Næringslivets sikkerhets-råd

# Mørketalls-undersøkelsen 2022

# INNHOLD

# FORORD

Da forrige mørketallsundersøkelse ble utgitt for to år siden var vi og verden preget av Covid-19-pandemien. Året ble beskrevet som et unntaksår, og spørsmålene knyttet til konsekvensen av den hurtige digitaliseringen var mange. Hvor sårbare var vi når det meste av virksomhet var flyttet til hjemmekontoret over natten? I dag kan vi si at vi kom godt ut av det. Effekten av den hurtige digitaliseringen vil tjene oss godt i fremtiden. Det er mulig å endre samfunnet raskt når vi må, og vi tilpasser oss raskt en ny virkelighet. Det trengs, for utfordringene har ikke blitt mindre i løpet av de siste to årene.

Det er krig i Europa. Det russiske angrepet på Ukraina 24. februar i år, innledet en ny sikkerhetspolitisk epoke. Krig mellom stater må igjen sees på som en realitet vi må ta hensyn til. Den militære seieren president Putin håpet å innkassere hurtig, kom ikke. I stedet har vi sett et fremoverlent Ukraina som har benyttet tiden siden 2014 til forberedelser. Ikke bare militært, men også sivilt har landet gjort en betydelig innsats for styrking av sitt totalforsvar. Den militære- og den sivile delen av samfunnet må kunne virke sammen – samtidig, om landet skal klare å motstå et angrep utenfra. Det gjelder i Ukraina, og det gjelder i Norge. Klarer vi det?

Fortsatt herjer pandemien i deler av verden. Det påvirker lange og kompliserte verdikjeder. Energimangel, strømpriser, inflasjon og politisk polarisering skaper vanskelige forhold for styrket samarbeid både nasjonalt og internasjonalt. Dette skjer i en tid der samarbeid om å møte klimautfordringene burde være første prioritet.

I skyggen av alle disse utfordringene opererer trusselaktører med ulike hensikter. Det digitale trusselbildet har i løpet av de siste årene gjennomgått et taktskifte. Såkalte sammensatte trusler vil prege vår fremtid slår Nasjonal sikkerhetsmyndighet fast i sin rapport Risiko 2022.

Årets Mørketallsundersøkelse vil bidra til å beskrive den digitale sikkerhetstilstanden i Norge. Det er den 13. undersøkelsen om den digitale sikkerhetstilstanden i norsk næringsliv og noen offentlige virksomheter. Undersøkelsen er utvidet med 1000 respondenter for å sikre et bedre statistisk grunnlag. I tillegg er noen av spørsmålene endret for å speile det aktuelle trusselbildet bedre. Vi håper Mørketallsundersøkelsen 2022 vil bidra til styrket strukturert og forebyggende sikkerhetsarbeid basert på økt kunnskap om risikobildet, og forslag om tiltak for å håndtere risikoen.

Jeg vil avslutningsvis rette en stor takk til alle som har støttet undersøkelsen økonomisk, og gitt sine bidrag til rapporten. Deres engasjement og vilje til å bidra til fellesskapet gjennom å dele erfaringer er uvurderlig for utvikling, aktualitet og kvalitet i sikkerhetsarbeidet.

Lykke til med det kunnskapsbaserte, strukturerte og forebyggende sikkerhetsarbeidet!

Oslo 9. september 2022.

Odin Johannessen
Direktør Næringslivets Sikkerhetsråd


NASJONAL
SIKKERHETSMYNDIGHET


DEN NORSKE KRIGSFORSIKRING FOR SKIB
GJENSIDIG FORENING


telenor


Statkraft


coop


NORGES BANK


ADVANSIA
PART OF AFRY


sopra steria


VISMA


ATEA


mnemonic


ARBEIDSGIVERFORENINGEN
SPEKTER


Norges
Rederiforbund
Norwegian
Shipowners'
Association


storebrand


transcendent
group
GOVERNANCE
RISK
COMPLIANCE


NTNU CCIS
Center for Cyber and
Information Security


NHO

# SAMMENDRAG

Forsøk på datainnbrudd / hacking og phishing er de mest vanlige hendelsene virksomheter med 5 ansatte eller flere utsettes for. Hhv. 10 og 9 prosent har blitt utsatt for dette i løpet av kalenderåret 2021. Blant de minst vanlige hendelsene finner vi misbruk av it-ressurser for utvinning av kryptovaluta sammen med tyveri eller eksfiltrasjon av data (begge 1 prosent).

Sammenlignet med tidligere undersøkelser er det langt lavere andel som oppgir at de har opplevd hendelser forårsaket av ansatte. I forrige undersøkelse fra 2020 spurte vi om hendelser i kalenderåret 2019, altså før pandemien og utstrakt jobbing fra hjemmekontor.

Av de som har opplevd hendelser er det 11 prosent som mener det skjedde som følge av bruk av hjemmekontor, men tilfeldigheter og uflaks er de vanligste årsakene til at uønskede hendelser skjer. Menneskelige feil og manglende sikkerhetsbevissthet blant de ansatte følger på de neste plassene.

Mens hendelsene i stor grad skyldes tilfeldigheter eller uflaks, er det også en stor andel av virksomhetene som oppdager hendelsene ved en tilfeldighet. 40 prosent av de som utsettes for hendelser, oppdager det ved en tilfeldighet. Like mange (41 prosent) oppgir imidlertid at de oppdaget hendelsen ved rutinemessig intern sikkerhetsmonitorering.

2 prosent har blitt utsatt for løsepengevirus. Blant disse er det ingen som oppgir at de har betalt for å bli kvitt løsepengeviruset eller betalt for at informasjon ikke skulle legges ut på nett. 1 prosent oppgir at de har betalt for at det ikke skal skje igjen, mens 26 prosent av de som var utsatt for løsepengevirus anmeldte til politiet.

For 19 prosent av de som opplever hendelser er en av konsekvensene et økonomisk tap. I 2 prosent av tilfellene fører det til oppsigelser, mens det mest vanlige er involvering av ledelse og styre. Samtidig er det over halvparten som endret policy eller rutiner som følge av hendelsen de opplevde. I løpet av det siste året er det 52 prosent som har gjennomført aktiviteter for å øke ansattes bevissthet rundt sikkerhet. Dette er mer vanlig blant de store virksomhetene, der 84 prosent har gjennomført aktiviteter, mens det er 47 prosent av de med 5 til 19 ansatte som har gjort det samme.

# INNLEDNING

## Bakgrunn

På oppdrag fra Næringslivets Sikkerhetsråd har Opinion gjennomført Mørketallsundersøkelsen 2022. Dette er den 13. gangen Mørketallsundersøkelsen gjennomføres av NSR. Før undersøkelsen i 2016 ble det gjort en del endringer i undersøkelsens spørsmål og datainnsamlingsmetode. Sammenligninger blir derfor ikke gjort med resultater tidligere enn 2016

## 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 3. mars til 12. mai 2022. Data er vektet på størrelse (antall ansatte) og bransje (RIM-vektet). Data for tidligere undersøkelser fra 2016, 2018 og 2020 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%.

## Karakteristikker

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

| Sektor | Antall (n) | Andel intervju |
|---|---:|---:|
| Privat | 2234 | 89 % |
| Offentlig | 266 | 11 % |
| Totalt | 2500 | 100 % |

## Virksomhetsstørrelse

Undersøkelsen omfatter virksomheter i følgende størrelsesgrupper.

| Virksomhetsstørrelse | Antall intervju | Andel intervju |
|---|---:|---:|
| 5 til 19 ansatte | 1520 | 61 % |
| 20 til 99 ansatte | 820 | 33 % |
| 100 ansatte eller flere | 160 | 6 % |
| Totalt | 2500 | 100 % |

## Geografi

Under er en oversikt over respondentenes fylkesvise tilhørighet:

| Region | Antall | Andel intervju |
|---|---|---|
| Nord-Norge | 298 | 12 % |
| Midt-Norge | 322 | 13 % |
| Vestlandet | 531 | 21 % |
| Østlandet | 730 | 29 % |
| Sørlandet inkl. TeVe | 328 | 13 % |
| Oslo | 291 | 12 % |
| Totalt | 2500 | 100 % |

## Bransje

Undersøkelsen omfatter virksomheter i følgende bransjer.

| Bransje | Antall | Andel intervju |
|---|---|---|
| Industri etc. | 375 | 15 % |
| Bygg- og anleggsvirksomhet | 370 | 15 % |
| Varehandel etc. | 594 | 24 % |
| Transport og lagring | 118 | 5 % |
| Overnattings- og serverings-virksomhet | 126 | 5 % |
| Tjenesteytende næringer | 543 | 22 % |
| Offentlig administrasjon | 54 | 2 % |
| Undervisning | 96 | 4 % |
| Helse og sosial | 165 | 7 % |
| Kulturell virksomhet | 59 | 2 % |
| Totalt | 2500 | 100 % |

# 1.

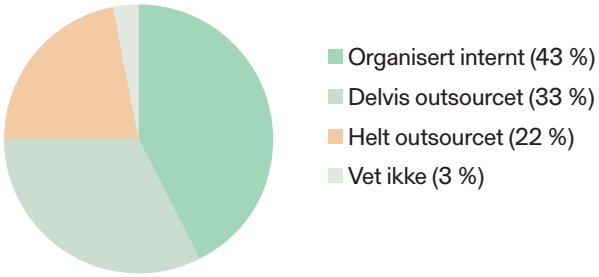
# Organisering av IT-driften

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

## 1.1 Outsourcing

22 prosent har helt outsourcet it-driften, mens 33 prosent har delvis gjort det. I 43 prosent av virksomheter med 5 ansatte eller flere er it-driften organisert internt. Resultatene er på nivå med tidligere undersøkelser (helt outsourcet: 22 prosent i 2016, 19 prosent i 2018, 22 prosent i 2020).

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




*Figur 1*

Det er ikke klare forskjeller på virksomheter i ulike størrelser på dette spørsmålet når det gjelder å sette ut driften helt. Virksomheter med 20 til 99 ansatte outsourcer delvis i noe større grad enn de minste bedriftene, mens de med 5 til 19 ansatte i noe større grad enn de mellomstore organiserer det internt. Virksomheter i overnatting og servering utmerker seg med å organisere internt i større grad enn andre, mens offentlige virksomheter i noe større grad enn private outsourcer helt.

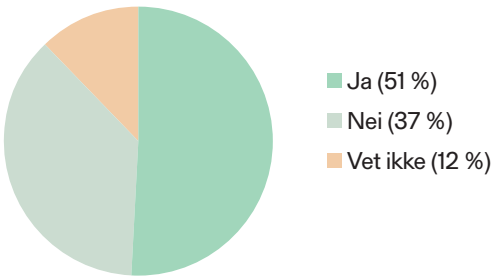
Blant de som benytter seg av outsourcing helt eller delvis, er det 14 prosent som benytter outsourcingtjenester i utlandet. Det er på nivå med de tre siste målingene. Det er ikke forskjell på virksomhetsstørrelse, mens det er noe mer vanlig i varehandel og tjenesteytende, samt i virksomheter med et rammeverk for informasjonssikkerhet og som driver med FoU.

Blant de som benytter outsourcingtjenester i utlandet, er det 78% som vet hvor data fysisk er lagret.

## 1.2 Styringssystem og rammeverk

Halvparten av virksomhetene har et rammeverk og/eller styringssystem for informasjonssikkerhet.

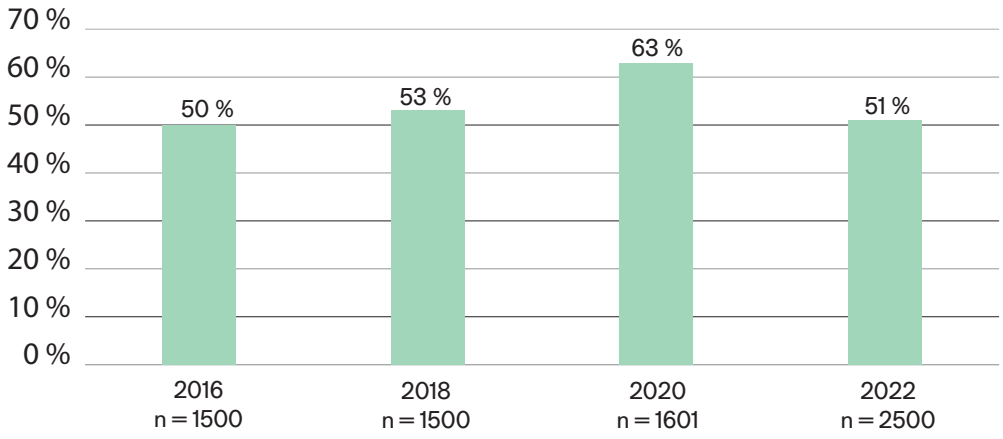
Figur 2. Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerhet? Total sample; base n = 2500




*Figur 2*

Sammenlignet med de foregående undersøkelsene er dette på nivå med 2016 og 2018, men noe lavere enn i 2020.

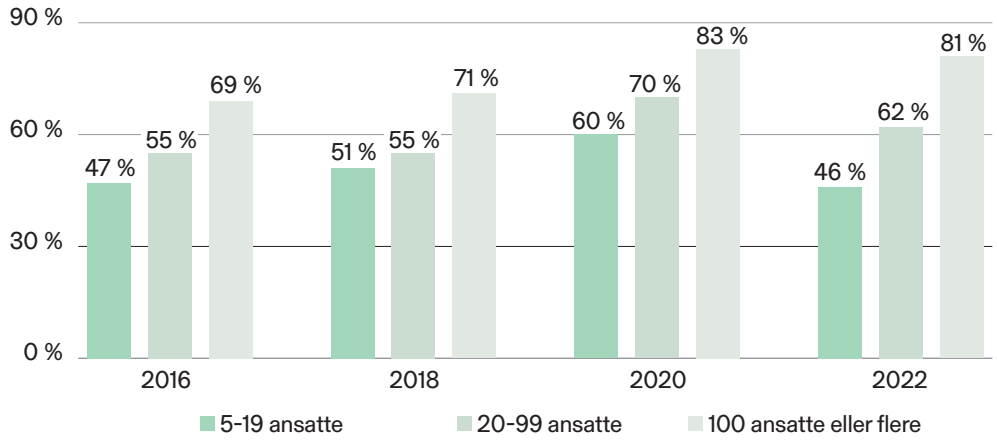
Figur 3. Har virksomheten et rammeverk og/eller styringssystem for informasjons-sikkerhet? ( andel som svarer ja) Total sample; base n = 7101




*Figur 3*

Store virksomheter har rammeverk i større grad enn små bedrifter. 46 prosent av virksomheter med 5 til 19 ansatte har det, 62 prosent av de med 20 til 99 ansatte og 81 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.
Total sample; base n = 7101

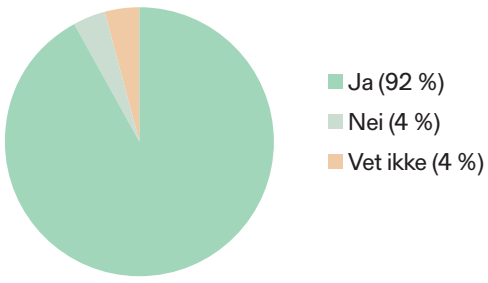



*Figur 4*

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 et 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.

De som har et rammeverk eller styringssystem mener i stor grad at det etterleves i organisasjonen. Ni av ti er av den oppfatningen. 92 prosent svarer ja, som er på nivå med 2018 og 2020 da hhv. 90 og 91 prosent svarte det samme.

