Næringslivets sikkerhets-råd

Mørketalls-undersøkelsen 2020

INNHOLD

FORORD

2020 kommer til å gå inn i historien som et unntaksår. Et år der et virus – Covid-19 – har påvirket det meste av det vi foretar oss, som mennesker, bedrifter, myndigheter og nasjonalstater. Et virus, og en pandemi som har satt økonomisk utvikling i beste fall på vent i flere år, og hvis menneskelige konsekvenser vi i skrivende stund ikke ser rekkevidden av. Samtidig har dette viruset fremtvunget endringer i måten vi omgås på og får samfunnshjulene til å rulle videre. Stikkordet er digitalisering.

Vi er et av verdens mest digitaliserte land, og pandemien har forsterket og fremskyndet digitaliseringen av det norske samfunnet i sin helhet. Under et foredrag i Oslo nylig hevdet Casper Klynge, Danmarks første teknologiambassadør, men som nå er knyttet til Microsoft, at vi i løpet av denne perioden har forsert ca. tre års digital utvikling i samfunnet som helhet. Det er bra for oss, men det kommer ikke uten en medfølgende risiko som også må håndteres, først og fremst gjennom forebyggende virksomhet. Spørsmålet er – gjør vi det? Sikrer vi oss mot digitale trusler eller satser vi på flaks eller tilfeldigheter?

Nasjonalt tok Stortinget nylig et viktig og riktig skritt da ny lov om Etterretningstjenesten ble vedtatt, og vi har nå et lovverk som setter våre myndigheter i stand til å beskytte oss mot utenlandske trusselaktører. Digital sikkerhet er ikke bare en myndighetsoppgave. Digital sikkerhet er en "allemanns-oppgave". Som ledere i næringslivet påhviler det oss et spesielt ansvar for vår virksomhets digitale sikkerhet.

Mørketallsundersøkelsen 2020 er den 12. undersøkelsen om den digitale sikkerhetstilstanden i norsk næringsliv og noen offentlige virksomheter. Denne undersøkelsen har i år blitt utvidet til også å beskrive digital sikkerhet under Covid-19 pandemien. Vi har tatt noen av de opprinnelige spørsmålene og anmodet et noe mindre antall respondenter om å dele sine inntrykk og opplevelser etter noen ukers drift i en periode vi var pålagt meget strenge virksomhetsbeskrankninger av våre politiske myndigheter.

Vi håper årets undersøkelse og rapport vil bidra til bedre og helhetlig sikkerhetsforståelse gjennom økt kunnskap om risikobildet knyttet sammen med behovet for godt forebyggende sikkerhetsarbeid.

Til slutt vil jeg rette en stor takk til alle som har støttet undersøkelsen og gitt sine viktige bidrag til rapporten. Deres engasjement og vilje til å bidra og dele egne erfaringer og synspunkt er uvurderlig for aktualitet og kvalitet i sikkerhetsarbeidet.

Oslo 7. september 2020

Odin Johannessen
Direktør


NASJONAL
SIKKERHETSMYNDIGHET


POLITIET
POLITIDIREKTORATET


telenor


Nordea


coop


NORGES BANK


ADVANSIA
PART OF AFRY


sopra steria


VISMA


ATEA


mnemonic


NTNU CCIS
Center for Cyber and
Information Security

SAMMENDRAG

21 prosent av virksomhetene har fullt ut outsourcet it-driften. Det er på nivå med tidligere undersøkelser, og i 2018 var det 17 prosent som gjorde det. Videre er det 31 prosent som delvis outsourcer, også det på nivå med forrige undersøkelse (33 prosent). Sju av ti av virksomhetene har et rammeverk og/eller styringssystem for informasjonssikkerhet. Det er en økning fra 2016 og 2018, da rundt seks av ti virksomheter hadde det.

Blant de som er utsatt for sikkerhetsbrudd er det tilfeldigheter og uflaks som ses som den vanligste årsaken. Halvparten mener det skyldes menneskelige feil og 39 prosent mener det er mangel på sikkerhetsbevissthet hos ansatte som er årsaken.

Når det gjelder hvordan sikkerhetsbruddet ble oppdaget, er det like mange som sier det var en tilfeldighet som sier ved rutinemessig intern sikkerhetsmonitorering. Når det gjelder årsaker til at hendelser blir oppdaget, er det enkelte forskjeller på de som har rammeverk for informasjonssikkerhet og andre. Blant de som har et rammeverk er det 47 prosent som oppdaget hendelsene ved rutinemessig intern sikkerhetsmonitorering, mot 35 prosent blant andre virksomheter. Samtidig sier 59 prosent av de som ikke har et rammeverk at hendelsene ble oppdaget ved en tilfeldighet, mot 38 prosent av de som har et rammeverk for informasjonssikkerhet.

Blant de som er utsatt for sikkerhetshendelser fører det i 69 prosent av virksomhetene til at selskapets ledelse blir involvert og 38 prosent rapporterer om hendelsen til styret. Når det gjelder følger av hendelsene er det endring av policy og rutiner som er mest vanlig (56 prosent), mens 23 prosent innfører sterkere kontroll av leverandører og konsulenter. Hendelser blir i størst grad rapportert til administrator av det aktuelle system. 4 prosent rapporterer til sektor CERT, mens 2 prosent rapporterer til NorCERT.

Etter at nytt personvernregelverk ble innført i juli 2018 er det 84 prosent som har gjort endringer og/eller forbedringer i arbeidet med personvern og informasjonssikkerhet. Videre er det 10 prosent som i løpet av det siste året har opplevd brudd på personopplysningssikkerheten. Av disse er det 34 prosent som har rapportert dette til Datatilsynet.

77 prosent av virksomhetene har i løpet av det siste året gjennomført aktiviteter som øker de ansattes bevissthet rundt sikkerhet. Blant aktivitetene som er gjennomført er det interne foredrag som er det mest vanlige.

