsatsen fra operative ressurser i saksmottak og etterforskning, kan gi raske og effektive resultater.

Tidlig oppdagelse og godt forarbeid

Det hele startet med at Coops sikkerhetsavdeling identifiserte uregelmessigheter i transaksjoner som først virket som isolerte tilfeller. Gjennom grundig internt arbeid, inkludert dokumentasjon av transaksjonslogger, IP-adresser, kortdata og handlingsmønstre, ble det raskt klart at dette dreide seg om en systematisk og sofistikert svindeloperasjon. Etter å ha samlet og organisert informasjonen kontaktet vi politiet.

Det godt dokumenterte forarbeidet vårt ble trukket frem av politiet som en viktig årsak til at etterforskningen kunne starte umiddelbart. Alt lå til rette for en rask og effektiv innsats, noe som ble en nøkkelfaktor i sakens videre utvikling.

Politiets næringslivskontakt som nøkkel

Politiets næringslivskontakt i Sørøst politidistrikt spilte en viktig rolle i å etablere en god dialog med ressurser på riktig nivå i politiet. Slik fikk vi tilgang til operative ressurser som arbeidet raskt og presist. I løpet av mindre enn én uke var hovedgjerningsmannen pågrepet, beslaglagt utstyr sikret, og saken ble overlatt til påtalemyndigheten for videre håndtering. Det gjenstår fortsatt noe etterforskning, men påtalemyndigheten har vært tett involvert hele veien.

Dette understreker viktigheten av å benytte politiets næringslivskontakter. De kjenner godt til næringslivets utfordringer og kan bidra med råd og formidling som gjør en forskjell.

Anbefalinger til andre virksomheter

Erfaringen fra denne saken viser hvor viktig det er for virksomheter å være proaktive i kampen mot økonomisk kriminalitet. Våre anbefalinger er klare:

- **Vær forberedt:** sørg for å oppdage og dokumentere mistenkelig aktivitet tidlig. Gode interne rutiner kan være avgjørende.
- **Engasjer politiets næringslivskontakter:** de er en verdifull ressurs med ekspertise og nettverk som kan hjelpe deg å komme i kontakt med riktig instans i politiet.
- **Samarbeid for å beskytte samfunnet:** ved å samarbeide med politiet og andre aktører bidrar vi ikke bare til å beskytte egen virksomhet, men også til å redusere risikoen for andre bedrifter og forbrukere.

Samfunnsansvar i praksis

Som en av Norges største virksomheter ser Coop det som en del av vårt samfunnsansvar å bidra til å beskytte norske bedrifter og forbrukere mot økonomisk kriminalitet. Gjennom samarbeidet med politiet har vi vist at det er mulig å håndtere slike saker effektivt – og samtidig lære av prosessen for å styrke fremtidige tiltak.

Denne suksesshistorien er ikke bare vår. Den er et eksempel på hva som kan oppnås når næringslivet og politiet jobber sammen mot felles mål. Vi håper dette kan inspirere andre virksomheter til å ta i bruk de ressursene som finnes og aktivt bidra til et tryggere og mer robust samfunn.

7.3 Erfaringer fra Telenor

Trusselsituasjonen i og mot Norge har endret seg mye de siste årene. Som et resultat har også trusselen mot Telenor og våre kunder økt. Trusselaktørene som angriper Telenor og våre kunder, er interessert i alt fra å stjele penger fra oss eller kundene, skape forstyrrelser, gjennomføre målrettet innsamling av data og informasjon, inkludert kartlegging av nettverk for seinere angrep, eller gjøre konkrete forberedelser for angrep.

Telenors sikkerhetssenter har i snitt håndtert mer enn 20 alvorlige hendelser månedlig det siste året. Dette dreier seg blant annet om avverging av ransomware-angrep og fjerning av såkalte «informasjons-stjelere» i nettverk, som brukes av kriminelle til å hente ut lister med brukernavn fra bedriften.
I tillegg registreres det hver måned i snitt rundt 140 DDoS-angrep (tjenestenektangrep) mot Telenor infrastruktur og kunder av Telenor med DDos-beskyttelse, som har som mål å overbelaste og lamme servere og nettverk

En dreining i angrep av norske virksomheter

Det siste året har sikkerhetssenteret registrert endringer i måten norske virksomheter angripes på. Det er spesielt to fremgangsmåter som utmerker seg.