Figur 5. Opplever du at rammeverket / styringssystem for sikkerhet blir etterlevd i organisasjonen? Total sample; base n = 1335; total n = 2500; 1165 missing




*Figur 5*

# 2.

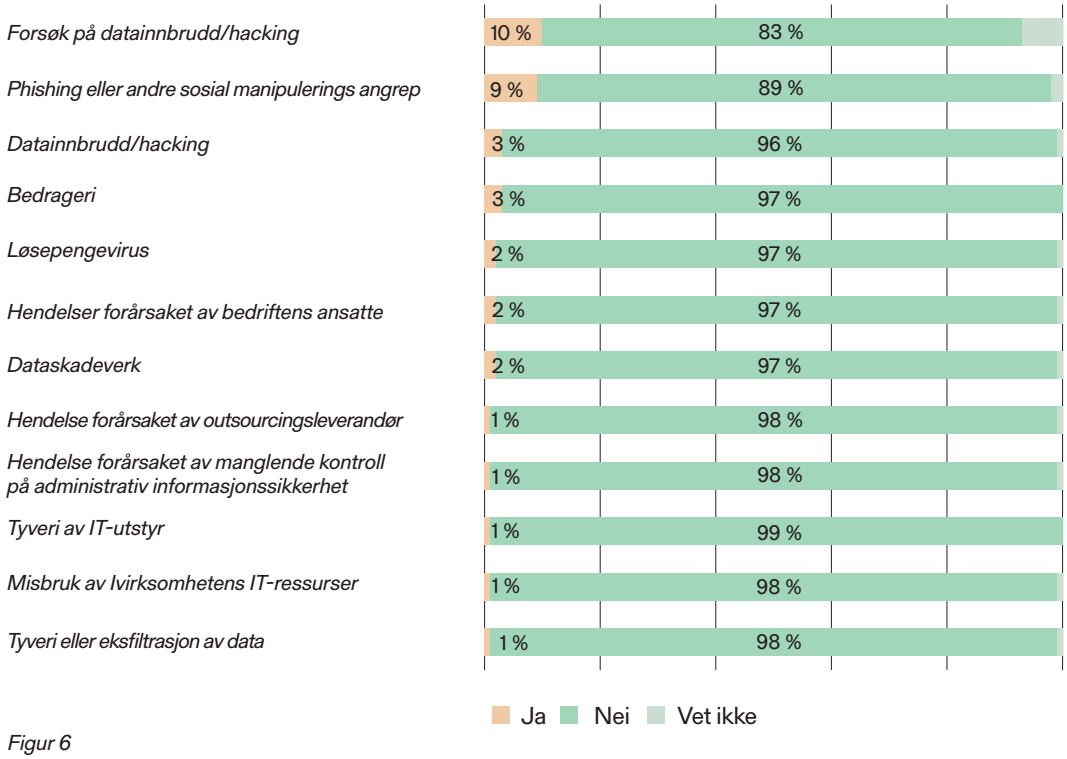
# Hendelser

Dette tema handler om hvilke informasjons-sikkerhetshendelser virksomhetene er utsatt for, hendelser med negativ påvirkning og hva som anses som de mest alvorlige hendelsene.

## 2.1 Informasjonssikkerhetshendelser

De mest vanlige uønskede hendelsene er forsøk på datainnbrudd / hacking og phishing eller andre manipuleringsangrep som 10 og 9 prosent av virksomhetene har vært utsatt for i løpet av kalenderåret 2021. Disse forholdene var også de mest vanlige i 2019. De minst vanlige hendelsene er tyveri eller eksfiltrasjon av data (0,7 prosent), misbruk av it-ressurser for utvinning av kryptovaluta, nedlasting av ulovlig innhold og/eller spredning av skadevare (0,8 prosent) og tyveri av it-utstyr (0,9 prosent).

*Figur 6. 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 2021? Total sample; base n = 2500*

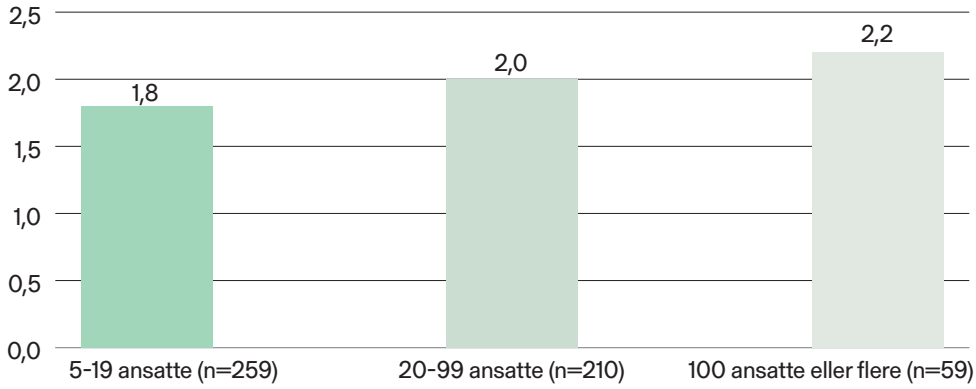



*Figur 6*

I gjennomsnitt er alle virksomhetene med 5 ansatte eller flere rammet av 0,4 av de ulike informasjonssikkerhetshendelsene vi har spurt om. (i 2019 var tallet 0,7 hendelser i snitt, men listen over hendelser vi spør om er endret, så dette er ikke sammenlignbare tall). Blant de som har opplevd en hendelse, har man i snitt opplevd 1,9 forskjellige type hendelser. I både 2018 og 2020 fant vi at store virksomheter hadde opplevd flere ulike typer hendelser. I år finner vi ikke signifikant forskjell når det gjelder størrelse. (Vi snakker her om antall forskjellige typer hendelser, ikke antall hendelser totalt.)

*Snitt antall type hendelser blant virksomheter (n=528 – svart ja på en eller flere alternativ i spørsmålet over).*

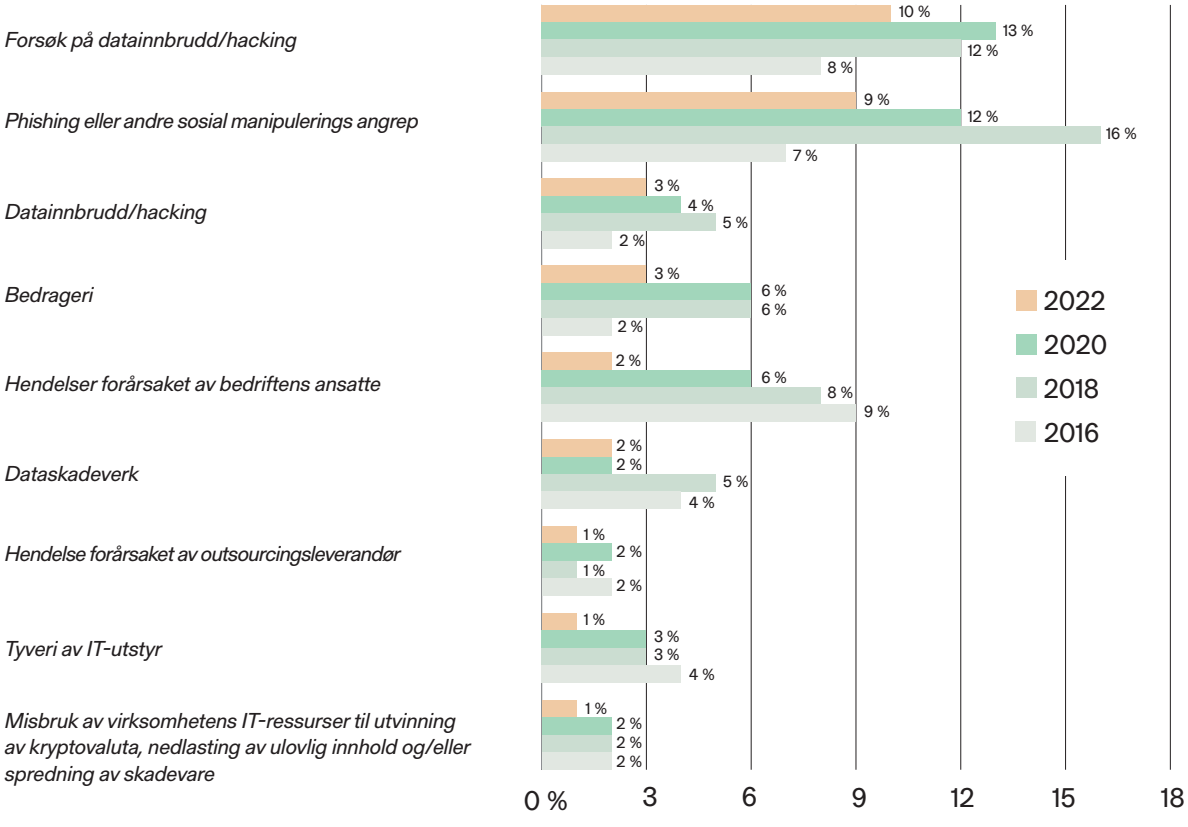
*Figur 7. Filter: Har opplevd hendelser; base n = 528; 79% filtered out*




*Figur 7*

Sammenlignet med tidligere undersøkelser, er det langt lavere andel som oppgir hendelser forårsaket av bedriftens ansatte. I og med at det er endringer i flere svaralternativer i dette spørsmålet, skal vi være forsiktig med å konkludere når det gjelder endringer over tid.

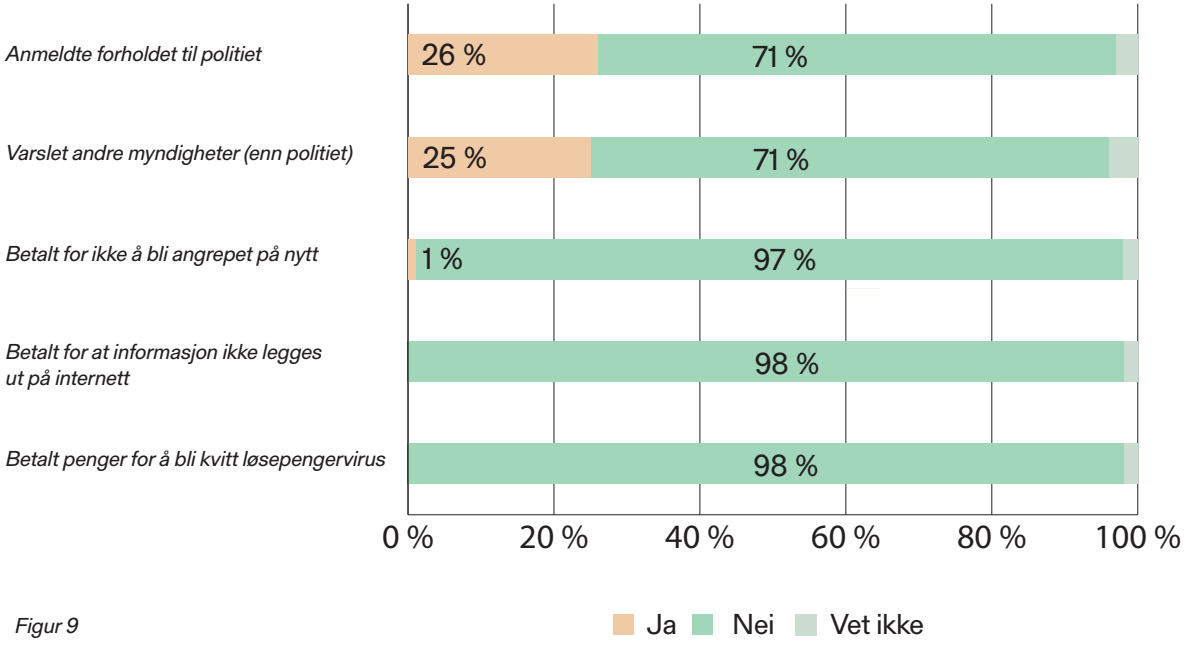
*Figur 8. Hendelser over tid. Total sample; base n = 7101*




*Figur 8*

De som svarer at de er utsatt for løsepengevirus har fått oppfølgingsspørsmål om hva de gjorde.

*Figur 9. I forbindelse med løsepengevirus, gjorde dere noe av følgende?*
*Total sample; base n = 63; total n = 2500; 2437 missing*




*Figur 9*

Av de som er blitt utsatt for løsepengevirus, er det 26 prosent som anmeldte det til politiet og 25 prosent varslet andre myndigheter. Det er ingen som oppgir at det har betalt for å bli kvitt løsepengevirus eller for at informasjon ikke skal legges ut på internett, men 1 prosent har betalt for å ikke bli angrepet på nytt.

## 2.2 Hendelser med negative konsekvenser

På spørsmål om informasjonssikkerhetshendelser som påvirket virksomheten negativt i form av økonomisk tap eller svekket markedsposisjon er det 10 prosent av virksomhetene som vet at de har hatt slike hendelser og som klarer å tallfeste hvor mange. 86 prosent svarer at de ikke har hatt hendelser med negative konsekvenser, mens 4 prosent ikke ønsker å oppgi om de har hatt slike hendelser eller ikke.

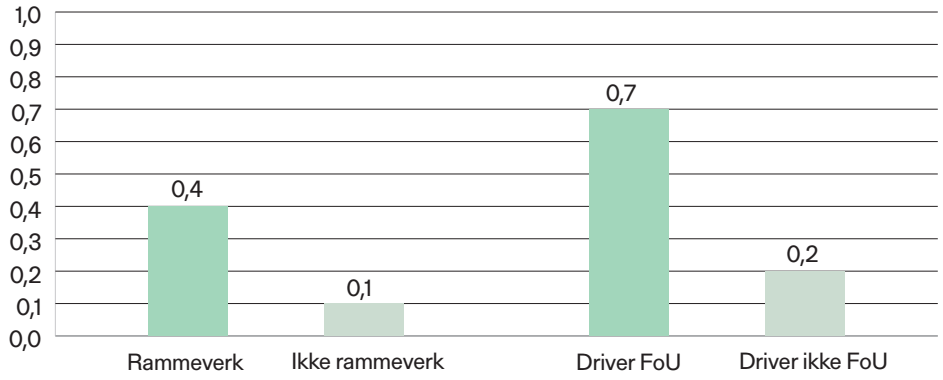
Blant de som har opplevd hendelser som har hatt negative konsekvenser med økonomisk tap eller svekket markedsposisjon, har man i gjennomsnitt opplevd 3 slike hendelser i løpet av 2021, mens median er 1 hendelse. I forrige undersøkelse var resultatet 9,4 i snitt og en median på 2, der noen få bedrifter med mange slike hendelser trakk snittet opp.

Hvis vi antar at de virksomhetene som ikke oppgir et antall, heller ikke er utsatt for slike hendelser, er gjennomsnittet i hele populasjonen (virksomheter med 5 eller flere ansatte) 0,3 hendelser med negative konsekvenser i løpet av 2021. I forrige undersøkelse var det klare forskjeller mellom små og store virksomheter. De med 5 til 19 ansatte hadde i snitt opplevd 0,85 hendelser med negative følger, mens snittet for de med 100 ansatte eller flere var 3,74. I årets undersøkelse finner vi ikke en signifikant forskjell selv om de store oppgir noe flere hendelser (5 til 19 ansatte har 0,26, 20 til 99 har 0,37 og 100 eller flere ansatte har et snitt på 0,7). Det er heller ikke signifikant forskjell på privat og offentlig sektor.

De som har et rammeverk for informasjonssikkerhet og de som driver med FoU opplever noe flere hendelser enn andre.

*Gjennomsnittlige antall hendelser med negative konsekvenser i form av økonomisk tap eller svekket markedsposisjon.*

*Figur 10. Gjennomsnittlige antall hendelser med negative konsekvenser i form av økonomisk tap eller svekket markedsposisjon. Total sample; base n = 2500*




*Figur 10*

Når det gjelder hva som var den mest alvorlige hendelsen, uavhengig av om hendelsen fikk negative konsekvenser eller ikke, så er det hacking, phishing, løsepengevirus og bedrageri som går igjen (stilt som et åpent spørsmål).

*Figur 11. Hva var den mest alvorlige hendelsen i 2021?*
*Total sample; base n = 550; total n = 2500; 1950 missing*


*Figur 11*

Når det gjelder grunnen til at man opplever en hendelse som den mest alvorlige, er det potensielt skade-omfang samt mulig og reelt økonomisk tap som er gjengangere.