INNLEDNING

Bakgrunn

På oppdrag fra Næringslivets Sikkerhetsråd har Opinion gjennomført Mørketallsundersøkelsen 2020. Dette er den 12. 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 1601 intervju i undersøkelsen.

Datainnsamling

Datainnsamling er gjennomført ved hjelp av telefonintervjuer (CATI), i perioden 4. til 21. februar 2020.

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 1601 respondenter eller intervjuer (n=1601) kan vi med 95 % sannsynlighet si at det riktige resultatet ligger innenfor ± 1,1 og ± 2,4 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	1017	67 %
Offentlig	530	33 %
Totalt	1601	100 %

Virksomhetsstørrelse

Undersøkelsen omfatter virksomheter i følgende størrelsesgrupper.

Virksomhetsstørrelse	Antall intervju	Andel intervju
5 til 19 ansatte	844	52,7 %
20 til 99 ansatte	537	33,5 %
100 ansatte eller flere	220	13,7 %
Totalt	1601	100 %

Geografi

Under er en oversikt over respondentenes fylkesvise tilhørighet:

Fylke	Antall	Andel intervju
Oslo	189	11.8 %
Rogaland	152	9.5%
Møre og Romsdal	95	5,9 %
Nordland	92	5.7 %
Viken	319	19,9 %
Innlandet	142	8.9 %
Vestfold og Telemark	120	7.5 %
Agder	90	5.6 %
Vestland	200	12.5 %
Trøndelag	128	8,0 %
Troms og Finnmark	74	4.6 %
Totalt	1601	100,0 %

Bransje

Undersøkelsen omfatter virksomheter i følgende bransjer.

Bransje	Antall	Andel intervju
Primær	14	0,9 %
Industri etc.	148	9,2 %
Bygg- og anleggsvirksomhet	112	7,0 %
Varehandel etc.	411	25,7 %
Transport og lagring	42	2,6 %
Overnattings- og serverings-virksomhet	41	2,6 %
Tjenesteytende næringer	271	16,9 %
Offentlig administrasjon	103	6,4 %
Undervisning	177	11,1 %
Helse og sosial	250	15,6 %
Kulturell virksomhet	32	2,0 %
Totalt	1601	100,0 %

1.

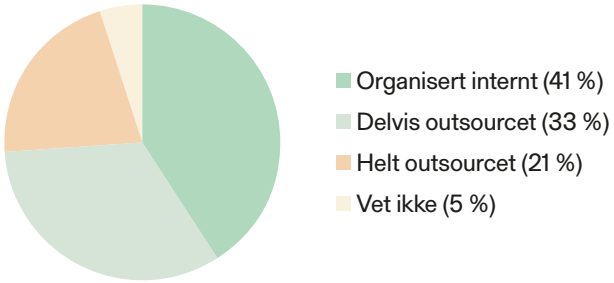
Organisering av IT-driften

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

1.1 Outsourcing

21 prosent av virksomhetene har outsourcet it-driften helt. 33 prosent av virksomhetene har delvis outsourcet, mens 41 prosent har organisert it-driften internt. Andelen som outsourcer helt er på nivå med tidligere (22 prosent i 2016 og 17 prosent i 2018).

Spørsmål: Er virksomhetens it-drift organisert ved at den er helt outsourcet, delvis outsourcet eller er all drift organisert internt? (n=1601)



Figur 1

I 2018 fant vi at det er mer vanlig å sette ut hele it-driften blant virksomheter med mindre enn 100 ansatte enn for virksomheter med 100 ansatte eller flere. I 2020 er det 21 prosent av virksomheter med 5-19 ansatte som setter ut hele driften, 22 prosent av de med 20 til 99 og 16 prosent av de med 100 ansatte eller flere. Disse forskjellene er ikke statistisk signifikante, men årets resultater følger samme mønster som tidligere undersøkelser.

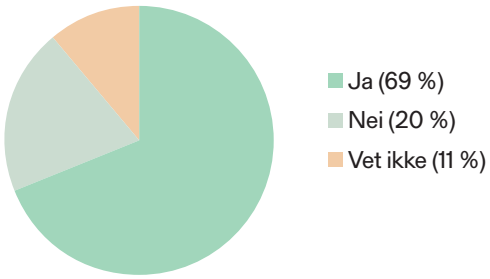
Blant de som benytter seg av outsourcing helt eller delvis, er det 14 prosent som benytter outsourcingtjenester i utlandet. Det er noe mer utbredt blant store virksomheter med 100 ansatte eller mer. I 2016 var det 8 prosent som outsourcet til utlandet og i 2018 var det 14 prosent.

Blant de som benytter outsourcingtjenester i utlandet, er det 74 prosent som vet hvor data fysisk er lagret eller blir behandlet, mens 26 prosent ikke vet det.

1.2 Styringssystem og rammeverk

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

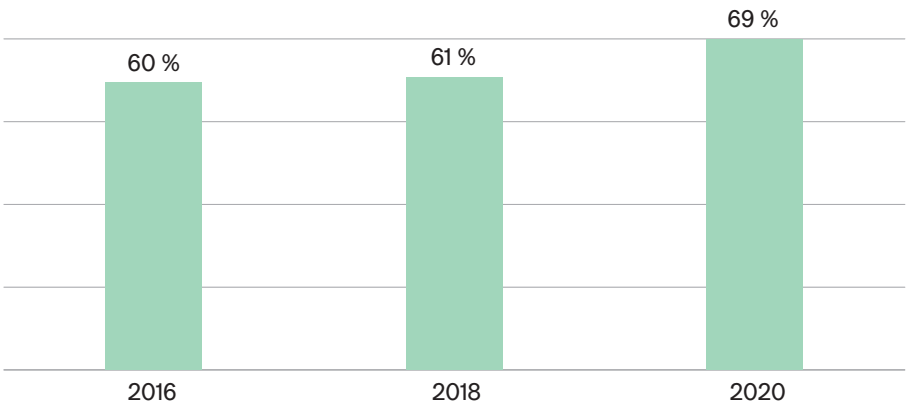
Spørsmål: Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerhet? (n=1601)