1) Stjeler ansattes brukernavn og passord eller session-tokens

En av de mest utbredte metodene som brukes for å angripe virksomheter, er at kriminelle overtar og utnytter virksomhetens legitime brukerkontoer, framfor å utnytte svakheter.
Dette skjer blant annet ved at:

- Angriperne bruker passord som er lekket etter datainnbrudd på andre tjenester, og matcher disse med brukere som har brukt tilsvarende passord på jobbkontoen.
- Angriperne tester de mest utbredte passordvariantene mot tusenvis av brukere i ulike bedrifter.
- En ansatt blir lurt til å installere en «informasjons-stjeler» på PC-en, som kopierer ut innloggingsdetaljer og session-cookies. Dersom man får tilgang til session-cookies eller andre session-tokens, vil angriperen ha tilgang til systemet uten å trenge passordet.
- En ansatt blir lurt til å oppgi brukernavn og passord ved hjelp av phishing.

Dersom virksomheten benytter seg av skytjenester kan denne typen angrep få store konsekvenser fordi angriperen lett kan få tilgang til flere ulike systemer via én konto.

2) Kommer seg inn via edge devices

En annen fremgangsmåte angriperne ofte benytter seg av, er å aktivt gå etter såkalte edge devices i virksomhetens nettverk.

Dette er endepunkter i nettverket som er eksponert direkte mot nettet.

Blant annet dreier dette seg om VPN-endepunkter, MDM-servere, e-postservere og fildelingsservere. Mange av disse har begrensede sikkerhetssystemer, og kan være relativt enkle å kompromittere. Problemet omfatter også edge devices som er designet for å stå direkte eksternt eksponert, da de ikke er «vanlige» servere og vedlikeholdsaktivitet på dem ofte vil gi tjenesteavbrudd. Da blir sikkerhetspatching ofte hengende langt etter, med sårbarhet som resultat. Det er også en rekke eksempler på at sårbarheter i management web-grensesnitt på edge devices blir utnyttet, noe som strengt tatt ikke burde vært eksponert til hele internett i det hele tatt.

Etter å ha fått tilgang via en slik enhet, kan angriperne hente ut lister med brukernavn og forflytte seg videre innover i nettverket.

Kjøper cyberangrep

Den teknologiske utviklingen og profesjonaliseringen innen cyberkriminalitet gjør muligheten til å angripe mye mer utbredt. Tidligere var man prisgitt egen teknologisk evne for å utføre angrep, men nå kan trusselaktører – spesielt økonomisk motiverte - i stor grad kjøpe dette som tjenester gjennom samvirkende nettverk av stadig mer spesialiserte organiserte kriminelle aktører. Både ransomware- og ande skadevareangrep, samt phishingkampanjer, kan lett kjøpes som tjenester på nett.

Et eksempel på skadevareangrep som kan kjøpes på nett er «Lumma stealer.» Her blir brukerne lurt til å laste ned skadevare som stjeler informasjon fra nettverket, som kan brukes til å gjøre ytterligere skade eller legge grunnlaget for nye angrep.

Ransomware gjennomføres nå raskere enn noen gang, og evnen til å detektere, rapportere og håndtere indikasjoner på et ransomware-angrep er viktigere enn noensinne. Tidligere har fremgangsmåten vært å kryptere data for å be om løsepenger. Nå ser vi at dette kombineres med trusler om videresalg av den krypterte informasjonen, og for mål der trusselen om publisering vurderes å være tilstrekkelig, tar angriper seg iblant ikke bryet med å kryptere.

Sommeren 2024 oppdaget man også de første eksemplene på Vultur i Norge. Vultur er en ondsinnet banktrojaner som først ble oppdaget i 2021. Programvaren, en modifisert versjon av McAfee Security-appen, gir svindlerne tilgang til offerets telefon og bankinformasjon. Skadevaren ble spredt via SMS som ga seg ut for å være fra et inkassoselskap

7.4 Erfaringer fra Netsecurity

Netsecurity observerer flere trender som vil forme fremtidens trusselbilde. En av de mest markante endringene er den økte kompleksiteten i cybersikkerhetslandskapet. Flere norske virksomheter er i gang med arbeidet knyttet til informasjonssikkerhet, men fremdeles har vi en vei å gå særlig innenfor områdene risiko- og sikkerhetsstyring, samt beredskap, hvor det har vært store forskjeller i arbeidet gjort av små og mellomstore virksomheter i Norge.