# 3.

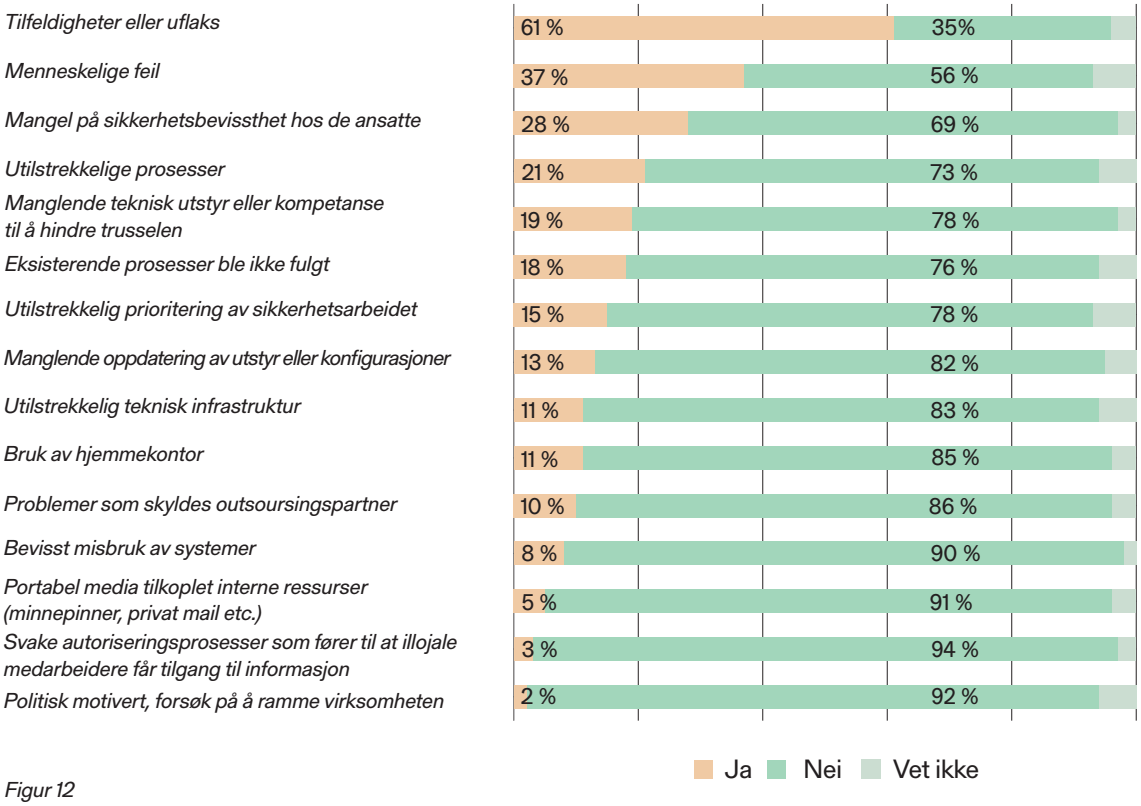
# Årsaker

Dette temaet handler om hvorfor sikkerhets-bruddene oppsto og hva som var årsaken til at virksomheten oppdaget hendelsen.

## 3.1 Hvorfor sikkerhetsbrudd oppsto

I størst grad mener norske virksomheter at sikkerhetsbruddene har oppstått som en følge av tilfeldigheter eller uflaks.

*Figur 12. Var noen av følgende faktorer medvirkende til at sikkerhetsbruddet oppsto?*
*Total sample; base n = 550; total n = 2500; 1950 missing*




*Figur 12*

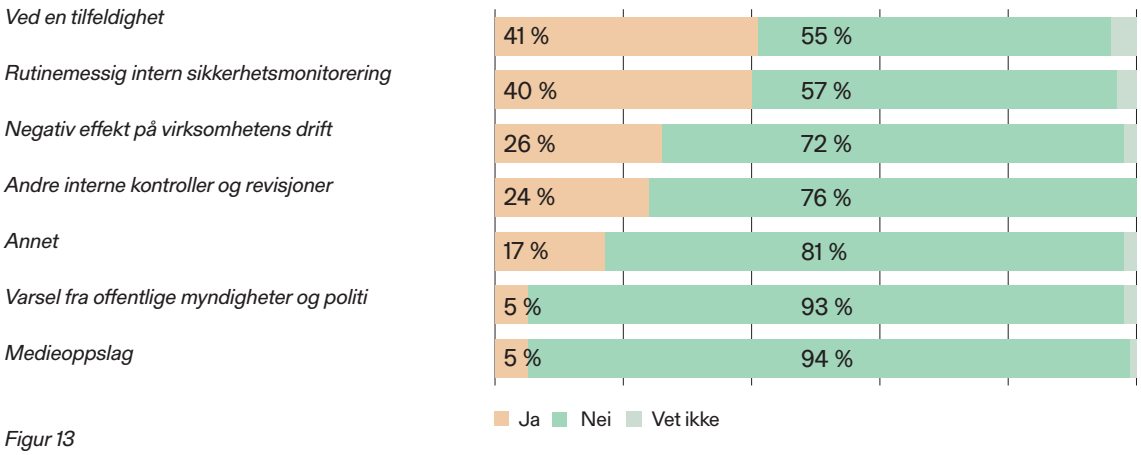
Blant de som har opplevd hendelser er det 61 prosent som mener årsaken var tilfeldigheter eller uflaks, mens 37 prosent mener det skyldes menneskelige feil.

Det er ikke klare forskjeller eller mønstre i hvilke type virksomheter som opplever de ulike årsakene til at sikkerhetsbrudd skjer. Det er enkelte signifikante forskjeller som at de minste virksomhetene i mindre grad enn større peker på mangel på sikkerhetsbevissthet blant ansatte og at prosesser ikke ble fulgt. At eksisterende prosesser ikke ble fulgt er også noe mer vanlig i virksomheter med et rammeverk for informasjonssikkerhet, mens problemer som skyldes outsourcing-leverandør er mer vanlig i privat enn i offentlig sektor.

## 3.2 Hvordan sikkerhetsbruddet ble oppdaget

Når det gjelder hvordan sikkerhetsbruddet ble oppdaget, er det like mange som sier det var en tilfeldighet som sier ved rutinemessig intern sikkerhetsmonitorering. Det samme fant vi i forrige undersøkelse.

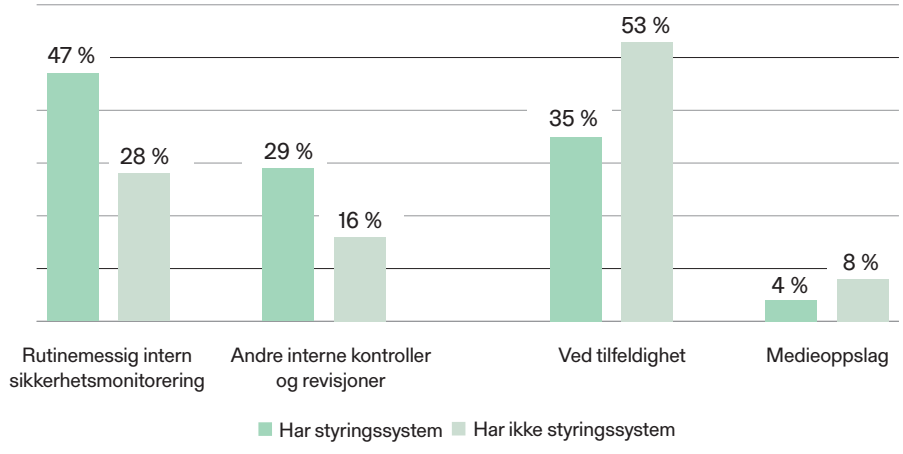
*Figur 13. Var noe av følgende årsak til at hendelsen ble oppdaget?*
*Total sample; base n = 550; total n = 2500; 1950 missing*




*Figur 13*

Virksomheter med et rammeverk for informasjonssikkerhet har i større grad enn andre oppdaget hendelsen ved rutinemessig kontroll og andre interne kontroller og rutiner. De som ikke har et rammeverk, har i større grad oppdaget hendelsen ved en tilfeldighet og via medieoppslag.

*Figur 14. Var noe av følgende årsak til at hendelsen ble oppdaget / styringssystem.*
*Total sample; base n = 550; total n = 2500; 1950 missing*

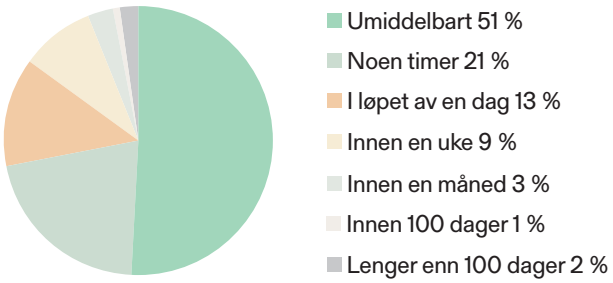



*Figur 14*

Store virksomheter (med 100 ansatte eller flere) oppdager forholdene i større grad på grunn av rutinemessig intern monitorering enn andre. Det samme gjelder offentlige virksomheter som skiller seg fra private på dette forholdet. Det er ikke klare forskjeller mellom ulike typer virksomheter når det gjelder hvor lang tid det tok å oppdage hendelsen. Offentlige virksomheter svarer i større grad enn private at de oppdaget det umiddelbart (64 mot 49 prosent), men svarer samtidig i større grad enn private at det tok mer enn 100 dager (6 mot 1 prosent).

*Figur 15. Hvor lang tid tok det fra hendelsen skjedde til den ble oppdaget?*
*Total sample; base n = 550; total n = 2500; 1950 missing*

*Figur 15*



# 4.

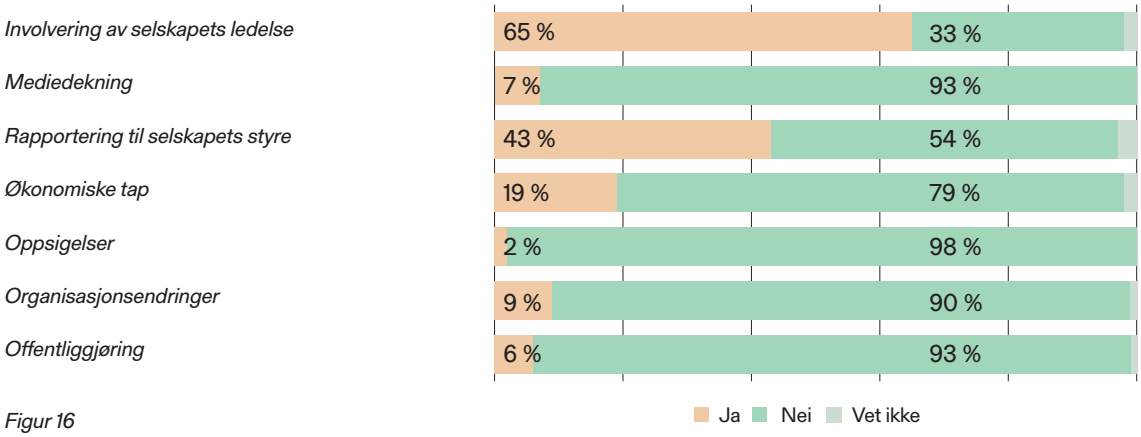
# Følger og håndtering av hendelser

Dette tema handler om forhold som hvilke følger hendelsen fikk, hvem den ble rapportert til, organisatoriske følger og kostnader.

## 4.1 Følger av hendelsen

I 65 prosent av virksomheter som er utsatt for informasjonssikkerhetshendelser er en av følgene at selskapets ledelse blir involvert i saken..

*Figur 16. : Førte denne spesifikke hendelsen til følgende? Respondent svarer utfra siste / mest alvorlige hendelse. Total sample; base n = 550; total n = 2500; 1950 missing*

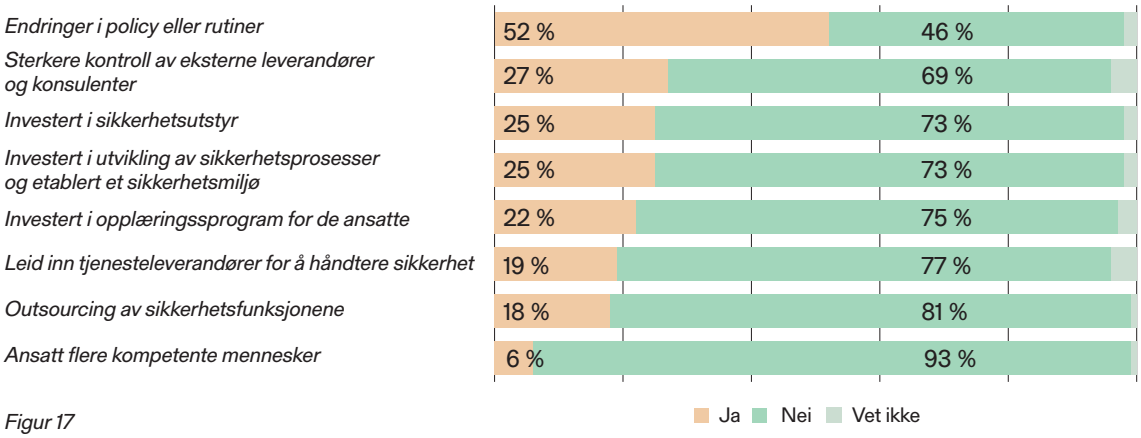



*Figur 16*

Involvering av selskapets ledelse og styre er de vanligste følgene, på samme måte som i tidligere undersøkelser. Involvering av selskapets ledelse er mer vanlig i private virksomheter enn i offentlige (67 mot 55 prosent), mens offentliggjøring er mer vanlig følge i offentlige virksomheter (11 mot 5 prosent). Virksomheter med et rammeverk for informasjonssikkerhet involverer styret i noe større grad enn andre (46 mot 36 prosent).

I tillegg til følgene nevnt over, har sikkerhetshendelsene også ført til endinger i en del av de utsatte organisasjonene, der 52 prosent har endret policy og rutiner.

*Figur 17. Som et resultat av hendelsen, ble noen av følgende endringer gjort i organisasjonen? Total sample; base n = 550; total n = 2500; 1950 missing*

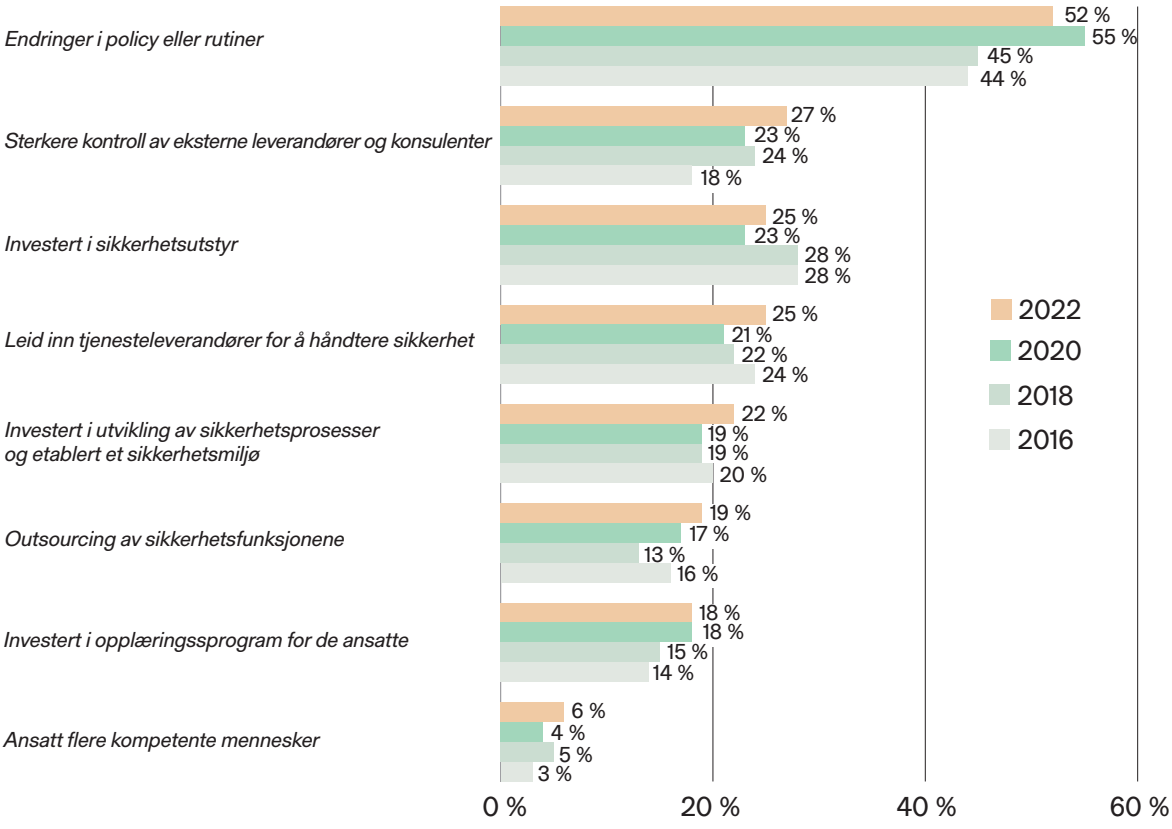



*Figur 17*

Virksomheter med 20 ansatte eller flere har i større grad enn mindre virksomheter investert i opplæringsprogram for de ansatte og investert i sikkerhetsutstyr. Virksomheter med et rammeverk for informasjonssikkerhet har i større grad investert i opplæringsprogram, investert i utvikling av sikkerhetsmiljø og innført sterkere kontroll av eksterne leverandører. Private virksomheter har outsourcet sikkerhetsfunksjonene i større grad enn offentlige, mens virksomheter med FoU-aktivitet i større grad har ansatt flere kompetente medarbeidere og investert i opplæring. Det er ikke spurt om fysiske ødeleggelser, driftsproblemer for kunder eller tap av arbeidstid.