Figur 2

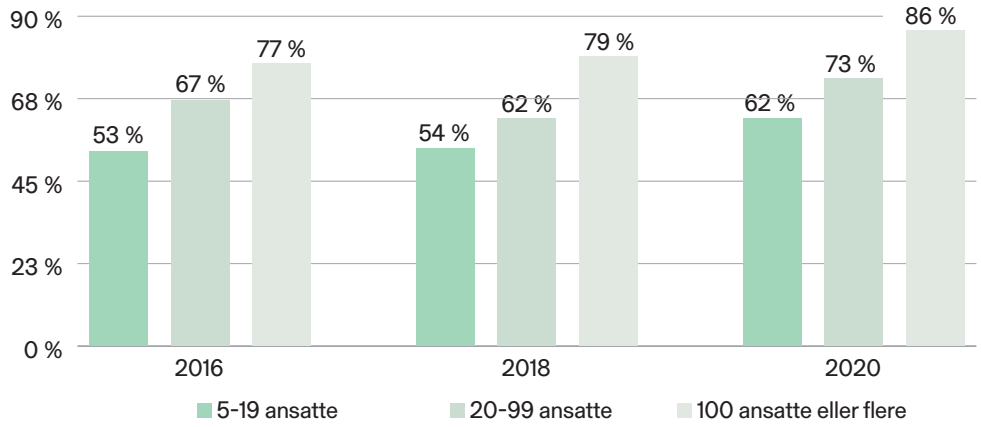
Sammenlignet med tidligere undersøkelser er det en høyere andel som har et rammeverk og/eller styringssystem for informasjonssikkerhet. Mens det i 2016 var 60 prosent som hadde det, er det nå 69 prosent.

Spørsmål: Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerhet? (n=1500/1601) (Andel som svarer ja)



Figur 3

Det er forskjeller mellom de minste og de største virksomhetene på dette spørsmålet. Mens 62 prosent av virksomheter med 5 til 19 ansatte har det, er det 73 prosent av de med 20 til 99 ansatte og 86 prosent av de med 100 ansatte eller flere som har rammeverk eller styringssystem for informasjonssikkerhet. Tilsvarende mønstre har vi funnet i tidligere undersøkelser.

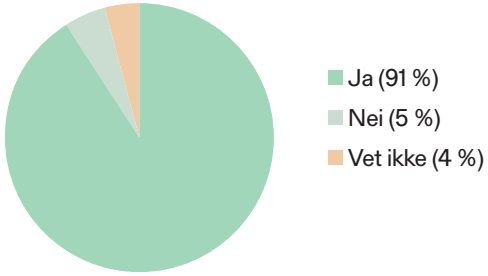


Figur 4

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

De som har et rammeverk eller styringssystem mener i stor grad at det etterleves i organisasjonen; ni av ti er av den oppfatningen. 91 prosent svarer ja, som er på nivå med 2018 da 88 prosent svarte det samme.

Spørsmål: Opplever du at rammeverk/styringssystem for sikkerhet blir etterlevd i din organisasjon? (n=1107 – de som har rammeverk/styringssystem)



Figur 5

Foto: Unsplash

2.