Netsecurity har registrert betydelige forskjeller i hvordan norske virksomheter håndterer informasjonssikkerhet. Til tross for at det finnes flere prosesser for å ivareta informasjonssikkerheten, er disse prosessene i varierende grad etterlevd. Dette fører til utfordringer som avhengighet av enkeltpersoner, spesielt i mindre bedrifter der kompetansen på informasjonssikkerhet ofte er knyttet til noen få nøkkelpersoner. Denne situasjonen skaper en risiko for kontinuiteten i sikkerhetsarbeidet, ettersom det kan være vanskelig å opprettholde sikkerhetsstyringen uten tilstrekkelig menneskelige ressurser og relevant kompetanse. Selv med lov om digital sikkerhet på trappene har det vært stor variasjon blant små og mellomstore virksomheter når det gjelder i hvilken grad de har kartlagt hvor virksomheten står i dag mot de forventede

kravene i loven. Samtidig er det mange SMB'er som ikke vil underlegges digitalsikkerhetsloven, som bidrar til at informasjonssikkerhet ikke får nødvendig fokus i daglig drift. Netsecurity erfarer at mange virksomheter er mer opptatte av om de er underlagt lovkrav eller ikke, fremfor å fokusere på og prioritere sikkerhetsarbeid. Alle virksomheter, uavhengig av underleggelse, oppfordres til å følge lovkravene i digitalsikkerhetsloven for å unngå å bli et svakere ledd i kjeden og dermed mer attraktivt mål for trusselaktørene.

Økonomisk motivasjon fortsetter å være den dominerende drivkraften bak cyberangrep, men de geopolitiske spenningene har ført til en økning i angrep rettet mot kritisk infrastruktur. Som en konsekvens av den pågående geopolitiske situasjonen, hvor Norge har blitt en sentral energileverandør til Europa, har landet blitt et mer attraktivt mål for cyberoperasjoner. Dette understreker behovet for å styrke beskyttelsen av Norges kritiske infrastruktur. Statlige aktører, spesielt fra Russland og Kina, utgjør en betydelig trussel mot Norges sikkerhet. Disse aktørene benytter et bredt spekter av metoder, inkludert nettverksoperasjoner, rekruttering av kilder og strategiske oppkjøp for å få tilgang til sensitiv informasjon og påvirke beslutningsprosesser. Netsecurity samarbeider med kunder i alle sektorer og ser at det er nødvendig å etablere felles risikoforståelse for alle typer trusler som er aktuelle for virksomhetene.

Daglig ledelse og styre har vanligvis god forståelse for HMS-risiko og storulykkepotensiale for industrivirksomheter. På den andre siden har toppledelsen ofte begrenset forståelse for hvordan cybertrusler kan utgjøre en fare for OT-miljøet og hvordan disse truslene kan resultere i HMS-ulykker og storulykker. Den økende integrasjonen mellom IT og OT skaper nye sårbarheter og utvider angrepsflatene, noe som kan få alvorlige konsekvenser for drift og sikkerhet. For å håndtere disse risikoene må integrasjoner og avhengigheter også risikovurderes. Dette krever tydelig ansvarsfordeling, tettere samarbeid mellom IT og OT, og en helhetlig tilnærming for å sikre motstandsdyktighet mot trusselaktører.

Samlet sett viser disse trendene at cybersikkerhet også i fremtiden vil kreve en helhetlig tilnærming, der både teknologi, menneskelige ressurser og lovgivning må integreres for å møte de økende truslene. Sikkerhet må være en integrert del av virksomheters digitale transformasjon, og det er avgjørende å investere i både kompetanseutvikling og robust infrastruktur for å sikre fremtidig motstandskraft. Netsecurity ser at alle sektorer kan bli utsatt for cyberoperasjoner gjennom målrettede cyberangrep, eller ved tilfeldigheter og/eller uflaks. Virksomheter som systematiserer sitt arbeid med informasjonssikkerhet ved å anvende ulike rammeverk og/eller standarder står bedre rustet til å håndtere informasjonssikkerhetshendelser.

7.5 Erfaringer fra Abelia

Norske bedrifter blir angrepet hver dag

Ifølge NHO og Næringslivets Sikkerhetsråd har hver femte norske bedrift opplevd forsøk på digital kriminalitet. Mange velger å ikke anmelde, og mørketallene er store.

Vi som arbeidsgivere og bedriftsledere må være vårt ansvar bevisst, og forstå alvoret i situasjonen. Det organiserte arbeidslivet har en avgjørende rolle den i digital sikkerheten.