Sammenlignet med tidligere undersøkelser er det i 2020 og 2022 høyere andel som svarer endring i policy og rutiner. Sammenlignet med forrige undersøkelse er det ingen signifikante forskjeller på dette spørsmålet.

*Figur 18. Som et resultat av hendelsen, ble noen av følgende endringer gjort i organisasjonen? Over tid. Total sample; base n = 1988; total n = 7101; 5113 missing*

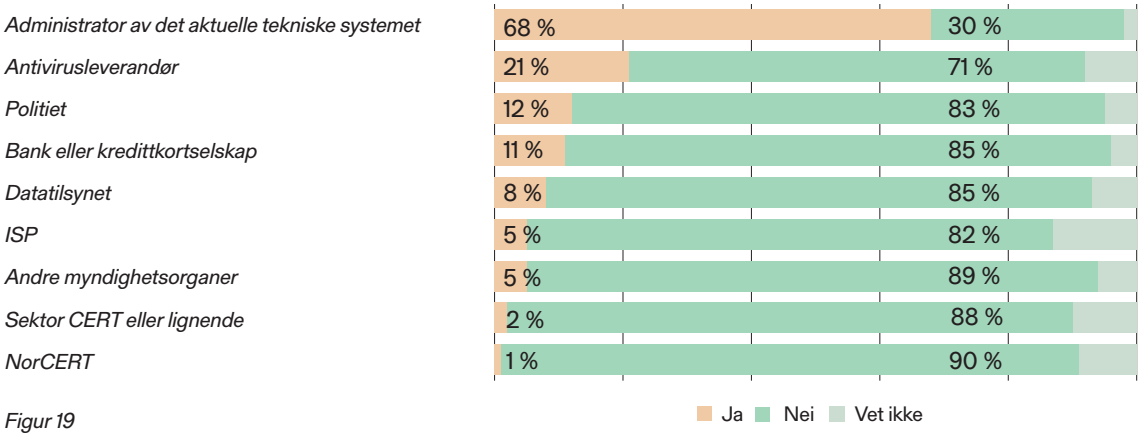



*Figur 18*

## 4.2 Rapportering

Sju av ti virksomheter som har opplevd sikkerhetshendelser har rapportert hendelsen til administrator av det aktuelle tekniske systemet, 21 prosent har rapportert til antivirusleverandør og 12 prosent har rapportert hendelsen til politiet. Rapportering til sektor CERT eller NorCERT er det kun 2 og 1 prosent som gjør.

*Figur 19. Ble hendelsen rapportert til noen av følgende?*
*Total sample; base n = 550; total n = 2500; 1950 missing*

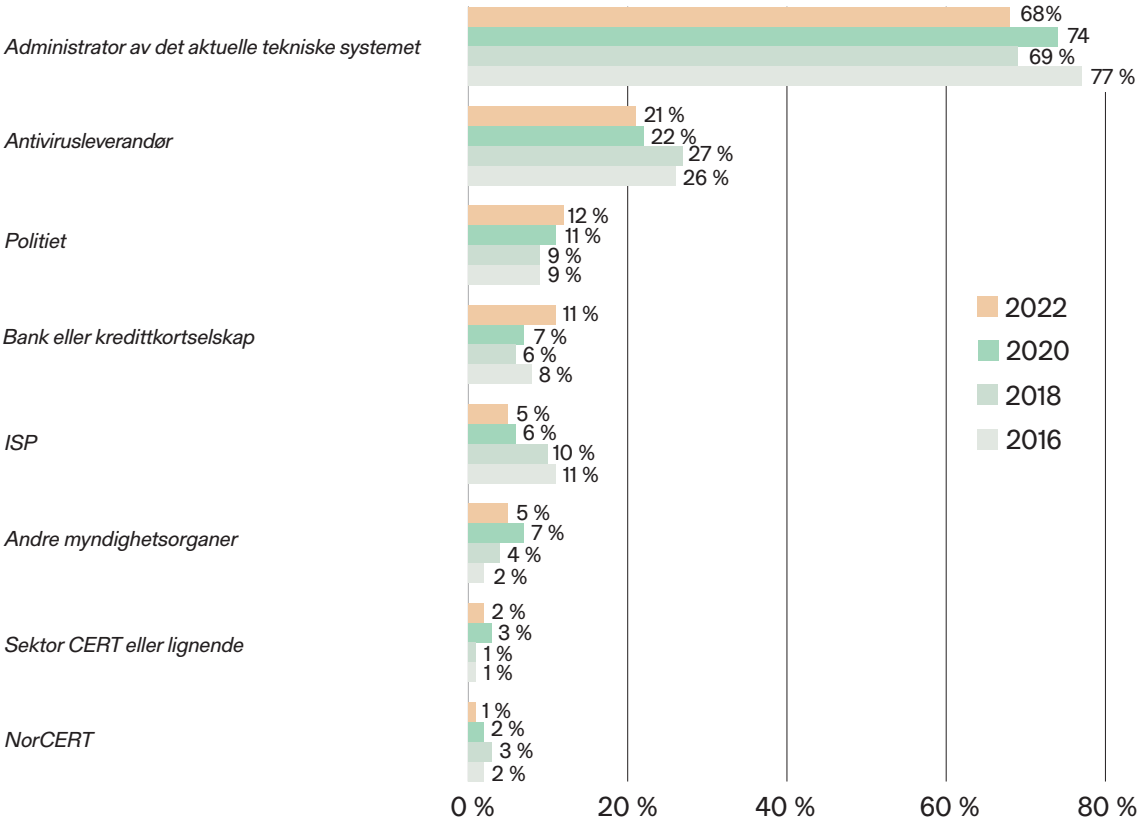



*Figur 19*

Store virksomheter skiller seg fra de små når det gjelder rapportering til NorCERT og sektor CERT. Mens det er kun 1 prosent av virksomheter med under 100 ansatte som rapporterer til NorCERT, er det 10 prosent av virksomhetene med 100 ansatte eller flere som rapporterer. For sektorCERT er tallene 1 prosent (5 til 19 ansatte), 3 prosent (20 til 99 ansatte) og 14 prosent (100 ansatte eller flere). Offentlige virksomheter rapporterer også i større grad til NorCERT og sektor CERT enn private (4 mot 1 prosent og 9 mot 1 prosent). Store virksomheter og offentlige virksomheter rapporterer i større grad til Datatilsynet. Samtidig ser vi at virksomheter med rammeverk for informasjonssikkerhet skiller seg fra andre på flere av forholdene og i større grad rapporterer til antivirusleverandør, administrator for det aktuelle systemet, ISP, sektor CERT og Datatilsynet.

Sammenlignet med 2020 er det et stabilt bilde når det gjelder hvem hendelsen rapporteres til.

*Figur 20. Ble hendelsen rapportert til noen av følgende?*
*Total sample; base n = 1988; total n = 7101; 5113 missing*




*Figur 20*

På spørsmål om hvem som sto bak hendelsen, er det ansatt og ukjent som er de ordene som går igjen i størst grad.

*Figur 21. Hvem sto bak hendelsen? Total sample; base n = 550; total n = 2500; 1950 missing*


*Figur 21*

## 4.3 Hendelsens kostnad

De som har vært utsatt for uønskede hendelser er spurt om hvilken kostnad dette medførte. I denne gruppen (som har opplevd uønskede hendelser) er det 74 prosent som klarer å tallfeste kostnaden, 25 prosent vet ikke hva kostnaden er og 1 prosent ønsker ikke å opplyse om det.

Blant virksomheter som har opplevd uønskede hendelser, har det i gjennomsnitt medført en kostnad på 43 159,- kroner. Det er verdt å merke seg at median og typetall er 0, så den typiske virksomhet som utsettes for hendelser har ingen (kjente) kostnader. Det er ikke signifikant forskjell på virksomheter i ulike størrelsesgrupper eller i offentlig og privat sektor, men de som har et rammeverk for informasjonssikkerhet oppgir en større kostnad enn andre (53 570,- mot 29 721,-).

5.

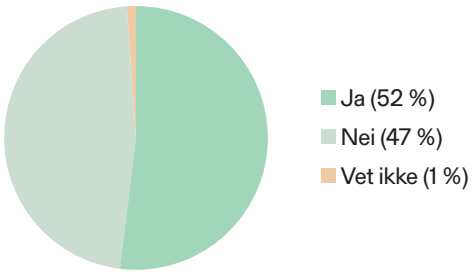
# Tiltak for økt sikkerhet

Dette tema handler om aktiviteter virksomhetene har gjennomført siste året for å øke sikkerhetsbevissthet blant ansatte.

## 5.1 Økt sikkerhetsbevissthet blant ansatte

Drøyt halvparten av virksomheter med 5 ansatte eller flere har i løpet av det siste året gjennomført tiltak for å øke de ansattes bevissthet rundt sikkerhet.

*Figur 22. Har virksomheten gjennomført aktiviteter som øker ansattes bevissthet rundt sikkerhet i løpet av det siste året? Total sample; base n = 2500*

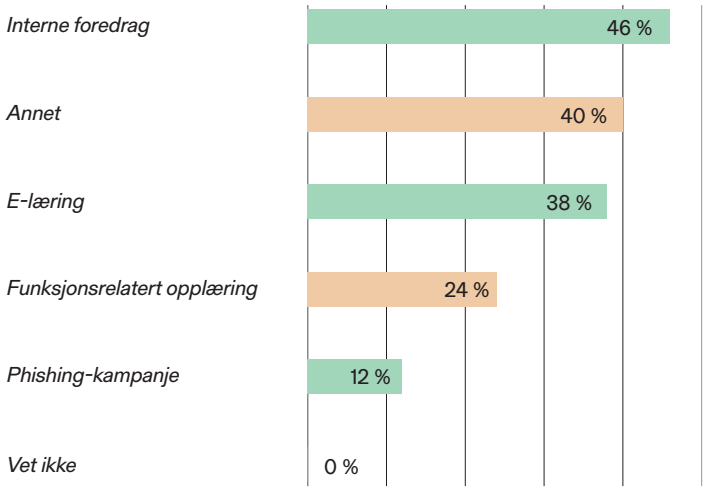



*Figur 22*

Det er stor forskjell på store og små virksomheter. Mens 47 prosent av de minste virksomhetene (5 til 19 ansatte) har gjort det, er det 84 prosent av de største som svarer det samme. Samtidig er dette mer vanlig i offentlige enn i private virksomheter (76 mot 49 prosent) og i virksomheter med rammeverk for informasjonssikkerhet (69 mot 33 prosent).

Blant de som har gjennomført aktiviteter er det interne foredrag som er det mest benyttede.

*Figur 23. Hvilken type aktiviteter som øker ansattes bevissthet rundt sikkerhet er gjennomført i løpet av det siste året? Total sample; base n = 1371; total n = 2500; 1129 missing*




*Figur 23*

Det er små forskjeller mellom ulike typer virksomheter. De største og offentlige benytter e-læring i noe større grad enn andre, men hovedbildet er at dette fordeler seg jevnt blant alle typer virksomheter.

# 6.

# Analyse

# 6.1 NTNU

Av Sokratis Katsikas, direktør SFI NORCICS, NTNU og Nils Kalstad, instituttleder IIK og direktør NTNU CCIS, NTNU

Hovedformålet med Mørketallsundersøkelsen går ut over det å gi en kvantitativ vurdering av omfanget av datakriminalitet som ikke anmeldes til Politiet i Norge. Målsetningen er å beskrive den digitale sikkerhetstilstanden i Norsk næringsliv og noen offentlige virksomheter. Populasjonen for undersøkelsen er norske virksomheter i privat og offentlig sektor med mer enn fem ansatte. Dette er et mangfoldig utvalg med stor variasjon i forutsetningene for å drive digitalt sikkerhetsarbeid.

Det finnes mange rammeverk og anbefalinger for å organisere og gjennomføre arbeidet med digital sikkerhet. Grunnprinsipper for IKT-sikkerhet fra Nasjonal sikkerhetsmyndighet er ett slik rammeverk som har blitt tilpasset norsk kontekst. Vi vil i det følgende vurdere den digitale sikkerhetstilstanden i Norsk næringsliv og offentlige virksomheter opp mot hovedkategoriene i dette rammeverket.

## Identifisere og kartlegge

Eksistens av et rammeverk eller et styringssystem for informasjonssikkerhet er en indikasjon på om en virksomhet har et bevisst forhold til sine digitale verdier, relevante trusler mot verdiene og arbeidet med å beskytte disse. I årets undersøkelse svarer bare 51% av respondentene at de har et slik rammeverk og/eller system. Nedgangen er på hele 12% fra 2020. Den negative utviklingen kommer hovedsakelig fra virksomheter med mindre enn 100 ansatte. Hos virksomheter med mer enn hundre ansatte er tallet (81%) på nivå med 2020 tallet.

Innføringen av personvernforordningen i 2018 bragte med seg et løft i antallet virksomheter som etablerte styringssystem for informasjonssikkerhet, da dette var et krav i forordningen. Det kan virke som om denne effekten nå har avtatt. Årets undersøkelse har tatt et bevisst valg om ikke å undersøke aspekter knyttet til personvernforordningen. Vi må finne nye drivere for virksomhetenes systematiske arbeid med identifikasjon og kartlegging av digitale verdier og trusler.

## Beskytte og opprettholde

Det finnes tre hovedkategorier tiltak for å ivareta forsvarlig sikring av digitale systemer over tid: teknologiske-, menneskelige- og organisatoriske tiltak. Som i 2020 er det også i år en urovekkende stor andel (61%) av respondentene som svarer at sikkerhetsbruddene oppsto som en følge av tilfeldigheter eller uflaks. Dette kan til en viss grad henge sammen med manglende prioritering av arbeidet med å identifisere og kartlegge verdier og trusler. Det er grunn for å frykte at det i tillegg er en indikasjon på manglende evne eller mulighet til å vurdere årsaken til hendelser.

Menneskelige feil og mangel på sikkerhetsbevissthet hos de ansatte oppgis som årsaken til henholdsvis 37% og 28% av hendelsene. Selv om vi ser en nedgang i uflaks og menneskelige feil fra 2020 til 2022 er det grunn til å være bekymret over disse svarene. Tilsvarende svar i eksempelvis forbindelse med HMS arbeid hadde utløst stor usikkerhet og iverksettelse av omfattende organisatoriske og teknologiske tiltak for å avlaste mennesket og tilfeldighetene som feilkilde. Det kan hende at de relativt moderate

rapporterte økonomiske konsekvensene av hendelsene (43.159 kr i snitt) er noe av årsaken til at det ikke oppstår tilsvarende reaksjoner innen digital sikkerhet.

Mørketallsundersøkelsen 2022 er gjennomført i kjølvannet av Russlands invasjon av Ukraina. Vi finner få indikasjoner i svarene som tilsier at norske virksomheter nå føler seg mer utsatt for målrettede eller politisk motiverte angrep enn tidligere. Halvparten av respondentene sier de har gjennomført tiltak for å øke ansattes bevissthet rundt digital sikkerhet. Dette kan gjøre Norge som nasjon mer motstandsdyktig mot sammensatte trusler. Videre ser vi at 52% velger å gjøre endringer i policy eller rutiner etter en hendelse.

## Oppdage

Evnen til å oppdage og fjerne kjente sårbarheter og trusler er en viktig del av sikkerhetsarbeidet. Tidlig deteksjon av en hendelse eller en hendelse som er under oppbygning kan redusere, og i beste fall fjerne, konsekvensene. Som i 2020 er det i år omtrent like mange respondenter som sier at hendelsene ble oppdaget ved rutinemessig intern sikkerhetsmonitorering som ved en tilfeldighet. Tallene er henholdsvis 41% og 40%. Den høye andelen av hendelser som oppdages ved en tilfeldighet er urovekkende høyt.

Det er også interessant at 85% av respondentene oppgir at en hendelse oppdages innen en dag etter at den oppsto. Svarene i 2020 var tilsvarende. Rapporter fra faktiske hendelser nasjonalt og internasjonalt dokumenterer svært lange tidslinjer fra systemet for første gang er kompromittert til at hendelsen oppdages, ofte mer enn hundre dager. Bare 1% av respondentene har benyttet seg av den kategorien i årets undersøkelse.