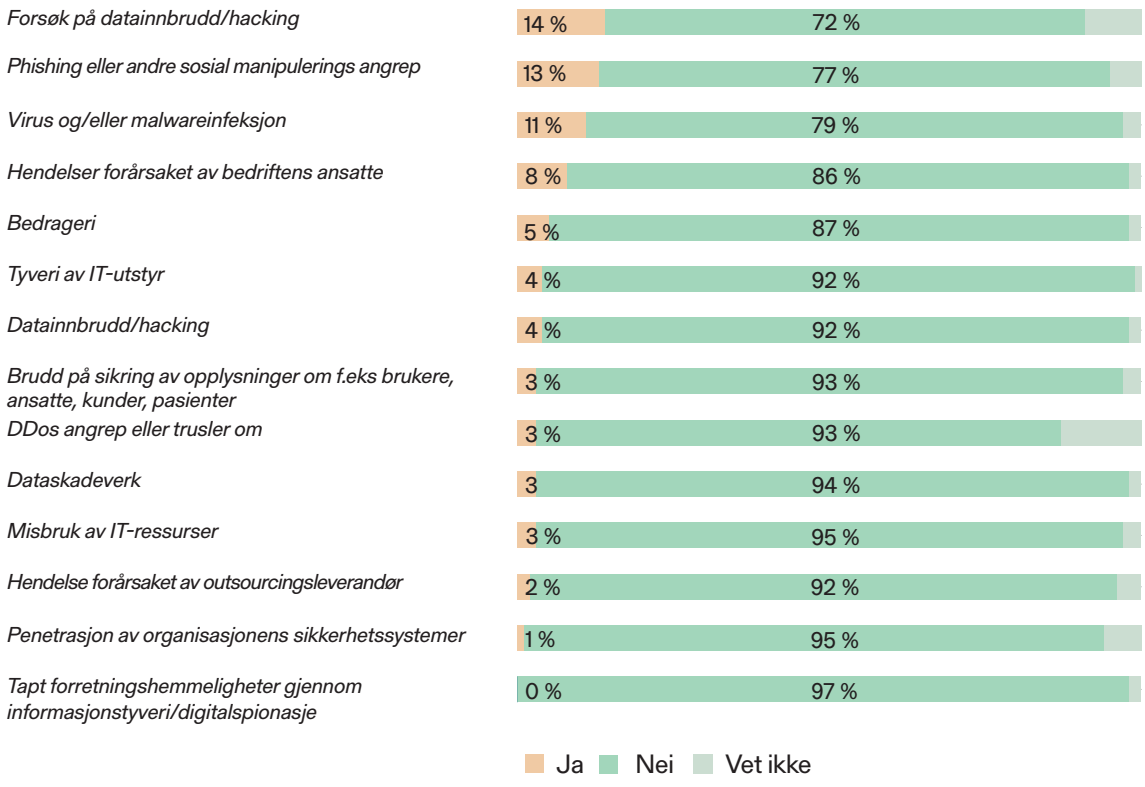
Hendelser

Dette kapitlet 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

Forsøk på datainnbrudd/hacking, phishing og virus og/eller malwareinfeksjon er de mest vanlige hendelsene. Henholdsvis 14, 13 og 11 prosent av virksomhetene har opplevd disse. Hendelser forårsaket av outsourcingleverandør er på den andre siden langt mindre utbredt. Det samme gjelder penetrasjon av virksomhetens sikkerhetssystem og tapte forretningshemmeligheter på grunn av digital spionasje som kun 0,2 prosent sier de har opplevd.

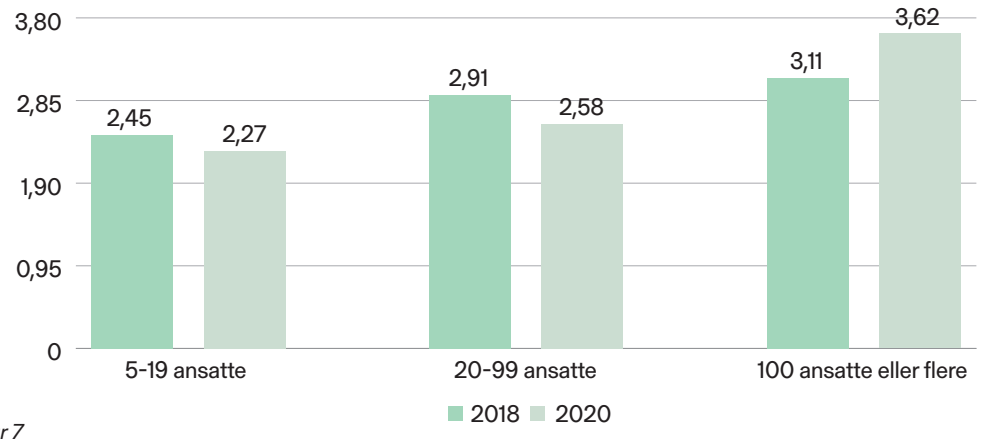
Spørsmål: Jeg vil nå lese opp noen mulige informasjonssikkerhetshendelser og ber deg svare ja eller nei på om virksomheten har vært utsatt for disse i kalenderåret 2019? (n=1601)



Figur 6

I gjennomsnitt er alle virksomhetene rammet av 0,7 av de ulike typer informasjonssikkerhetshendelse vi har spurt om. Blant de som har opplevd en hendelse, har man i snitt opplevd 2,6 forskjellige typer hendelser. Ikke unaturlig er det mer vanlig med slike hendelser jo større virksomheten er. (Vi snakker her om antall forskjellige typer hendelser, ikke antall hendelser totalt.)

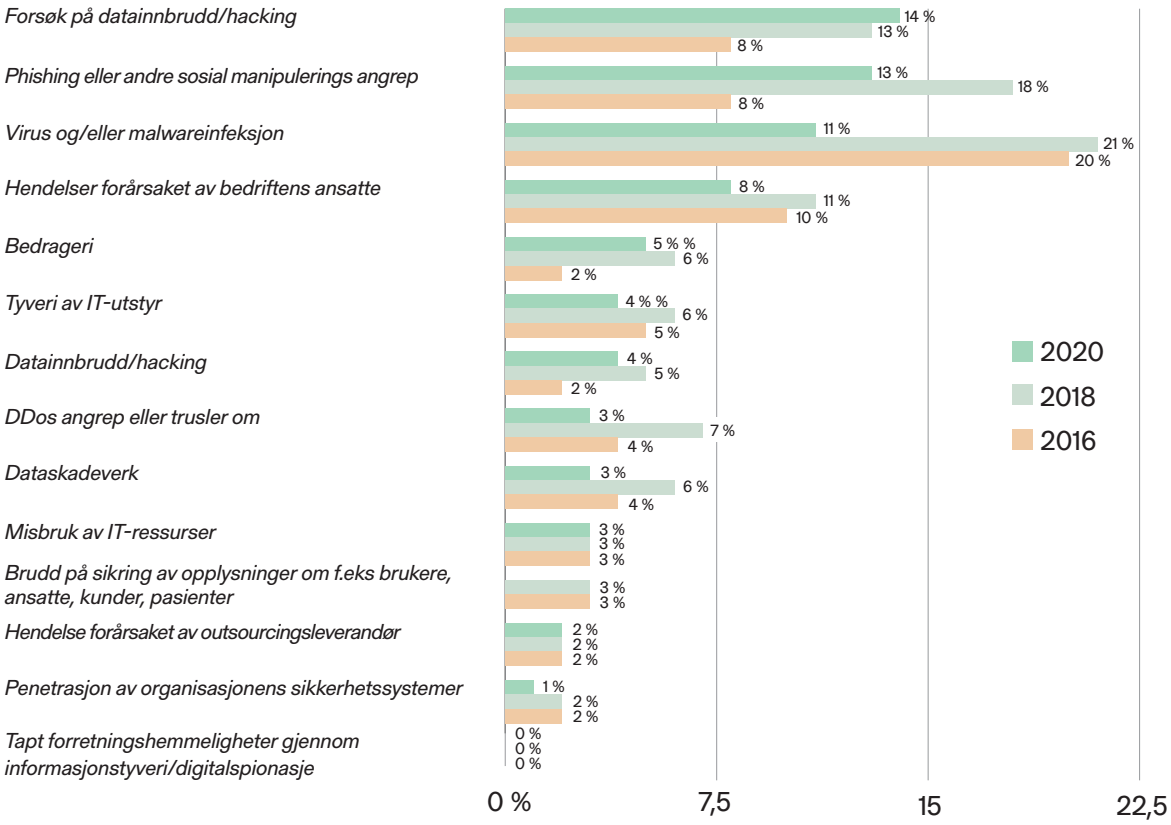
Snitt antall type hendelser blant virksomheter (n=563 – svart ja på en eller flere alternativ i spørsmålet).