Det er bedriftene i Norge som forvalter noe av den mest kritiske infrastrukturen. Det kan være 5G-nettet, datasentre, banksystemene og energisystemene våre. Med andre ord er det ikke bare viktig for bedriftene at ledere har kunnskap om sikkerhet, det er viktig for hele Norge. Derfor bekymrer det Abelia at vårt omstillingsbarometer viser at det er stor mangel på IT-sikkerhetskompetanse i Norge, selv om oppmerksomheten rundt temaet er stadig økende.

Telenors sikkhetspuls-undersøkelse viste at ni av ti personer er blitt forsøkt svindlet, og at Telenor alene stoppet mer enn 300 millioner forsøk på digital kriminalitet i fjerde kvartal 2024. Og når cyberkriminalitet vokser seg til å bli den tredje største økonomien i verden, bak USA og Kina, bør innsatsen for å motvirke dette trappes opp tilsvarende.

Bedriftene trenger både kompetanse og kunnskap for å kunne jobbe tilstrekkelig aktivt med sikkerhet og beredskap. I en nyere medlemsundersøkelse fra Abelia svarer mindre enn halvparten at de jobber aktivt med risikovurderinger på dette området, og over 20 prosent jobber lite eller ikke med det i det hele tatt. Det er et tankekors, i den verden vi lever i.

Særlig for små og mellomstore bedrifter er risikoen høy, og kunnskapsbehovet stort. For å sikre arbeidsgivere og arbeidstakere når verden blir mer urolig, er samarbeid vårt beste forsvar. Det gjelder samarbeid i Norden, med deling av erfaringer og personell. Men også samarbeid mellom offentlig og privat sektor. I dag er dessverre ansvarsoppgaver og informasjon svært fragmentert. Abelia har derfor lenge bedt om en felles informasjonsportal for digital sikkerhet.

I tillegg til en mer koordinert organisering, og bedre informasjonsdeling, er også kompetanse sentralt. Her er det positive signaler i totalberedskapsmeldingen, som vi håper følges opp. Innføring av nye regler for IKT-sikkerhet, krever at folk har kunnskap til å iverksette dem. Dette handler om god opplæring av eksisterende ansatte, men også om at det må bli lettere for bedriftene å ansette utenlandsk kompetanse, og om at vi må utdanne flere IKT-spesialister.

Vi ser til stadighet eksempler på hvordan dataangrep setter viktige samfunnsfunksjoner ut av spill, og mange angrep hører vi ikke om fordi de har blitt stoppet. Det skal ikke mer enn én ansatt til for at sikkerheten skal svekkes. Derfor trenger vi: Bevisste arbeidstakere, tydelig kultur og ledelse fra arbeidsgivere, og aktiv politikk og informasjonsdeling fra myndighetene om digital sikkerhet.

8.

Forebyggende aktivitet og trender

Dette kapittelet handler om hvordan virksomhenene kan forebygge hendelser, og er skrevet av mnemonic.

8.1 Sårbarheter

Sårbarheter i det digitale domenet utnyttes stadig raskere og mer raffinert av trusselaktører. I 2023 og 2024 har vi sett en videre økning i angrep som tar sikte på utnyttelse av tredjepartsapplikasjoner, eksponerte tjenester på internett, og ikke-patchede systemer. Trusselaktører benytter også i økende grad sårbarhetskjeder for å oppnå større innvirkning, noe som skaper utfordringer for virksomheter i alle sektorer.

Tredjepartsapplikasjoner

Mange virksomheter er avhengige av tredjepartsapplikasjoner for daglig drift. Disse applikasjonene kan utgjøre en kritisk del av virksomhetens økosystem, men kan også være en inngangsport for trusselaktører. I flere tilfeller har vi sett at trusselaktører retter seg mot leverandører i forsyningskjeden for å få tilgang til større mål.

Eksempler på slike angrep inkluderer kompromittering av applikasjoner for fjernstyring og samarbeidsverktøy som ansatte bruker for å koble seg til virksomhetens nettverk. Dette kan også omfatte systemer som er designet for å styrke nettverkssikkerheten, men som ender opp med å bli sårbarheter og inngangspunkter for kompromitteringer. Når disse applikasjonene eller systemene ikke oppdateres regelmessig, eller er tilstrekkelig konfigurert sikkerhetsmessig, kan trusselaktører enkelt utnytte kjente sårbarheter for å få et innledende fotfeste i virksomheten.