## Håndtere og gjenopprette

Når en hendelse oppdages er det viktig å ta tak i denne og gjenopprette normal systemtilstand eller drift så raskt som mulig. Mørketallsundersøkelsen kartlegger ikke direkte hvilke planer og prosesser som er benyttet for å håndtere de ulike hendelsene, men vi finner noen indikasjoner ved å se på endringer som kommer som følge av hendelsen. De vanligste grepene som senere vil øke evnen til å håndtere og gjenopprette er sterkere kontroll av eksterne leverandører og konsulenter (27%), innleie av tjenesteleverandører for å håndtere sikkerhet (25%) og investering i utvikling av sikkerhetsprosesser og etablere et sikkerhetsmiljø (22%).

Involvering av selskapets ledelse og styre ved hendelser holder seg på et godt nivå (65%). Dette kan være et tegn på at virksomhetene tar hendelsene mer alvorlig enn de estimerte gjennomsnittlige kostnadene ved en hendelse skulle tilsi. Det er fortsatt en betydelig underrapportering til Politiet, Datatilsynet og andre myndighetsorganer. Rapporteringsgraden til Politiet har ligget stabilt rundt 10% over mange år. Politiet på sin side har over tid styrket kapasitet og kompetanse både lokalt og sentralt til å håndtere IKT-relatert kriminalitet. Som en oppfølger av de mange profilerte hendelsene sent i 2021 publiserte Næringslivets sikkerhetsråd sin Nødplakat for digitale angrep. Her oppfordres virksomhetene til å varsle Politiets næringslivskontakter og Politiets cybersikkerhetssenter (NC3) om en hendelse skulle inntreffe. Plakaten hadde kun vært offentlig i noen måneder før datainnsamlingen til Mørketallsundersøkelsen 2022 ble gjennomført, og det blir spennende å se om dette tiltaket vil ha en effekt til neste undersøkelse.

## Oppsummert

Mørketallsundersøkelsen 2022 viser at:

- Det systematiske arbeidet med digital sikkerhet (rammeverk og/eller styringssystem) har stagnert hos de store virksomhetene og gått noe tilbake i de mindre
- En stor andel hendelser oppdages ved en tilfeldighet uten at virksomhetene synes å ha en klar formening om når hendelsen inntraff eller den faktiske årsaken til hendelsen
- Av reaktive tiltak som fremheves av respondentene etter en hendelse ser vi en god balanse mellom teknologiske-, organisatoriske og menneskelige tiltak
- 2/3 av virksomhetene involverer ledelsen og styre når en hendelse inntreffer.

Hovedinntrykket er at arbeidet med digital sikkerhet fortsatt er hendelsesdrevet, men det siste punktet gir grunn til optimisme. Ledelsesforankring er en forutsetning, men ikke i seg selv tilstrekkelig, for systematisk proaktivt arbeid med digital sikkerhet i norske virksomheter.

# 6.2 Ledelsen utgjør det største innsideproblemet!

Av Inge Kampenes, spesialrådgiver i Advansia

Mørketallsundersøkelsen 2022 inneholder mange interessante funn. Undersøkelsen har blitt gjennomført siden 1997, men sist revidert i 2016, og det er dermed mulig å få et bilde på status og trender. Vi kan for eksempel se både at 51% av virksomhetene har et rammeverk eller styringssystem for informasjonssikkerhet, og at utviklingen på dette området er negativ. Jeg kommer tilbake til denne ubehagelige innsikten.

Undersøkelsen gjelder for kalenderåret 2021, et år preget av pandemi og økende global usikkerhet. Utstrakt bruk av hjemmekontor der virksomhetenes digitale verktøy ble spredd for alle vinder samtidig som kriminelle og statlige etterretningsaktører fikk flere angrepsflater og blod på tann, burde tilsi at antallet informasjonssikkerhetshendelser gikk opp. Det bekrefter også Nasjonal sikkerhetsmyndighet i sin siste årlige rapport Risiko 2022; i 2021 var det en kraftig økning i sikkerhetstruende hendelser. Da er det besynderlig at Mørketallsundersøkelsen viser en generell nedgang i antall opplevde hendelser. Det kan være flere grunner til dette. Kanskje Nasjonal sikkerhetsmyndighet har forbedret sin evne til å oppdage cyberangrep? Kanskje virksomhetene ikke oppdager at de er blitt hacket eller infiltrert? Kanskje er ansatte blitt generelt flinkere til å gjennomskue forsøk på manipulasjon? Kanskje angriperne har blitt dyktigere og i større grad går mot enklere og naive leverandører i stadig mer komplekse leveransekjeder? Eller kanskje virksomhetene ikke vil fortelle at de har blitt utsatt for angrep – altså at det er mørketall også i Mørketallsundersøkelsen? Jeg tror svaret er ja på alle disse spørsmålene.

Undersøkelsen avdekker at det er få virksomheter i Norge som rapporterte sikkerhetshendelser til myndighetene. Det gjelder både til Politiet, til Datatilsynet og til sektor-CERT eller Nasjonalt cybersikkerhetssenter. Kun 1-2% rapporterte hendelser til de to sist nevnte, og små virksomheter i mindre grad enn store, og private i mindre grad enn offentlige. Dette kan tyde på at tilliten til disse sikkerhetsaktørene er svært lav, eller at virksomhetene i liten grad vet at de finnes. Begge forholdene bekreftes i en annen undersøkelse som nylig er utført av Nordstat på vegne av LO Stat og Utsyn – forum for utenriks og sikkerhet. Dette burde bekymre Nasjonal sikkerhetsmyndighet.

Det burde også bekymre myndighetene at kun 5% av virksomhetene rapporterte sikkerhetshendelsene til Datatilsynet. Dataangrep berører ofte personopplysninger, og da slår personopplysningsloven (GDPR) inn. Da plikter virksomhetene å melde fra til Datatilsynet innen 72 timer. Men det gjør altså de færreste - og det burde bekymre den enkelte av oss.

Den notorisk manglende rapporteringen, sammen med undersøkelsens funn om at kun 6% av sikkerhetshendelsene resulterte i en offentliggjøring, tyder på at virksomhetenes ledere i svært liten grad er opptatt av å bli sett i kortene eller i informasjonsdeling.

Tilbake til poenget innledningsvis om rammeverk eller styringssystem for informasjonssikkerhet. Det er for dårlig at halvparten av virksomhetene i Norge ikke har dette, og at det er stadig færre som velger å ha det. Undersøkelsen avdekker at de som har et rammeverk for informasjonssikkerhet opplever noe flere hendelser enn andre, og at de fleste oppdager sikkerhetsbrudd under sikkerhetsmonitorering eller interne kontroller. Det kan tyde på at mange av de som ikke har et rammeverk for informasjonssikkerhet faktisk ikke får med seg at de blir eller har blitt angrepet. Når det samtidig kommer frem at det er 10-14% sjanse for at angrepene på virksomhetene får negative konsekvenser, så burde dette motivere alle virksomhetsledere til å ta informasjons- og cybersikkerhet på et mye større alvor.

Hvis vi går hele fire år tilbake i tid, så hevdet Nasjonal sikkerhetsmyndighet i Risiko 2019 at for mange virksomheter ikke hadde oversikt over egne sårbarheter og hvilken risiko de er utsatt for. I årets nasjonale trusselvurdering hevdet Politiets sikkerhetstjeneste at nye nettverksoperasjoner vil ramme norske mål i år. Virksomheter knyttet til forsvar, beredskap, politikkutforming eller teknologi hvor Norge er langt fremme, vil være særlig utsatt. Og de av oss ledere som har tiltro til våre hemmelige tjenester tar dette på alvor. Eller?

Det største innside-problemet i en organisasjon er en ledelse som ikke erkjenner cybertrusselen. Jeg venter i spenning på Mørketallsundersøkelsen i 2024.

# 7.

# Risikobildet/ trender

## 7.1 Nasjonal sikkerhetsmyndighet

Norge står overfor et komplekst digitalt risikobilde der statlige og kriminelle aktører forsøker å utnytte sårbarheter i funksjoner, virksomheter og systemer ved bruk av et bredt utvalg digitale virkemidler. Digitaliseringen medfører økt effektivisering og innovasjon, men samtidig introduseres nye sårbarheter, avhengigheter og konsentrasjonsrisikoer som kan utnyttes og derfor må håndteres.

Siden forrige Mørketallsundersøkelse har NSM pekt på at vi står overfor et taktskifte innenfor digital risiko i Norge. Nasjonalt Cybersikkerhetssenter (NCSC) i NSM har de siste to årene observert en betydelig økning i ondsinnet aktivitet mot norske virksomheter.

Bruken av løsepengevirus vedvarer i omfang inn i 2022, og NCSC blir stadig kontaktet av virksomheter i flere sektorer som har blitt utsatt for dette. Flere av de rammede forvalter viktige samfunnsverdier i Norge. NCSC vurderer at aktørene bak løsepengetrusselen blir stadig mer profesjonelle.

Siden krigen i Ukraina startet i februar 2022 har flere pro-russiske cyberaktører lovet støtte til Kreml eller truet med å gjennomføre cyberoperasjoner for å gjengjelde angrep mot Russland eller materiell-støtte til Ukraina. I slutten av juni ble flere norske virksomheter utsatt for tjenestenektangrep fra den pro-russiske hackergruppen Killnet, noe som førte til forstyrrelser og nedetid på en rekke norske nett-sider. Hendelsen fikk stor medieoppmerksomhet i Norge.

Samtidig er det fremdeles avanserte aktører som utfører komplekse spionasjeoperasjoner mot norske mål, inkludert der våre viktigste verdier forvaltes. Dette har konsekvenser for Norges stats- og sam-funnssikkerhet. NSM observerer fremdeles at virksomheter lengre nede i verdikjedene og utenfor sikkerhetsloven rammes av sikkerhetstruende virksomhet, enten som mål i seg selv eller som et ledd i å nå mål høyere opp i verdikjedene. Programvare- og leverandørkjedeangrep kan utføres for å få innpass hos et selskaps mange kunder, og NSM tror slike operasjoner vil ha konsekvenser for norske mål i tiden fremover. Cyberoperasjonene mot Stortinget i 2020 og 2021 viser alvorlighetsgraden i det nasjonale digitale risikobildet vi nå står overfor.

NCSC har de siste to årene observert store og komplekse operasjoner mot flere mål og på tvers av sek-torer, hvor aktøren benytter avanserte metoder og angrepsvektorer for å lykkes med sine operasjoner. Det er sannsynlig at enkelte avanserte aktører ønsker å oppnå et varig fotfeste i norske virksomheter med formål om å hente ut informasjon som vil være av etterretningsverdi på kort og lang sikt. Slike aktører er det siste året observert som aktive mot mål i blant annet forsknings- og utdanningssektoren, sentral-forvaltningen, innenfor høyteknologi og næring, og mot offentlige forvaltningsorganer.

Norske virksomheter står overfor et komplekst og stadig skiftende sårbarhetsbilde, og NCSC håndterer kritiske sårbarheter jevnlig. NCSC ser at kjente, tekniske programvaresårbarheter er den vanligste veien inn for få uautorisert tilgang til en virksomhets digitale systemer. NCSC ser stadig bred utnyttelse av sårbarheter i mye brukte tjenester, som for eksempel e-postløsningen Microsoft Exchange. Dette har vært gjort av både avanserte og ikke-avanserte trusselaktører. Også nulldagssårbarheter har preget det internasjonale bildet de siste årene.

Uoversiktlige verdikjeder og avhengigheter på tvers av samfunnsfunksjoner gjør at hendelser kan inn-virke både på samfunnssikkerheten og statssikkerheten etter hvert som skillet blir mindre tydelig.

Økt digitalisering og tjenesteutsetting av samfunnsfunksjoner medfører lengre verdi- og leverandørkjeder, og det blir vanskeligere å ha oversikt over sårbarheter som kan utnyttes av trusselaktører. Uoversiktlige verdikjeder gjør det vanskeligere å beskytte viktige nasjonale verdier.

Stadig flere prioriterer det digitale sikkerhetsarbeidet. Ifølge NSM har for mange norske virksomheter likevel ikke et forsvarlig sikkerhetsnivå for å beskytte viktige verdier. Mange av de virksomheter som rammes av løsepengevirus har i liten grad vært tilstrekkelig forberedt. Økt bevissthet om digital risiko har ofte ikke blitt omsatt i handling. Dette bør være et tema i alle styrerom og ledergrupper.

Tekniske sikkerhetstiltak alene vil ikke stoppe trusselaktører. Det er nødvendig med gode prosesser i virksomheten og god sikkerhetskultur hos brukere av systemer og hos virksomhetens ansatte. Dette øker robusthet, men også bevissthet og forståelse for sikkerhet hos den enkelte.

Utfordringene skissert over har direkte knytning til menneskelige, organisatoriske og teknologiske sårbarheter i samfunnet. Sårbarheter i komplekse verdikjeder generelt, og for skytjenester spesielt, er utbredt og ikke tilstrekkelig adressert eller kompensert. Utfordringer knyttet til leverandørkjederisiko har blitt oversett, og økt tjenesteutsetting krever bedre oppfølging av leverandørrisiko.

For alle norske virksomheter er det forebyggende sikkerhetsarbeidet med på å redusere digital risiko. Med det utfordrende risikobildet, hvor konsekvensene av cyberoperasjoner blir mer alvorlige, haster det mer enn tidligere å implementere risikoreduserende tiltak.

NCSC erfarer fortsatt at alle digitale hendelser kunne vært unngått eller skaden begrenset dersom virksomheter i større grad hadde implementert «NSM Grunnprinsipper for IKT-sikkerhet».

NSM publiserer i løpet av et år råd, tiltak, veiledere og varsler på sine nettsider. NSM oppfordrer alle virksomheter til å varsle relevante myndigheter om sikkerhetsbrudd eller sikkerhetstruende hendelser.

## 7.2 Kripos

IKT-kriminalitet tar stadig større plass i det totale kriminalitetsbildet, og politiets kjennskap til antall rammede bedrifter øker i takt med dette. Det er et komplekst kriminalitetsbilde med flere kriminelle aktører hvor modusene stort sett er kjente, men utvikler seg noe over tid. Således skiller datakriminalitet seg ikke fra annen kriminalitet.

Datakriminaliteten som rammer Norge, er i stor grad grenseoverskridende kriminalitet som begås av organiserte kriminelle som opererer fra land med manglende rettslig samarbeid. Kriminaliteten i Norge har likheter med vestlige land i Europa. Noen kriminelle opptrer i organisasjoner som fremstår som profesjonaliserte aktører med tydelig organisering og arbeidsfordeling lik bedrifter. Det være seg operasjonssjefer, økonomisjefer og rekrutteringssjefer. Profesjonaliteten effektiviserer kriminaliteten.

Den største digitale kriminalitetstrusselen er løsepengevirus. Løsepengevirus er en type programvare som låser eller krypterer hele eller deler av innholdet på et datasystem eller en datamaskin. Angriperen krever en løsepengesum for å låse opp innholdet. Infeksjon av løsepengevirus, eller ransomware, kan skje på ulike måter. Ett eksempel er at angriperen først skaffer seg tilgang til offerets system for deretter å installere løsepengevirus i offerets nettverk. I flere saker har det blitt observert at angriper har hatt

tilgang til nettverket i lang tid før løsepengeviruset starter å kryptere systemet. I nyere tid har det blitt vanlig med en påfølgende utpressing i saker hvor offeret er rammet av løsepengevirus. Angriperen truer ikke kun med å miste tilgang til kryptert data, men også med publisering eller salg av data hentet ut fra nettverket.

Størrelsen på noen løsepengegrav tilpasses etter bedriftenes betalingsevne. En sentral drivkraft for den kriminelle aktiviteten er bedriftenes betalingsvillighet samt muligheten for anonymitet gjennom kryptovaluta og VPN. Videre motiveres de kriminelle aktørene av manglende mulighet for straffeforfølgelse i enkelte land. Løsepengevirus får store økonomiske konsekvenser for fornærmede bedrift. Det knytter seg særlig til tapt produksjonstid og gjenopprettelse av produksjon. Løsepengevirus rammer små, mellomstore og store bedrifter.

IKT-relaterte bedragerier rettes mot offentlig så vel som privat sektor. Bedrifter blir i økende grad rammet av bedragerier der ansatte blir forledet til å overføre penger (direktørbedrageri) eller til å endre på fakturautbetalinger (fakturabedrageri).