Figur 7

De minste bedriftene har et snitt som er signifikant lavere enn de to andre størrelsesgruppene, og de med 100 ansatte eller flere er signifikant forskjellig fra de med 20 til 99 ansatte. Med andre ord blir store bedrifter rammet av flere typer hendelser.

Sammenlignet med 2018, er forsøk på datainnbrudd/hacking på samme nivå, mens det er lavere andel som mener de har vært utsatt for phising og virus.



Figur 8

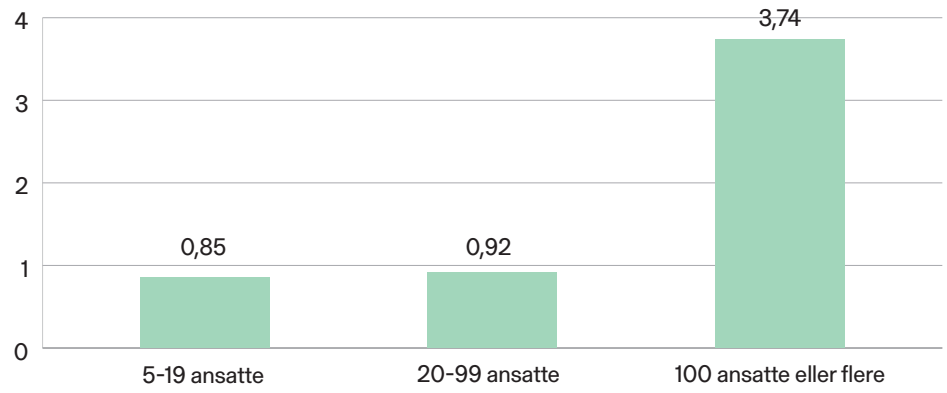
2.2 Hendelser med negative konsekvenser

På spørsmål om informasjonssikkerhetshendelser som påvirket virksomheten negativt i form av økonomisk tap eller svekket markedsposisjon er det 14 prosent av virksomhetene som vet at de har hatt slike hendelser og som klarer å tallfeste hvor mange.

Blant de som har opplevd hendelser som har hatt negative konsekvenser med økonomisk tap eller svekket markedsposisjon, har man i gjennomsnitt opplevd 9,4 slike hendelser i løpet av 2019. Median er 2 hendelser, så det er noen få virksomheter som trekker 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) 1,3 hendelser med negative konsekvenser i løpet av 2019. Virksomheter med 100 ansatte eller flere opplevde i snitt 3,7 sikkerhetshendelser med økonomisk tap eller svekket markedsposisjon. Blant de minste bedriftene er tallet 0,85 hendelser. Disse forskjellene er imidlertid ikke signifikante.

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



Figur 9

Når det gjelder hva som var den mest alvorlige hendelsen, uavhengig av om hendelsen fikk negativ konsekvenser eller ikke, er det virus, phishing, hacking og svindelforsøk som går igjen i størst grad.

Spørsmål: Hva var den mest alvorlige hendelsen i 2017?

Figur 10

Når det gjelder grunnen til at man opplever en hendelse som den mest alvorlige, er det faren for å tape informasjon eller at den kommer på avveie, samt tapt arbeidstid som er mest nevnt.

3.