Tjenester eksponert mot internett

Tjenester og applikasjoner som eksponeres på internett er blant de mest utsatte målene for angrep. Dette inkluderer blant annet epostservere, nettapplikasjoner, CRM-tjenester og skytjenester. Hvis disse ikke er beskyttet med robuste autentiseringsmekanismer, herdet sikkerhetskonfigurasjon og kontinuerlig sikkerhetsmonitorering, kan trusselaktører utnytte sårbarhetene for å få tilgang til sensitive data, eller til og med hele nettverk. Et typisk eksempel er utnyttelsen av uautentisert tilgang til API-er, hvor trusselaktører har klart å omgå sikkerhetsmekanismer og stjele store mengder data fra eksponerte systemer.

I de fleste større hendelsene hvor mnemonic har bistått kunder i 2023–2024, har inngangsvektoren vært en sårbarhet i en applikasjon som er eksponert på internett. I hovedsak har dette skyldtes manglende patching og en mindre robust infrastruktur for å forhindre videre lateral bevegelse. Vi har også sett flere tilfeller hvor årsaken til inntrengning er innlogging med gyldige brukernavn og passord som trusselaktører har skaffet seg gjennom kjøp på darkweb, stjeling av data fra virksomheten, eller brute-force angrep.

Raskere utnyttelse av sårbarheter

Tiden fra offentliggjøring av en sårbarhet til den blir utnyttet («time-to-exploit») har blitt ytterligere redusert siden forrige rapporteringsperiode. Tidligere kunne virksomheter ha dager eller uker på å implementere patcher, men nå blir sårbarheter ofte utnyttet innen timer. En viktig trend i denne sammenheng er bruken av automatiserte verktøy som skanner internett etter nye sårbarheter umiddelbart etter utgivelse av patch. Disse verktøyene kan raskt gi aktører tilgang til systemer og nettverk som mangler oppdaterte sikkerhetsløsninger.

Et annet moment er at avanserte aktører i økende grad vil forsøke å beskytte nye «zero-day» sårbarheter så lenge som mulig, før de blir offentlig kjent. Denne tilnærmingen påvirker angrepsmetodikken ved at slike sårbarheter kun benyttes når det er strengt nødvendig for å nå gitte mål, og disse målene må ha høy verdi før sårbarheten utnyttes. I tillegg, når sårbarheten først blir kjent, spesielt ved publisering av «Proof-of-Concept» kode, utnytter andre og opportunistiske aktører raskt tidsrommet før en patch er tilgjengelig, ofte ved hjelp av automatiserte skannings- og utnyttelsesverktøy. Vi har også sett eksempler på utnyttelse før patcher er lansert, ofte basert på informasjonsinnhenting fra åpne utviklerfora hvor «kodebugs» blir diskutert.

8.2 Anbefalte tiltak

Basert på det trusselbildet vi ser, er det avgjørende at både offentlige og private aktører prioriterer sikkerhetstiltak, investerer i robust digital infrastruktur og styrker deres samarbeid på tvers av sektorer, offentlige og private virksomheter, og nasjoner, spesielt når det gjelder tidsriktig deling av data og informasjon om trusler og angrepsmetoder. En solid digital infrastruktur, kombinert med en proaktiv tilnærming til digital sikkerhet, vil ikke bare redusere sårbarhetsflaten for angrep, men også styrke evnen til å oppdage, håndtere og respondere på hendelser når de oppstår. Dette er avgjørende for å møte utfordringene i et stadig mer komplekst, sammensatt og uforutsigbart trusselbilde.

Som anbefalte tiltak ønsker vi spesielt å fremheve noen forhold, basert på de fire hovedkategoriene i NSMs grunnprinsipper for digital sikkerhet

1. Identifisere og kartlegge

For å håndtere risikoen knyttet til eksponerte tjenester, bør virksomheter først gjennomføre regelmessige risikovurderinger og kartlegge hvilke systemer og applikasjoner som er tilgjengelige på Internett. Mange virksomheter er ikke klar over hva de eksponerer, noe som gjør dem sårbare for angrep.

I tillegg er det viktig å implementere sikkerhetsoppdateringer og patching uten forsinkelse, samt bruke sterke autentiseringsmekanismer som flerfaktorautentisering (MFA) for å beskytte eksponerte tjenester. I denne sammenheng bør sikkerhetsstyrken til de ulike MFA-løsningene vurderes, og her fremhever vi spesielt phishing-resistent MFA som FIDO og PKI-baserte løsninger. Nettverkssegmentering og isolering av kritiske systemer kan også bidra til å begrense konsekvensene av et angrep.