Bedrageriene varierer i kompleksitet fra oppringninger/e-poster fra kriminelle med lite forkunnskaper til profesjonaliserte aktører som har gjennomført datainnbrudd i forkant. I sistnevnte eksempel kan den kriminelle aktøren ha skaffet seg tilgang til e-poster som gjenbrukes for at e-posten skal fremstå troverdig.

Krigen i Ukraina har endret normalbildet i det digitale rom. Før krigen ble det observert profittmotiverte tjenestenektangrep mot norske nettsider med trusler om påfølgende angrep, dersom penger ikke ble utbetalt. Tjenestenektangrep (DoS) er et angrep på internett som innebærer at informasjon, ressurser eller tjenester blir helt eller delvis utilgjengelige. Under krigen har prorussiske grupper gjennomført tjenestenektangrep mot norske nettsider. Den mest fremtredende grupperingen er Killnet som rammet Norge i slutten av juni. Målene ble publisert på forhånd gjennom åpne kontoer i sosiale medier. Det fremstår som at aktiviteten har et politisk motiv. Konsekvensene av angrepene i Norge var nedetid av bedrifters nettsider av kortere varighet. Gode beskyttelsestiltak mot tjenestenektangrep er effektiv mot slike angrep.

Det eksisterer databaser på nett som inneholder brukernavn og passord som er stjålet i forbindelse med datainnbrudd og lekkasjer. Dette utgjør en sårbarhet da mange gjenbruker påloggingsdetaljer på tvers av ulike tjenester på nett. Kriminelles tilgang til slik informasjon kan gi uautorisert tilgang til bedrifters datasystem.

Verktøy, tilganger og tjenester for å gjennomføre datakriminalitet kan kjøpes. Dette skaper et økosystem der profitten fra løsepengeutbetalinger investeres i ny kriminalitet, som igjen øker omfanget av datakriminaliteten.

En kjent metode for å skaffe seg tilgang til datasystemer er gjennom e-post Phishing. E-posten kan inneholde en skadevare som kriminelle bruker for å innhente påloggingsdetaljer. En annen metode som benyttes er utnyttelse av kritiske sårbarheter. På slutten av 2021 var det en sårbarhet i det java-baserte loggverktøyet Log4j fra Apache.

Samarbeid med vestlige politimyndigheter har ført til resultater i pågående straffesaker. Organiserte kriminelle er pågrepet, utbytte er beslaglagt og kriminelle nettjenester er blitt stengt ned. Dette viser viktigheten av å varsle politiet når man utsettes for datakriminalitet.

# 7.3 Datatilsynet

## Brudd på personopplysningssikkerheten

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket i Norge, i tillegg veileder vi om hvordan regelverket skal forstås. Én av oppgavene våre er å motta meldinger om brudd på personopplysningssikkerheten fra virksomheter (se personvernforordningen artikkel 4 nr. 12). Kort skissert er dette sikkerhetsbrudd som omfatter personopplysninger. Virksomheter må rapportere sikkerhetsbrudd til oss «med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter» (se personvernforordningen artikkel 33). I praksis vil mange sikkerhetsbrudd omfatte personopplysninger, som igjen kan medføre risiko for de opplysningene gjelder. For eksempel risiko for å bli utsatt for svindel, for å miste tilgang til en tjeneste de trenger, for kompromittering av opplysninger mm. Derfor er også svært mange sikkerhetsbrudd meldepliktige til oss.

Kravet i personvernforordningen er at vi skal motta melding fra virksomheten innen 72 timer etter at de oppdaget bruddet, og bruddet kan meldes trinnvis. Basert på meldingene som vi får inn, kan vi si noe om trender i risikobildet i samfunnet vårt.

## Statistikk

I statistikken vår definerer vi hacking, phishing og skadevare i ulike kategorier. I praksis har disse kategoriene mye overlapp. Angripere bruker ofte phishing som inngangsdør til systemer i en virksomhet. På den måten kan de legge igjen programvare som gjør at de for eksempel kan gjennomføre større operasjoner senere, eller kryptere systemene deres for å fremme løsepengekrav. Noen ganger kan imidlertid ikke virksomhetene bekrefte at de har vært rammet av phishing, og da sorterer vi meldingen i én av de andre kategoriene. Vi omtaler de tre kategoriene samlet i teksten nedenfor, som «eksterne angrep».

I 2020 mottok vi 2009 meldinger om brudd på personopplysningssikkerheten, hvorav 9 % utgjorde eksterne angrep. I 2021 økte mengden meldinger til 2255, og andelen eksterne angrep økte til 13 %. Til og med juli 2022 har vi mottatt 1214 meldinger, og den foreløpige andelen eksterne angrep er på 6 %. Vår statistikk synes dermed å samsvare med funnene i mørketallsundersøkelsene for henholdsvis 2020 og 2022.

Når det gjelder rapportering av brudd til Datatilsynet antar vi at det finnes betydelige mørketall, hvilket også samsvarer med mørketallsundersøkelsen for 2022. Vi tror det er langt flere som opplever meldepliktige brudd på personopplysningssikkerheten enn de som melder fra til oss. Én grunn til at virksomheter ikke melder fra kan være uvitenhet om regelverket. En annen grunn kan være manglende internkontroll/styringssystemer, som mørketallsundersøkelsen har avdekket at gjelder mange virksomheter. Offentlige virksomheter står for over halvparten av meldingene vi mottar, og finanssektoren for omtrent en femtedel. Vi får også færre meldinger fra små virksomheter enn store.

## Trenden og hendelsene

I perioden mellom forrige mørketallsundersøkelse og årets undersøkelse har Datatilsynet sett en økning i antall sikkerhetsbrudd som var forårsaket av eksterne aktører med onde hensikter. Flesteparten av angrepene har begynt med et vellykket phishing-forsøk, med påfølgende kryptering av systemene til virksomheten og fremstilling av løsepengekrav fra angriperen. I tillegg har angriperne ofte hentet data ut av systemene, for å presse virksomheten til å betale løsepengene. Det er verdt å merke seg at

Et bredt spekter av virksomheter har rapportert lignende sikkerhetsbrudd til oss. Aktuelle eksempler fra offentlig sektor er Stortinget og Østre Toten kommune. Fra privat sektor kan vi nevne angrepene på Nordic Choice og Nortura.

I forkant av angrepet på Stortingets e-postsystem hadde de selv identifisert at manglende tofaktor-autentisering og sikkerhetskultur utgjorde høye risikoer. De hadde imidlertid ikke implementert tiltak for å redusere sårbarhetene da angripere brøt seg inn. I tillegg til personvernrisikoene kunne angrepet hatt langt mer alvorlige konsekvenser. En mer sofistikert aktør kunne forblitt uoppdaget og tilegnet seg vedvarende innsyn i stortingsrepresentantenes kommunikasjon. I verste fall kunne aktøren forsøkt å påvirke politikken de folkevalgte fører, for eksempel ved å drive utpressing med utgangspunkt i representantenes private e-postkorrespondanse.

Angrepene på Østre Toten kommune, Nordic Choice og Nortura fikk store umiddelbare konsekvenser. Kryptering førte til at de alle delvis ble utestengt av sine egne systemer, og at tjenestene deres brøt sammen. Østre Toten kommune måtte ty til penn og papir i saksbehandlingen, og det samme måtte de som hadde rett på tjenester fra kommunen. Desto verre var det at sikkerhetskopiene til kommunen ble slettet. Nordic Choice måtte håndtere inn- og utsjekking av hotellene sine manuelt. Fordi nøkkelsystemet deres ble rammet kunne de heller ikke gi besøkende nøkler til rommene sine. Hos Nortura fikk angrepet innvirkning på kjøttproduksjonen, og de hadde store utfordringer med å ekspedere varer i en begrenset periode.

En fellesnevner for slike meldinger om sikkerhetsbrudd, er at de har forårsaket skade for både virksomhetene og enkeltpersoner. Kostnadene har gjort innhugg i virksomhetenes økonomi. Renommèet har blitt påvirket. Privatpersoner har mistet kontroll over personopplysningene sine. Flere av bruddene er også i en slik skala at de kunne ha medført en risiko for samfunnssikkerheten for øvrig.

Vi ser at de virksomheter som har et etablert, operativt styringssystem for personvern og informasjonssikkerhet, inkludert definerte roller og ansvar, beredskapsplanlegging og hendelseshåndtering, er mer robuste overfor sikkerhetshendelser.

## Kjente sårbarheter

Selv om antall eksterne angrep har økt og årsaken har vært publisert offentlig, har de fleste virksomheter som har meldt brudd til oss likevel blitt rammet gjennom velkjente sårbarheter:

- Mangelfulle styringssystemer
- Utilstrekkelige risikovurderinger
- Manglende flerfaktorautentisering
- Utilstrekkelig tilgangsstyring
- Manglende nettverkssegmentering
- Utilstrekkelige rutiner for sikkerhetskopiering og gjenoppretting
- Utilstrekkelig testing av applikasjoner og oppdateringer
- Manglende frakobling av gamle og utdaterte systemer
- Mangel på beredskapsplan og øvelser
- Mangel på hendelseshåndtering
- Mangel på ledelsesforankring og – forståelse
- Mangel på definerte roller og ansvar

Vi har også mottatt meldinger fra virksomheter hvor angripere har kommet seg forbi flerfaktorautentiseringen deres. Rett implementasjon og testing er altså kritisk. Sårbarheter i løsninger for flerfaktorautentisering kommer høyst sannsynlig til å være et økende problem fremover.

# 8.

# Erfaringer

# 8.1 mnemonic

Erfaringer beskrevet her er basert på våre tjenesteleveranser til kunder i perioden 2021 og første halvår av 2022 – omtalt som rapporteringsperioden. Leveransene har omfattet granskning og håndtering av 23 omfattende datainnbrudd, innsamling og analyse av trusseletterretning og døgnkontinuerlig monitorering fra vårt operasjonssenter. Erfaringene er strukturert under to hovedtema: Overordnede utviklingstrekk innen cyberkriminalitet, og detaljer om metoder brukt av gjerningspersonene bak de sikkerhetshendelsene vi har gransket.

## Profesjonalisering av cyberkriminalitet

Det virker å være tilnærmet allmenn konsensus om at dataangrep har hatt sterk fremvekst de seneste år – både i omfang og alvorlighet. Flere estimater anslår at økonomisk motiverte organiserte kriminelle står bak det store flertall (opp mot 75-80%[1]) av registrerte dataangrep forrige år. Det er med andre ord profittmotiverte kriminelle som utgjør den mest sannsynlige cybertrusselen mot alle typer organisasjoner og virksomheter.

mnemonic ser denne utviklingen i sammenheng med en generell profesjonalisering av cyberkriminaliteten. Vi observerer en kommodifisering av ferdigheter, programvare og tekniske løsninger som brukes i utførelsen av mer sofistikerte profittmotiverte dataangrep – kanskje oftest eksemplifisert ved utbredelsen av ransomware[2]. Det er nå etablert flere undergrunnsmarkeder – og en forståelse om at kriminalitet kan anskaffes som et produkt eller en tjeneste. Bakdører eller påloggingsinfo til offernettverk, avansert skadevare, hvitvasking av løsepenger, og en rekke andre kapabiliteter som tidligere tok tid og kunnskap å bygge opp selv, har nærmest blitt ferdigpakket hyllevare.

Denne evolusjonen av det cyberkriminelle økosystemet har pågått ihvertfall siden 2015-2016. Men det var kanskje først i 2021 ransomware tok steget opp til å bli den dominerende formen for profittmotiverte dataangrep. Parallelt med økt tilgjengelighet av kapabiliteter, har lønnsomheten på dataangrep, med ransomware i spissen, gått opp. Den amerikanske statskassen publiserer årlige analyser av kryptovaluta og andre transaksjoner, som i 2020 identifiserte rundt $416.000.000 i løsepengeutbetalinger, som antas doblet påfølgende år basert på over $600.000.000 dokumentert utbetalt i første halvår 2021[3]. Samlet sett antas økningen i tilgjengelighet av kapabiliteter og lønnsomhet å være viktige drivere for stadig mer sofistikerte angrep, og for rekrutteringen av stadig flere angripere.

## Observasjoner av trusselaktørers metodikk

Hendelseshåndteringen vår innebærer blant annet kriminaltekniske analyser av kundenes data for å avdekke digitale spor etterlatt av gjerningspersoner (også kalt trusselaktører). Basert på dette kan vi si en del om trusselaktørenes aktiviteter og metoder i forbindelse med dataangrep utført i rapporteringsperioden. Vi observerer over tid ofte de samme metodene benyttet i flere forskjellige angrep av antatt ulike trusselaktører. Gjenbruk og kopiering av metoder fremstår altså som utbredt, så kunnskap om metodene og hvordan de brukes av trusselaktører kan ha stor verdi for fremtidig forsvar av nettverk og ressurser.

1) https://go.crowdstrike.com/crowdstrike-global-threat-report-2021.html
2) https://www.mnemonic.io/resources/security-report/security-report-2020/
3) https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data

Vi har levert hendelseshåndtering til et meget variert utvalg av kunder i rapporteringsperioden. Private og offentlige virksomheter av ulik størrelse innen sektorene finans, industri, energi, transport, landbruk, forvaltning, luftfart, kommunikasjon, underholdning og handel. Hendelsenes alvorlighet har variert – fra å kreve enkeltkonsulenter innen kundens normale arbeidstid, til akutt utrykning av mnemonic Incident Response Team (mIRT) bestående av flere spesialister med innsats på kveld og helg.

## Første tilgang – initiell kompromittering

I tre tilfeller var første observerte aktivitet fra trusselaktør en pålogging med legitime bruker kredensialer som lyktes på første forsøk. Ut i fra øvrige omstendigheter, anslår vi det mest sannsynlig at disse var enten: (1) tidligere kjøpte kredensialer, (ref. avsnitt over om cyberkriminalitet som en tjeneste), eller (2) et forsyningskjedeangrep, hvor trusselaktør kompromitterer ulike leverandører av produkter eller tjenester (ofte programmer levert som en tjeneste). Deretter utnytter trusselaktøren tillit til leverandøren for å omgå deres kunders forsvarsverk – for eksempel ved å misbruke leverandørens påloggingskredensialer til å logge på kundenes nettverk, eller å inkludere ondsinnet kode i ellers legitime programvare-oppdateringer.

Vi har ved flere anledninger konkludert med at manglende to-faktor autentisering til VPN-tjenester har muliggjort at trusselaktør har kunnet gjette riktig påloggingsinfo (gjennom variasjoner av såkalt brute forcing, password spraying, credential stuffing). Også miskonfigureringer av servere med liten eller ingen tilgangsstyring, som utilsiktet kan nåes direkte fra internett er observert som en inngangsvektor ved flere anledninger.

Til tross for at det er et populært tema innen IKT-sikkerhet, har mnemonic ikke dokumentert at phishing har vært initiell kompromitteringsvektor på noen sikkerhetshendelser vi har håndtert i rapporterings-perioden. Men det kan ikke utelukkes at phishing kan ha vært årsaken i tilfeller hvor det ikke har fantes nok data til å fastslå trusselaktørens første inngangsvektor. Tilsvarende har vi kun noen få dokumenterte tilfeller hvor eksternt utnyttbare sårbarheter har blitt benyttet som vektor for initiell tilgang.

## Etablere permanent tilgang

Første tilgang kan ofte være sårbare for oppdagelse eller sletting, typisk hvis den første kompromitterte enheten mister nettverkstilgang, eller slås av og på. For å befeste sin tilgang, ser vi ofte at trusselaktører anvender verktøy utviklet for å teste nettverkssikkerhet, oftest Cobalt Strike og Metasploit til å etablere mer robuste og skjulte bakdører inn i offerets nettverk etter første tilgang er oppnådd. Tidvis ser vi også at andre kommersielt tilgjengelige eller proprietære bakdører blir benyttet.

## Kartlegging og tilgangseskalering

Etter at pålitelig tilgang er etablert, har vi sett at trusselaktører virker å foretrekke å misbruke legitim programvare, fremfor noen spesialisert skadevare for kartlegge hvilke ressurser som kan nåes og øvrige tilkoblinger til den kompromitterte enheten. Dette reduserer sannsynligheten for å bli oppdaget, og applikasjoner som Teamviewer, PstPassword.exe, Passwordfox, Advanced IP Scanner har vi sett at kan gi trusselaktører alt de trenger for å skaffe høyere tilganger fra den første kompromitterte enheten. Vi har

også funnet tilfeller hvor trusselaktør har brukt mer spesialiserte og spissede verktøy skrevet for sikkerhetstesting, så som Mimikatz og Powershell Empire, selv om det kan påløpe økt risiko for oppdagelse.