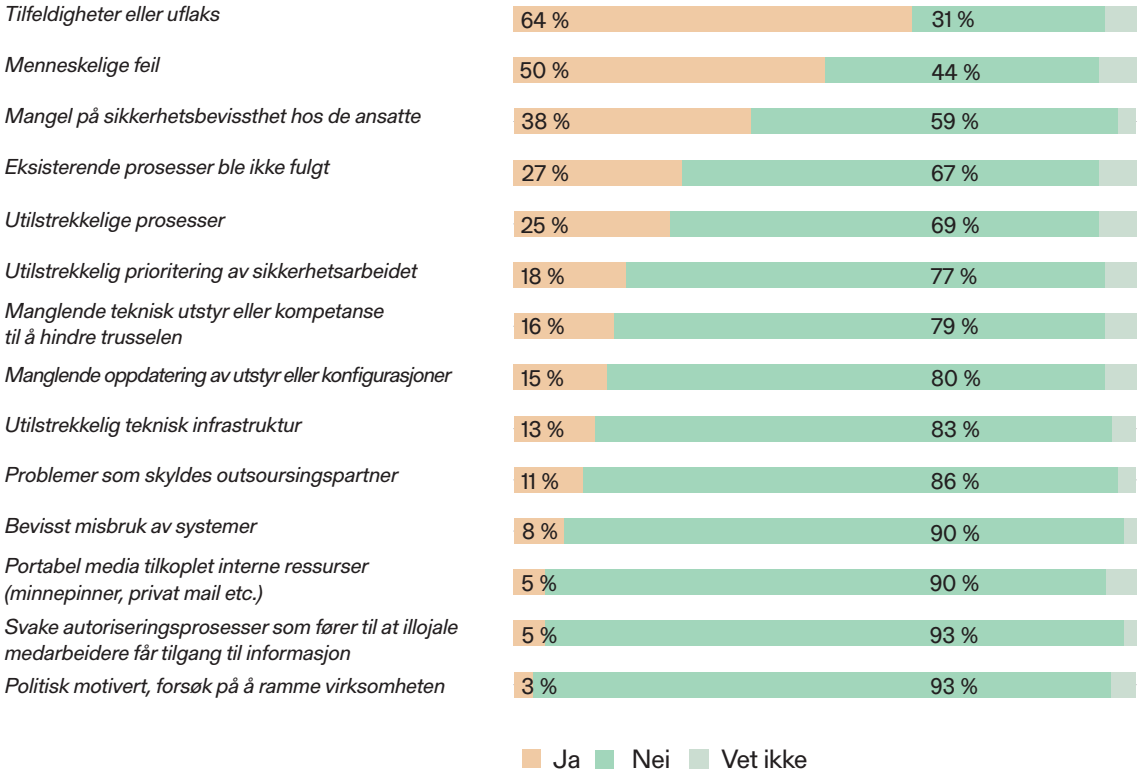
Årsaker

Dette kapitlet handler om hvorfor
sikkerhetsbruddene 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.

Spørsmål: Var noen av følgende faktorer årsak til at sikkerhetsbruddet oppsto? (n=454)



Figur 11

Blant de som har opplevd hendelser er det 64 prosent som mener årsaken var tilfeldigheter eller uflaks, mens halvparten også tilskriver sikkerhetsbruddet menneskelige feil.

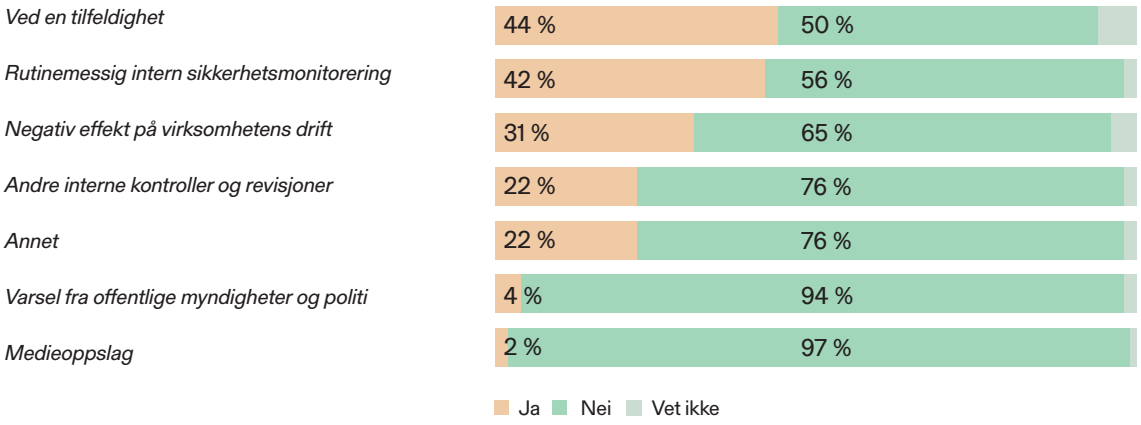
Tilfeldigheter og uflaks er like utbredt i alle typer virksomheter. Menneskelige feil er i større grad en årsak i store virksomheter enn i små. Mens 49 og 46 prosent av virksomheter i de to minste størrelsesgruppene som har opplevd hendelser mener at det skyldes menneskelige feil, er det 63 prosent av de med 100 ansatte eller flere som sier det samme.

Hvis vi ser på forskjeller mellom virksomheter som enten har eller ikke har et rammeverk og/eller styringssystem for informasjonssikkerhetsarbeidet finner vi enkelte forskjeller. De som har et rammeverk opplever i mindre grad at sikkerhetshendelser kommer av utilstrekkelige prioriteringer av sikkerhets-arbeidet, utilstrekkelige prosesser og manglende oppdatering av utstyr.

3.2 Hvordan sikkerhetsbruddet ble oppdaget

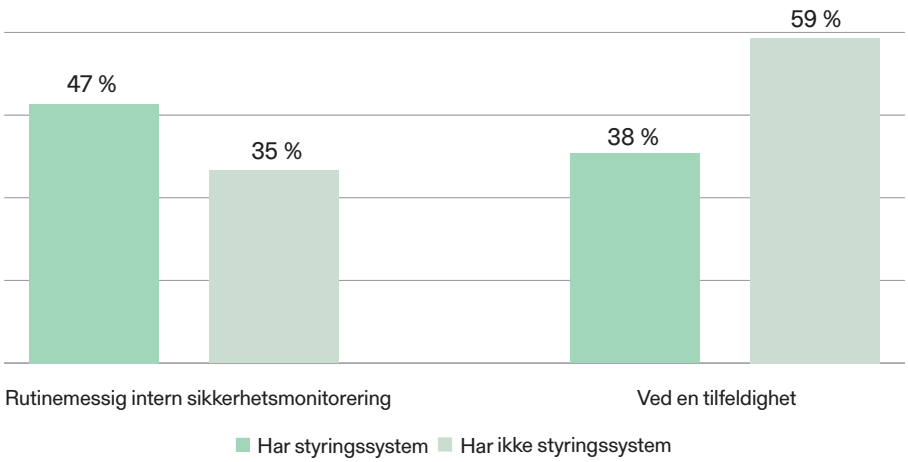
Når det gjelder hvordan sikkerhetsbruddet ble oppdaget, er det like mange som sier det var en tilfeldighet, som sier ved rutinemessig intern sikkerhetsmonitorering.