2. Beskytte og opprettholde

For å sikre hybride infrastrukturer er det avgjørende å etablere en robust arkitektur og riktig konfigurasjon og herding av skytjenester. Det er spesielt viktig i denne sammenheng å ha full kontroll over API-nøkler og aksesstoken, og sørge for at omfanget (scope) for disse nøklene er redusert til et absolutt minimum innenfor de tjenesteområdene de brukes til.
I hybride arkitekturer er det essensielt å ha kontroll på identitets- og tilgangsstyring. Effektiv beskyttelse og kontroll av tilganger er avgjørende for å hindre misbruk, spesielt med et økt fokus på «credential harvesting»-operasjoner fra kriminelle aktører. En nyere endring er at økt bruk av MFA har ført til utviklingen av angrep som forsøker å omgå slike mekanismer, som for eksempel Adversary in The Middle («AiTM»). Virksomheter bør tilstrebe å etterleve «least privilege»-prinsippet for sine identiteter, og kartlegge mulige bevegelseskanaler fra sky- til on-premise miljøer.

3. Oppdage

For å oppdage og håndtere sikkerhetshendelser effektivt, er det avgjørende å ha kontinuerlig sikkerhetsmonitorering av innsamlet data. Her kan med fordel virksomheter kartlegge hvilken telemetri som er tilgjengelig i sine sky-løsninger, og vurdere kompenserende tiltak dersom dette ikke er tilstrekkelig for å håndtere angrep utfra virksomhetens trusselprofil. Ved mistanke om inntrenging er det viktig å ha evnen til rask nedstengning av berørte systemer for å begrense skaden.

Logging av brukeraktivitet spiller en sentral rolle, da den gir viktige spor ved datainnbrudd. Virksomheter bør ikke bare logge mislykkede innloggingsforsøk, men også vellykkede innlogginger, for å få et helhetlig bilde av hendelsen. Videre bør virksomheter loggføre brukeradferd for å identifisere unormal aktivitet og potensielle trusselaktiviteter. En effektiv tilnærming er å sikkerhetsmonitorere ikke bare systemtilgang, men også hvordan brukerne interagerer med applikasjoner og data. Dette kan bidra til å oppdage mistenkelige handlinger som ellers ville gått ubemerket hen.

4. Håndtere og gjenopprette

For effektivt å håndtere sikkerhetsangrep og påfølgende gjenoppretting, er det avgjørende at virksomheter har etablerte prosedyrer og et på forhånd grundig testet beredskapsplanverk. Å ha klare føringer for hvordan man raskt skal reagere på et angrep, kan gjøre forskjellen mellom en effektiv mitigering med minimal skade versus langvarige negative konsekvenser. Virksomheter bør derfor jevnlig gjennomføre øvelser, som for eksempel skrivebordsøvelser, der ulike scenarier simuleres for å teste og øve på virksomhetens evne til å håndtere alvorlige angrep. Slike øvelser kan også gi verdifull innsikt i mulige svakheter i eksisterende planer og prosesser.

I tillegg til å ha en solid og øvet beredskapsplan, er kontinuerlig evaluering og læring etter hendelser viktig for å forbedre fremtidig responsevne. Etter et angrep bør virksomheter grundig evaluere hvordan hendelsen ble håndtert, hvilke tiltak som var effektive, og hva som kan forbedres. Læring fra faktiske angrep, samt øvelser og simuleringer, er essensielt for å sikre at virksomheter er bedre forberedt på å håndtere fremtidige trusler. Gjennom kontinuerlig forbedring kan virksomheter styrke sine evner til å håndtere sikkerhetsangrep, øke sin digitale sikkerhetsforståelse, samtidig som de reduserer risikoen for gjentakelse.

Mørketallsundersøkelsen bekrefter den utviklingen NSM har sett de senere årene. De store virksomhetene, som ofte er leverandør av samfunnskritiske tjenester, har et rammeverk og/eller styringssystem for informasjonssikkerhet. Utfordringen er de mange mindre virksomhetene, som ikke har det. Små virksomheter med dårlig informasjonssikkerhet, kan være en enkel vei inn for trusselaktører. NSM anbefaler derfor alle virksomheter å benytte NSMs grunnprinsipper for IKT-sikkerhet. Det vil gjøre virksomheten mye mer robust mot digitale trusler.

Harald Kristian Næss, seksjonssjef for Råd og tiltaksutvikling ved Nasjonalt cybersikkerhetssenter.

Forside: Istock

Næringslivets
sikkerhets-
råd

www.nsr-org.no