I noen tilfeller er det observert kopiering og eksport fra offerets katalogtjeneste (eksempelvis Microsoft Active Directory) ved bruk av den ellers legitime applikasjonen DCSync. Slike eksporter kan omfatte blant annet brukernavn, tilganger og hash-verdier av passord. Slik kan trusselaktører med analyseverktøy som Bloodhound og Sharphound kartlegge offerets brukerkonti, nettverk, tilgangsregler og knekke passord i ro og mak på en identisk kopi, i stedet for å risikere deteksjon på et miljø som er i drift. Katalogtjenestedata kan også selges videre til andre trusselaktører eller meglere på undergrunns markeder for direkte profitt i seg selv.

## Lateral spredning og anti-forensics

Selv etter at de har oppnådd tilstrekkelige tilganger, vil trusselaktører rutinemessig ta grep for skjule sine spor og vanskeliggjøre en rekonstruksjon, selv etter formålet er oppnådd (også kjent som anti-forensics). Vanlige metoder inkluderer å spre prosesser og kjøring av applikasjoner og de tilhørende sporene de etterlater seg over flere maskiner, eksempelvis en RDP tilkobling fra maskin A til maskin B, deretter en SMB tilkobling fra maskin B til C, før det opprettes en reverse shell fra maskin C tilbake på maskin A for å kjøre en kommando. Dette er åpenbart mer tungvint for trusselaktør enn å kun kjøre kommandoen på maskin A – men slik må en gransker senere ha data fra flere enheter for å gjenskape et fullstendig bilde av hendelsen. Sletting av autentiserings- og hendelseslogger, manipulering av tidsstempler, deaktivering av anti-virus og andre kjørende sikkerhetsverktøy er også ofte sett.

## Datatyveri/eksfiltering

Det er vanskelig å stadfeste hvordan en trusselaktør har greid å få ut stjålne data av offerets nettverk (kjent som eksfilterting). Vi har imidlertid hypoteser som går på at trusselaktører ofte vil opprette anonymiserte konti til engangsbruk hos legitime leverandører av skylagringstjenester (gjerne samme leverandør som offeret selv benytter), og deretter initiere en synkroniseringsprosess fra en ressurs i offerets nettverk til trusselaktørens skylagringskonto. Hypotesen støttes av at vi i et mindre antall hendelser har kunnet observere denne type oppførsel. Trusselaktøren benyttet her det legitime verktøyet RCLONE til å synkronisere data fra delte filområder til en skylagringsløsning. Alternativt støtter tidligere nevnte rammeverk som Cobalt Strike også ulike former for dataeksfiltrering, da oftest kryptert og/eller maskert via protokoller og nettverksporter normalt ikke brukt til dataoverføring, sånn som DNS.

## Kryptering

I tilfeller hvor trusselaktøren har kryptert offerets data (oftest gjennom kjøring av en type løsepengevirus/ransomware, har vi sett to variasjoner: (1) Enten «nuke it all», full kryptering fra innsiden av operativsystemet på målmaskinen – kan være mer krevende i sanntid, og dermed gi offeret større mulighet til å avbryte prosessen. (2) Tilpasset kryptering som kun rammer spesifikke filtyper, som for eksempel SQL databaser og ESX lager.

### Utpressing

I tilfeller hvor det er et fullbyrdet angrep, ser vi oftest at løsepengeviruset automatisk genererer eller laster ned et forhåndsdefinert utpressingsbrev på offerets maskiner etter krypteringen, med ulike variabler som løsepengesummen, adressen til en kryptovaluta-lommebok som løsepengene skal overføres til, e-postadresser hvor offeret kan kontakte trusselaktøren med en kryptert fil som deretter kan returneres ukryptert for å sannsynliggjøre at krypteringen er reversibel. I noen tilfeller er alle de foregående variablene samlet på én enkelt nettside på det mørke nettet, hvor offeret kun får en lenke til siden i utpressingsbrevet. Dersom løsepengeviruset er levert som en tjeneste fra etablerte kriminelle grupper, vil disse ofte drifte offentlig tilgjengelige oversikter (kalt leak blogs/leak sites) på både det mørke nettet og det åpne nettet, hvor de annonserer vellykkede angrep og navn på ofre. Dersom løsepengekravet ikke innfris, trues det også med å lekke sensitive data her (også kjent som double extortion), og/eller å varsle offerets kunder og samarbeidspartnere om at de er kompromittert (triple extortion).

## 8.2 Telenor

### Mer målrettet svindel

Ettersom terrenget til de kriminelle aktørene har blitt mer utfordrende på grunn av skjerpet nettsikkerhet gjennom pandemien, har aktørene blitt presset til å lage mer troverdige kulisser for å lure til seg personopplysninger, kortinformasjon, penger, engangskoder og BankID. Det har også blitt vanlig å kombinere ulike digitale verktøy for å gjøre henvendelsen mer troverdig.

### Innsidetrussel - Slik forsøkte trusselaktører å rekruttere Telenor-ansatte

I løpet av 2021 mottok enkelte Telenor-ansatte kontaktforespørsler via LinkedIn. De som tok kontakt, hadde oppgitt at de hadde jobbet i en Telenorbutikken og at de ønsket å få utført SIM endringer.

Forespørselen kom fra en for dem ukjent person som tilsynelatende også jobbet i Telenor – en stor organisasjon med mange ansatte – og ble derfor godkjent uten videre ettertanke. Like etter kom SIM-forespørselen til de ansattes private e-postadresse, som bakmennene mest sannsynlig har hentet ut fra LinkedIn. Her er det altså blitt jobbet målrettet og spesifikt, med ett mål for øye: Å skaffe seg noen på innsiden, som kan gjøre en jobb for dem.

Telenor mistenker at avsender visste hva han var ute etter, og som gikk rett på Telenor-ansatte i forsøket på å nå dette målet. Telenor mistenker også at slike målrettede forsøk på rekruttering av innsidere skjer nok dessverre også i større omfang enn vi er klar over.

Når valget står mellom å bruke avanserte og ressurskrevende angrepsverktøy for å komme seg inn i en bedrifts stadig sikrere IT-systemer, eller å betale en ansatt noen tusenlapper for samme type tilganger eller informasjon, velger trusselaktørene gjerne minste motstands vei.

## Flubot – meget avansert Android malware

Flubot er et Android virus som spres via SMS og som er laget for å detektere og imitere bank- og crypto-valuta applikasjoner. Viruset skjuler seg i forskjellige apper (DHL, Voicemail osv) som lastes ned fra kompromitterte, legale nettsider.

I juni 2022 meldte Europol at de i samarbeid med en rekke lands politimyndigheter hadde lykkes å ta ned infrastrukturen til Flubot. Da hadde «viruset» herjet i Europa i over 1 år. Det var våren 2021 at vi så Flubot-viruset i Norge. Da hadde det allerede sirkulert i andre europeiske land i noen måneder.

Det krever en del godkjenninger og overstyring av sikkerhetsmekanismer av brukeren før viruset kan installeres. Blant annet må man gi tillatelse til nedlastning av ukjente apper, man må gi utvidede tillatelser til den aktuelle appen og man må godkjenne advarsler av typen «denne filtypen kan skade enheten din. Vil du allikevel installere?»

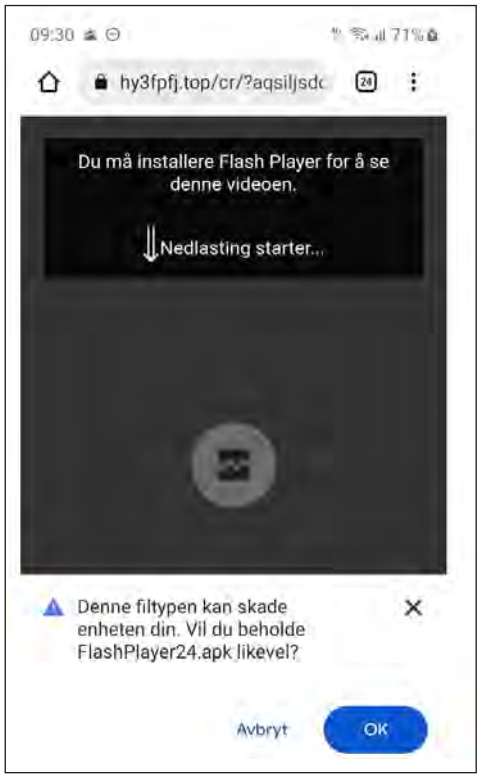
Når viruset dog først er installert, får den fullstendig kontroll over den infiserte terminalen ved blant annet å:

- Installere ny meldingsapp som overstyrer eksisterende. Dette medfører at innkommende SMS til en infisert terminal ikke vil kunne leses av brukeren, men vil kunne videresendes og leses av andre.
- Formere seg ved å sende spam SMS til kontakter som lastes ned fra Command&Control server.
- Sende offerets kontaktliste til C2 server
- Detektere bank- og kryptovaluta apper på den infiserte terminalen.
- Åpne falske "overlays" når offeret åpner bank/kryptoapper.
- Logge offerets kredittkortinformasjon og sender til C2 server
- Slå av Google Play Protect

I Norge hadde viruset stor spredning til mange terminaler, og Telenor måtte utvikle egne deteksjonsverktøy og blokkeringsmekanismer for å hindre spredning. Heldigvis er det ikke avdekket store svindelsaker som følge av spredningen. Men tatt i betraktning Flubot sin kapasitet kan skadene ha vært betydelige, særlig alvorlig vil spredning til ansatte i samfunnskritiskebedrifter og statlige intuisjoner. Flubot har/hadde et skadepotensiale langt utover økonomisk svindel.


09:52
74%
ammedicaltourism.com
DHL
Spor pakken din
Last ned App
1. Denne pakken er knyttet til telefonnummeret ditt og kan bare spores med appen vår.
2. Hvis det vises et vindu som forhindrer installasjonen, velger du "innstillinger" og aktiverer installasjonen av ukjente apper.
DHL15.apk. Åpne


11:59
100%
eis-innov.cf/w/?tjygcplc
telenor
Telenor: Du har ny telefonsvarer
Telefonnummeret ditt
930 89 134
Meldingslengde
2 minutter og 34 sekunder
Denne taleposten er i høykvalitetsformat og kan bare høres på med appen vår.
Last ned talepostappen
Hvis det vises et vindu som forhindrer installasjonen, velger du "innstillinger" og aktiver installasjonen av ukjente apper.


09:30
71%
hy3fpfj.top/cr/?aqsiljsdc
Du må installere Flash Player for å se denne videoen.
Nedlasting starter...
Denne filtypen kan skade enheten din. Vil du beholde FlashPlayer24.apk likevel?
Avbryt
OK


Your device is infected with the FluBot® malware
Android has detected that your device has been infected.
FluBot is an Android spyware that aims to steal financial login and password data from your device.
You must install an Android security update to remove FluBot.
Install security update
If a window appears preventing the installation, select "settings" and enable the installation of unknown apps.

## 8.3 Visma

I løpet av det siste året har Visma ikke sett store endringer i trusselbildet i cyberdomenet, men vi har lært mye av de pågående geopolitiske hendelsene og vår ekspansjon til nye markeder.

En viktig læringsarena for Visma er våre oppkjøp av selskaper som i stor grad gjøres utenfor Norge. Gjennom disse lærer vi mye om sikkerhetskultur og hvordan sikkerheten planlegges og eksekveres på tvers av landegrenser og markeder.

Når vi sammenstiller læringen herfra med læring fra våre sensornettverk samt etterretning og sikkerhet prosesser tegner det seg noen bilder som vi gjerne deler.

I cyberdomenet har vi i perioden sett "mer av det samme", så i praksis en økning i aktivitet fra trusselaktører på tvers av spekteret og noenlunde homogent fordelt i våre markeder.

Aktørene virker fortsatt til å være avhengig av "mindre teknisk avanserte" vektorer for å få initiell tilgang, og vi observerer en økning i Phishing og spesielt Infostealers (Mekanismer for å stjele cookies og lignende) og lignende metoder for å skaffe brukernavn, passord og informasjon som senere kan misbrukes.

I markedsplassene for salg av kontrabande (passord og lignende ) på "det mørke nettet" ser Visma at prisnivå og volum er nogenlunde konsistent med tidligere år.

Vi ser også en konsistent utvikling på svindelområdene, herunder CEO-fraud og variasjoner over samme tema (f.eks. aktører som prøver å lure kunder eller ansatte til å overføre penger eller gi fra seg data). Noen angrepsformer får innimellom ekstra oppmerksomhet som f.eks oppgangen i DDOS i en periode. Noen av disse ser ut til å være rene styrkedemonstrasjoner med nasjonalstatsmotivasjon, mens andre virker til å være forsøk fra vinningskriminelle.

Den siste observasjonen i svindeldomenet er at de vinningskriminelle blir mer profesjonelle og utvider porteføljen sin med relativt gode oversettelser mellom land. Dette er en utvikling som gir bekymringer i mindre land som Norge som trolig vil treffes hardere etter hvert som svindlere fra internasjonale organiserte kriminelle miljøer får bedre prosesser og metoder også her.

Når en aktør har fått initiell tilgang virker de fleste til å bruke sammenfallende metodikk for å unngå oppdagelse og øke tilgang. De fleste virker til å bruke metoder som CobaltStrike, BruteRatel og lignende rammeverk i en eller annen form. Noen aktører er svært profesjonelle og har egne konfigurasjoner som er laget for operasjonene, mens andre bruker "default settings" og virker ikke til å helt ha innsett potensialet i de verktøy de besitter.

Forsvar i dybden og i flere dimensjoner virker fortsatt til å være det som gir effekt også mot den typen angripere som vi ser for tiden. Videre ser vi at "bottom up" tekniske forsvarsmekanismer fundert i prinsipper som "tech excellence og agilitet" virker til å gi større effekt enn klassiske "top down" mekanismer (som Governance, ISMS-er osv).

Enkle virkemidler som å stenge ned unødvendige tjenester, etablere gode EDR mekanismer samt mekanismer for å disseminere IOC-er og annen nyttig informasjon for forsvarere har også vist seg å være svært effektivt. Vinningskriminelle ser ut til å "gi opp" om de møter kompetent motstand og heller bevege seg mot andre mål.

De store geopolitiske hendelsene har farget mye av våre observasjoner og lærdom i perioden. Oppbyggingen til krig og den senere invasjonen av Ukraina lærte oss mye om hvilke indikatorer som det er viktig å legge merke til i forkant. Disse lærdommene kommer til anvendelse i andre potensielle geopolitiske hendelser som følges nøye i tiden som kommer.

Vi lærer også mye ved å studere de anvendte taktiske stridsmidler i cyber fra alle parter, og vi observerer at disse er til forveksling lik de metoder som brukes av vinningskriminelle.

Vi erfarer også at attribusjon gjøres ekstra vanskelig da vinningskriminelle lærer svært fort av nasjonalstatens instrumenter, og vice versa.

Vi ser også at stridsmidler i cyberdomenet oppfører seg noenlunde disiplinert og får ikke stor smitteeffekt utenfor krigsteatrene. Den senere tiden har vi dog observert at enkelte cyberstridsmidler har blitt observert utenfor krigsteatrene med varierende grad av effekt i sine mål.

Informasjonsoperasjoner virker til å være en sentral del av verktøykassen til stridførende parter og observasjoner av deres metoder, adferd og budskap er sentrale elementer i vår læringsprosess.

Visma har også lært mye av å observere hvordan krigførende stater påføres forskjellige former for tap etter lekkasjer fra deres indre systemer. Vi har erfart at mengden av data som er lekket fra for eksempel russiske institusjoner og selskaper har vært langt større enn hva vi hadde forventet.

I kort så er Visma bekymret for utviklingen i cyberdomenet og oppfordrer både privat og offentlig sektor å investere i sikring av "det som er viktig for en" og bygge forsvar i dybden selv framfor å anta at "noen andre" vil sikre deg.

I valg mellom tech excellence og god "top down kontroll" så anbefaler VIsma å gå for Tech Excellence.

## 8.4 Sopra Steria

Erfaringene fra NCSC og Kripos samsvarer i stor grad med det Sopra Steria observerer mot våre kunder. Antall hendelser mot Sopra Steria og våre kunder har forholdt seg stabilt gjennom 2021 og 2022. Gjenåpningen i samfunnet og ansatte som vender tilbake på jobb har ikke påvirket disse tallene.