Spørsmål: Var noe av følgende årsak til at hendelsen ble oppdaget? (n=454)



Figur 12

Det er enkelte forskjeller mellom de som har et rammeverk for informasjonssikkerhet og andre virksomheter. Blant de som har et rammeverk er det 47 prosent som oppdaget hendelsene ved rutinemessig intern sikkerhetsmonitorering, mot 35 prosent av andre virksomheter. Samtidig sier 59 prosent av de som ikke har et rammeverk at hendelsene ble oppdaget ved en tilfeldighet, mot 38 prosent blant de som har et rammeverk for informasjonssikkerhet slik figuren nedenfor viser.

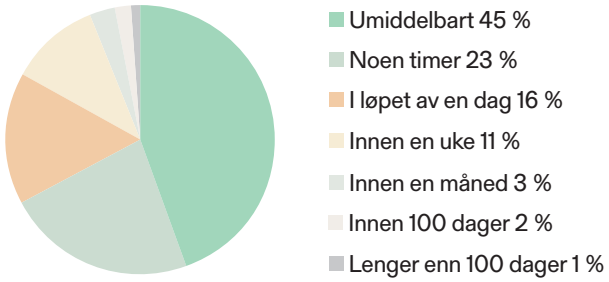


Figur 13

Samtidig ser vi at de minste virksomhetene med 5 til 19 ansatte i større grad enn større virksomheter oppdager hendelser ved en tilfeldighet.

Nær halvparten av virksomhetene oppdaget hendelsen umiddelbart (svarer for siste/mest alvorlige hendelse). Ytterligere 23 prosent oppdaget den i løpet av noen timer og 16 prosent i løpet av en dag. Det er ingen forskjell mellom virksomheter som har eller ikke har styringssystem for informasjonssikkerhet, eller store og små virksomheter, men virksomheter i privat sektor oppdager hendelsen umiddelbart i noe større grad enn offentlige (49 mot 39 prosent).

Spørsmål: Hvor lang tid tok det fra hendelsen skjedde til den ble oppdaget?



Figur 14

Foto: Unsplash

4.

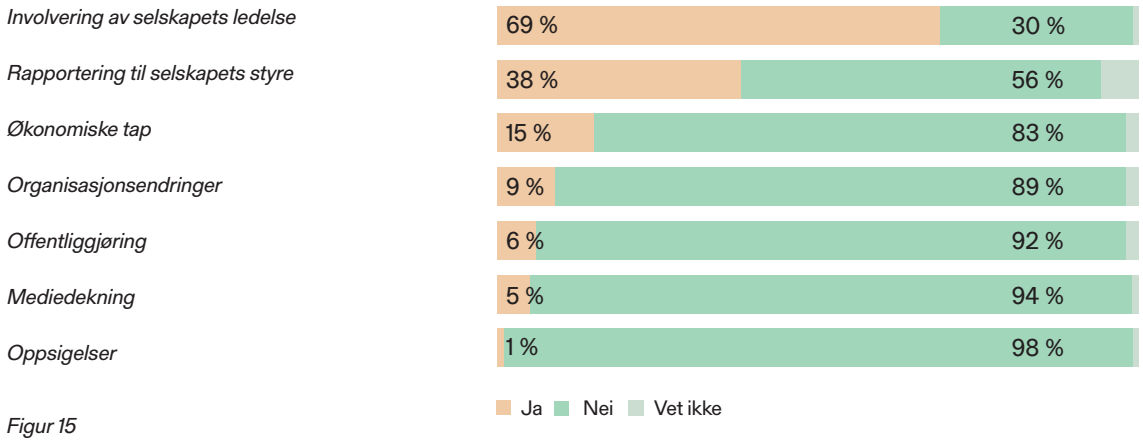
Følger og håndtering av hendelser

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

4.1 Følger av hendelsen

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

Spørsmål: Førte denne spesifikke hendelsen til følgende? (n=454)
Respondenten svarer ut fra siste hendelse/mest alvorlige hendelse.

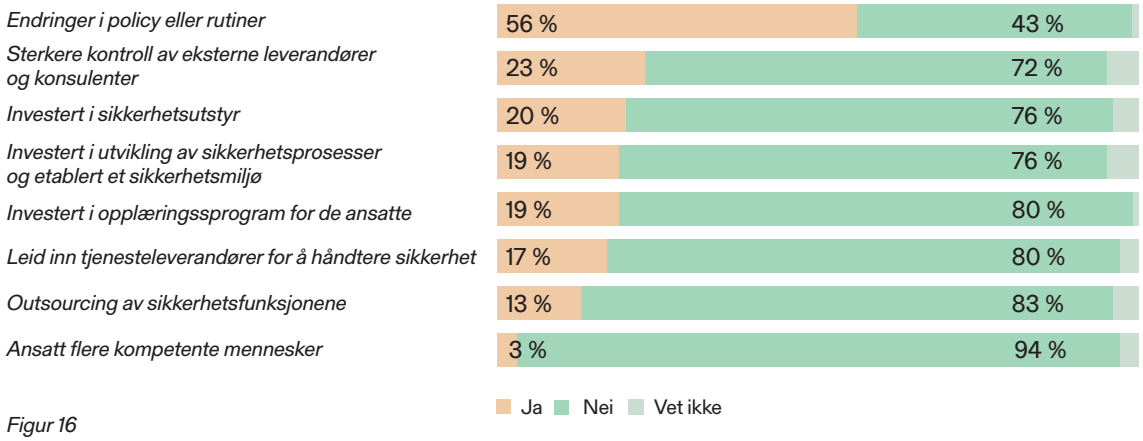


Figur 15

Involvering av selskapets ledelse og styre er de vanligste følgene, på samme måte som i tidligere undersøkelser. Det er i liten grad forskjell på ulike typer virksomheter med unntak av at følgene for offentlige virksomheter i større grad er mediedekning og offentliggjøring.

I tillegg til følgene nevnt over, har sikkerhetshendelsene også ført til endinger i en del av de utsatte organisasjonene, der 56 prosent har endret policy og rutiner.