Det er fortsatt daglige phishingkampanjer som retter seg mot et stort antall brukerkontoer hvor det enten forsøkes å lure til seg brukernavn og passord eller e-postene forsøker å få mottakeren til å laste ned skadevare. Flere av disse kampanjene kan knyttes til såkalte «Initial Access Brokers» som skaffer seg fotfeste i virksomheters infrastruktur før de selger denne tilgangen til andre kriminelle som f.eks. ransomware-gjenger.

Sopra Steria opplever at enkelte av de større hendelsene kommer av mulighetsrom som oppstår som følge av sårbarhetsfunn som umiddelbart blir utnyttet av både statlige og ikke-statlige trusselaktører. Tiden fra en sårbarhet blir kjent til det finnes en «proof-of-concept» som blir tatt i bruk av trusselaktører blir stadig mindre. Denne kampen mot klokken setter høye krav til oss som sikkerhetsleverandør for å raskt fange opp nye sårbarheter, men også virksomheters behov for å redusere tiden det tar å gjennomføre sikkerhetsoppdateringer. Vi observerer færre sikkerhetshendelser hos virksomhetene med gode patcherutiner, oversikt over egen infrastruktur og gjennomførte herdingstiltak mot angrepsflater som internetteksponerte tjenester.

Sopra Steria har observert flere DDoS-angrep mot våre kunder siste året. DDoS-angrepene har vært delt mellom to motiver. Vi har hatt hendelser hvor motivet har vært økonomisk vinning, hvor virksomheter opplever DDoS-angrep etterfulgt av et utpressingsbrev med trusler om påfølgende angrep hvis det ikke utbetales bitcoin.

De andre angrepene har vært aktivisme fra antatt pro-russiske grupperinger som rammet bredt i Norge eller aktivisme mot enkeltsaker.

## 8.5 Coop

Som Norges nest største dagligvarekjede, og med 2 millioner medeiere, ser vi stadig forsøk på svindelkampanjer rettet mot våre kunder og medeiere gjennom ulike kanaler som via e-post og falske profiler i sosiale medier. I tillegg til vanlige svindelsaker, opplever vi derimot mer avanserte og komplekse saker enn tidligere. En vedvarende og økende trend er trusler mot våre ansatte. Gjennom BEC-svindel (Business E-mail Compromise) benytter kriminelle e-post til phishing-, direktør- og fakturasvindelforsøk. Disse angrepene blir stadig mer sofistikert og målrettet, og dermed også treffsikre.

Coop vurderer at dagens trusselbilde blir stadig mer forverret, hvor trusselaktører blir stadig mer avansert i sine metoder. Dette resulterer i at cyberangrep også kan bli vanskeligere å oppdage.

Vi anser at en av de største og vedvarende truslene i dag er løsepengevirus og verdikjedeangrep. De siste årene har flere virksomheter blitt rammet på verdensbasis. The European Union Agency for Cybersecurity (ENISA) forventer en firedobling av angrep mot digitale verdikjeder i 2022. SolarWinds og Kaseya-angrepet er eksempler på dette, hvor sistnevnte også rammet driften til Coop Sverige. Lengre og mer komplekse verdikjeder øker den totale sårbarhetsflaten, samt medfører avhengigheter og mangel på kontroll. Vi i Coop arbeider derfor kontinuerlig med å sikre og kontrollere leverandører og tredjeparter, og anbefaler alle virksomheter til det samme. Still sikkerhetskrav til leverandører i anskaffelsesprosessen, og sørg for å velge leverandører som har en tilfredsstillende grad av sikkerhetsmodenhet. Det er i tillegg viktig å sikre og kontrollere at leverandøren faktisk etterlever de avtalte kravene.

Den pågående krigen i Ukraina ser vi også at har påvirket cyberdomenet. Vi har sett eksempler på flere hendelser som følge av krigen, deriblant tjenestenektangrep som lammet flere norske nettsider i juli. Det stadig skiftende trusselbildet kan være utfordrende, som vi i Coop har et bevisst forhold til. Trusseletterretning kan gi verdifull informasjon fra ulike kilder, som kan brukes til å minimere og redusere sikkerhetsrisikoer. På denne måten kan virksomheter innhente informasjon, og bruke det til egen fordel. Trusler oppdages og håndteres, og tiltak implementeres fortløpende. Gjennom trusseletterretning har vi aktivt fulgt med i ulike kilder, og varslet virksomheter om trusler i forkant. Vi oppfordrer alle virksomheter til å arbeide proaktivt, og følge med på cyberdomenet.

Samarbeid og informasjonsdeling på tvers av bransjer og virksomheter er også en viktig forutsetning for å kunne imøtekomme et stadig forverret trusselbilde. Coop har et godt samarbeid med våre kontakter, deriblant Næringslivets Sikkerhetsråd, og anbefaler dette også for andre. Et tett samarbeid med myndigheter og næringsliv er uten tvil en viktig faktor for å vinne kampen mot cyberkriminalitet.


PANOMERA
PANOMERA
PANOMERA
PANOMERA
Dallmeier

# Vedlegg

*1. utgave. Oppdatert 14. januar 2022*

# NØDPLAKAT
## FOR DIGITALE ANGREP

## VARSLE

Varsle IKT driftsorganisasjon, og mobiliser beredskapsorganisasjon i egen virksomhet.

### 23 20 80 00

Varsle **politiets nasjonale cyberkrimsenter (NC3)** via den døgnåpne desken til Kripos. Dette varselet er ingen formell anmeldelse, men NC3 ønsker å få tidskritisk informasjon tidlig, uavhengig av om saken er anmeldt eller ikke.

### 23 31 07 50

Varsle **Nasjonalt cybersikkerhetssenter (NCSC).** Dette er NSMs nasjonale responsfunksjon for digitale angrep, og er en arena for nasjonalt og internasjonalt samarbeid ved håndtering av digitale hendelser og rådgiving. NCSC er døgnbemannet.

### 23 29 14 05

Vurder varsling av **Økokrim**. Enheten for finansiell etterretning kan i mange tilfeller bistå ved internasjonal stans av transaksjon relatert til hvitvasking og terrorfinansiering.

## HÅNDTERE

Be om akutt bistand fra leverandører som tilbyr tjenester for håndtering av dataangrep. Disse har døgnåpne alarmtelefoner. Se liste over leverandører som er godkjent av myndighetene til høyre. Innhent råd om umiddelbare tiltak, og iverksett dette.

Gi gjerne hendelseshåndteringsleverandøren fullmakt til å ha direkte kontakt med myndighetene (NC3/NCSC), og å dele relevante informasjon med disse fortløpende.

### 02800

Anmeld saken til lokalt politidistrikt. Henvis lokalt politi til eventuell forutgående kontakt med NC3/NCSC.

Politiet kan også tipses om forhold, dersom man ikke ønsker å anmelde. Les mer om anmeldelse og tips til politiet om datakriminalitet ved å scanne QR-koden, eller besøke https://www.politiet.no/rad/datakriminalitet-og-bedrageri

Politiets næringslivskontakter har ingen operativ funksjon ved hendelser, men kan bistå med råd og veiledning.

## GJENOPPRETTE

Iverksett beredskapsplaner for nøddrift. Etter et dataangrep kan det ta mange uker å gjenopprette normal drift, så det er viktig å iverksette alternative driftsmetoder tidlig.

### Godkjente leverandører:

Leverandørene under har døgnåpne alarmtelefoner for håndtering av dataangrep, og er godkjent av NSM i henhold til deres kvalitetskrav.

**Defendable**
91 80 80 30
post@defendable.no

**mnemonic**
23 20 47 41
23 20 28 25
mirt@mnemonic.no

**ATEA**
03060
irt@atea.no

**Netsecurity**
92 24 73 65
irt@netsecurity.no

**sopra steria**
24 14 04 56
no.irt@soprasteria.com

*Vi gjør oppmerksom på at flere andre aktører tilbyr tilsvarende tjenester, selv om de ikke er en del av den frivillige kvalitetsordningen til NSM.*

### Politiets næringslivskontakter:

| | | | |
|---|---|---|---|
| Økokrim: | Torstein Eidet | 916 75 964 | torstein.eidet@politiet.no |
| Kripos: | Vakant | | |
| Oslo PD: | Christina T. Rooth | 404 34 545 | christina.rooth@politiet.no |
| Agder PD: | Jan Kåre Eriksen | 959 46 313 | jk.eriksen@politiet.no |
| Sør Øst PD: | Vakant | | |
| Sør Vest PD: | Kyrre Lindanger | 916 71 726 | kyrre.lindanger@politiet.no |
| Vest PD: | Sonja Lund | 924 97 728 | Sonja.Lund@politiet.no |
| Trøndelag PD: | Terje Lunde | 481 61 969 | terje.lunde@politiet.no |
| Troms PD: | Merethe Samuelsen | 915 17 939 | merethe.samuelsen@politiet.no |
| Møre og Romsdal PD: | Kjell Arne Hestad | 926 06 045 | hestad@politiet.no |
| Nordland PD: | Håvard Fjærli | 918 83 382 | havard.fjarli@politiet.no |
| Øst PD: | Jan Kevin Brunvoll | 975 77 266 | jan.kevin.brunvoll@politiet.no |
| Innlandet PD: | Lene Espelund | 958 99 584 | Lene.Espelund@politiet.no |
| Finnmark PD: | Jan Arne Pettersen | 900 96 960 | jan.arne.pettersen@politiet.no |

**Næringslivets sikkerhetsråd**

Næringslivets Sikkerhetsråd er stiftet av Finans Norge, NHO, Virke, Spekter, Rederiforbundet og Den Norske Krigsforsikring for skib, og arbeider kontinuerlig med å kartlegge, forebygge og bekjempe tilsiktede sikkerhetstrusler mot norsk næringsliv. Se våre nettsider www.nsr-org.no for flere detaljer.

Plakaten er utarbeidet i samarbeid med:
POLITIET
NASJONAL SIKKERHETSMYNDIGHET

## 1. Identifisere og kartlegge

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer
- 1.2 Kartlegg enheter og programvare
- 1.3 Kartlegg brukere og behov for tilgang

## 2. Beskytte og opprettholde

- 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser
- 2.2 Etabler en sikker IKT-arkitektur
- 2.3 Ivareta en sikker konfigurasjon
- 2.4 Beskytt virksomhetens nettverk
- 2.5 Kontroller dataflyt
- 2.6 Ha kontroll på identiteter og tilganger
- 2.7 Beskytt data i ro og i transitt
- 2.8 Beskytt e-post og nettleser
- 2.9 Etabler evne til gjenoppretting av data
- 2.10 Integrer sikkerhet i prosess for endringshåndtering

## 3. Oppdage

- 3.1 Oppdag og fjern kjente sårbarheter og trusler
- 3.2 Etabler sikkerhetsovervåkning
- 3.3 Analyser data fra sikkerhetsovervåkning
- 3.4 Gjennomfør inntrengingstester

## 4. Håndtere og gjenopprette

- 4.1 Forbered virksomheten på håndtering av hendelser
- 4.2 Vurder og klassifiser hendelser
- 4.3 Kontroller og håndter hendelser
- 4.4 Evaluer og lær av hendelser

# FEILMARGINTABELL

**Tabellen under viser feilmarginer ved rent lotterisk utvalg. Prosentresultatet pluss/minus feilmarginen som er angitt for den aktuelle utvalgsstørrelse og prosentresultat, gir et 95 prosent konfidensintervall. Et konfidensintervall på 95 prosent betyr at vi med 95 prosent sannsynlighet kan si at resultatet for hele populasjonen ligger innenfor det aktuelle intervallet. Beregningene av feilmarginer forutsetter at det ikke forekommer systematiske skjevheter og feil i utvalget eller rene målefeil.**

| | Prosentpoeng | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 5,0 % | 10,0 % | 15,0 % | 20,0 % | 25,0 % | 30,0 % | 35,0 % | 40,0 % | 45,0 % | 50,0 % |
| Utvalgsstørrelse | | | | | | | | | | |
| 25 | 8,5 % | 11,8 % | 14 % | 15,7 % | 17,0 % | 18,0 % | 18,7 % | 19,2 % | 19,5 % | 19,6 % |
| 50 | 6,0 % | 8,3 % | 9,9 % | 11,1 % | 12,0 % | 12,7 % | 13,2 % | 13,6 % | 13,8 % | 13,9 % |
| 75 | 4,9 % | 6,8 % | 8,1 % | 9,1 % | 9,8 % | 10,4 % | 10,8 % | 11,1 % | 11,3 % | 11,3 % |
| 100 | 4,3 % | 5,9 % | 7,0 % | 7,8 % | 8,5 % | 9,0 % | 9,3 % | 9,6 % | 9,8 % | 9,8 % |
| 150 | 3,5 % | 4,8 % | 5,7 % | 6,4 % | 6,9 % | 7,3 % | 7,6 % | 7,8 % | 8,0 % | 8,0 % |
| 200 | 3,0 % | 4,2 % | 4,9 % | 5,5 % | 6,0 % | 6,4 % | 6,6 % | 6,8 % | 6,9 % | 6,9 % |
| 250 | 2,7 % | 3,7 % | 4,4 % | 5,0 % | 5,4 % | 5,7 % | 5,9 % | 6,1 % | 6,2 % | 6,2 % |
| 300 | 2,5 % | 3,4 % | 4,0 % | 4,5 % | 4,9 % | 5,2 % | 5,4 % | 5,5 % | 5,6 % | 5,7 % |
| 400 | 2,1 % | 2,9 % | 3,5 % | 3,9 % | 4,2 % | 4,5 % | 4,7 % | 4,8 % | 4,9 % | 4,9 % |
| 500 | 1,9 % | 2,6 % | 3,1 % | 3,5 % | 3,8 % | 4,0 % | 4,2 % | 4,3 % | 4,4 % | 4,4 % |
| 600 | 1,7 % | 2,4 % | 2,9 % | 3,2 % | 3,5 % | 3,7 % | 3,8 % | 3,9 % | 4,0 % | 4,0 % |
| 700 | 1,6 % | 2,2 % | 2,6 % | 3,0 % | 3,2 % | 3,4 % | 3,5 % | 3,6 % | 3,7 % | 3,7 % |
| 800 | 1,5 % | 2,1 % | 2,5 % | 2,8 % | 3,0 % | 3,2 % | 3,3 % | 3,4 % | 3,4 % | 3,5 % |
| 900 | 1,4 % | 2,0 % | 2,3 % | 2,6 % | 2,8 % | 3,0 % | 3,1 % | 3,2 % | 3,3 % | 3,3 % |
| 1000 | 1,4 % | 1,9 % | 2,2 % | 2,5 % | 2,7 % | 2,8 % | 3,0 % | 3,0 % | 3,1 % | 3,1 % |
| 1200 | 1,2 % | 1,7 % | 2,0 % | 2,3 % | 2,5 % | 2,6 % | 2,7 % | 2,8 % | 2,8 % | 2,8 % |
| 1400 | 1,1 % | 1,6 % | 1,9 % | 2,1 % | 2,3 % | 2,4 % | 2,5 % | 2,6 % | 2,6 % | 2,6 % |
| 1600 | 1,1 % | 1,5 % | 1,7 % | 2,0 % | 2,1 % | 2,2 % | 2,3 % | 2,4 % | 2,4 % | 2,5 % |
| 1800 | 1,0 % | 1,4 % | 1,6 % | 1,8 % | 2,0 % | 2,1 % | 2,2 % | 2,3 % | 2,3 % | 2,3 % |
| 2000 | 1,0 % | 1,3 % | 1,6 % | 1,8 % | 1,9 % | 2,0% | 2,1 % | 2,1 % | 2,2 % | 2,2 % |

# Informasjonssikkerhetsutvalget

**Tønnes Ingebrigtsen**
mnemonic
(utvalgsleder)

**Maria Bartnes**
SINTEF Digital

**Veronica Jarnskjold Buer**
Datatilsynet

**Lars-Henrik Gundersen**
NorSIS

**Bente Hoff**
Nasjonalt cybersikkerhetssenter,
NSM

**Anders R. Hovdum**
Statens vegvesen

**Tea Knudsen**
Sopra Steria

**Johnny Mathisen**
Telenor

**Ole Tom Seierstad**
Microstoft

**Soner Sevin**
Coop

**Øystein Andreassen**
Nasjonalt Cyberkrimsenter,
Kripos

**Martha Eike**
Storebrand

**Vidar Østmo**
Euronext VPS

**Arne Røed-Simonsen**
Næringslivets Sikkerhetsråd
(utvalgssekretær)

Forside: Istock

Næringslivets
sikkerhets-
råd

www.nsr-org.no