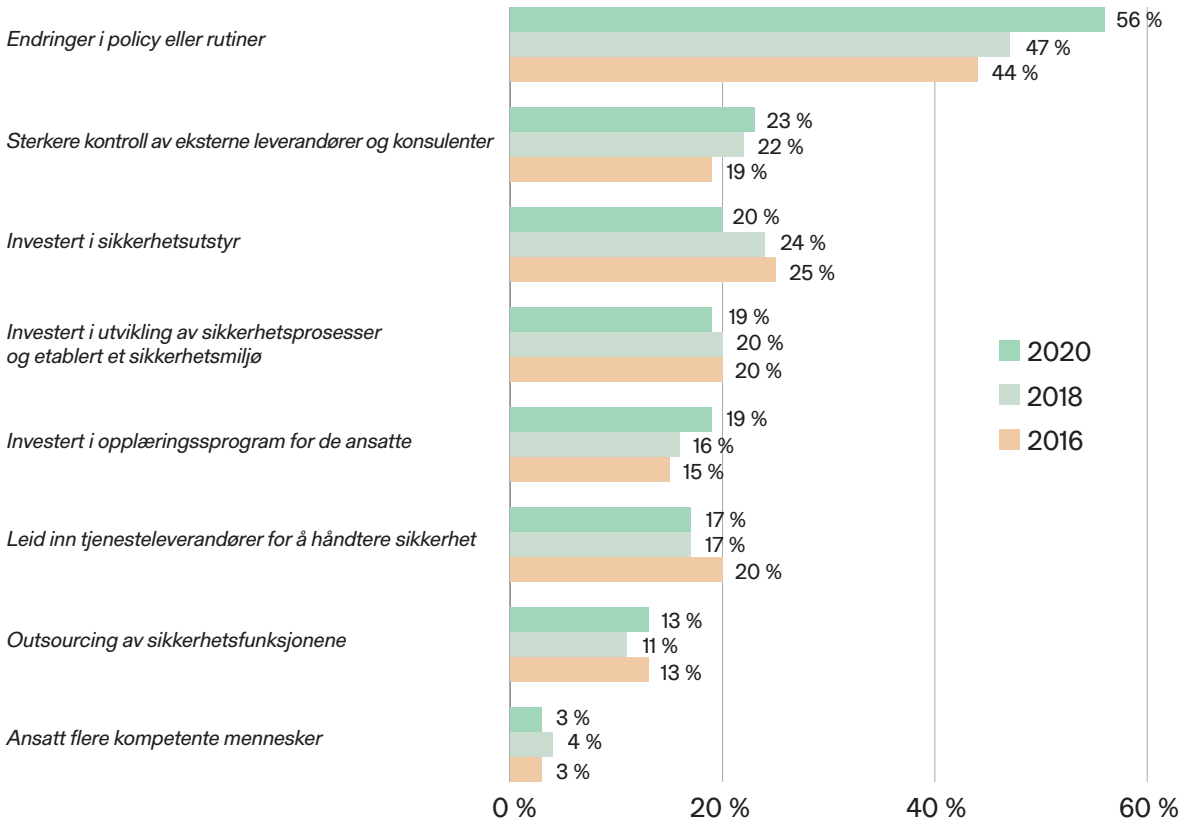
Spørsmål: Som et resultat av hendelsen, ble noen av følgende endringer gjort i organisasjonen? (n=454)



Figur 16

Private virksomheter har i noe større grad leid inn tjenesteleverandører for å håndtere sikkerhet enn det offentlige har gjort. Det samme gjelder virksomheter uten rammeverk for informasjonssikkerhet. Utover dette er det ikke klare forskjeller mellom ulike typer virksomheter på dette spørsmålet.

Sammenlignet med 2016 og 2018 er det en økning i andelen som har endret policy eller rutiner som følge av sikkerhetshendelsen.

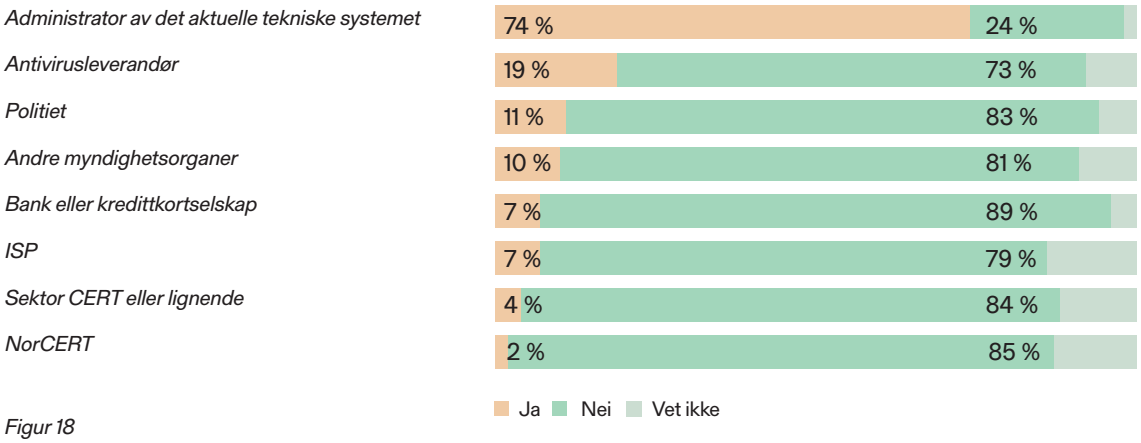


Figur 17

4.2 Rapportering

74 prosent av virksomheter som har opplevd sikkerhetshendelser har rapportert hendelsen til administrator av det aktuelle tekniske systemet, 19 prosent har rapportert til antivirusleverandør og 11 prosent har rapportert hendelsen til politiet. Rapportering til sektor CERT eller NorCERT er det kun 4 og 2 prosent som gjør.

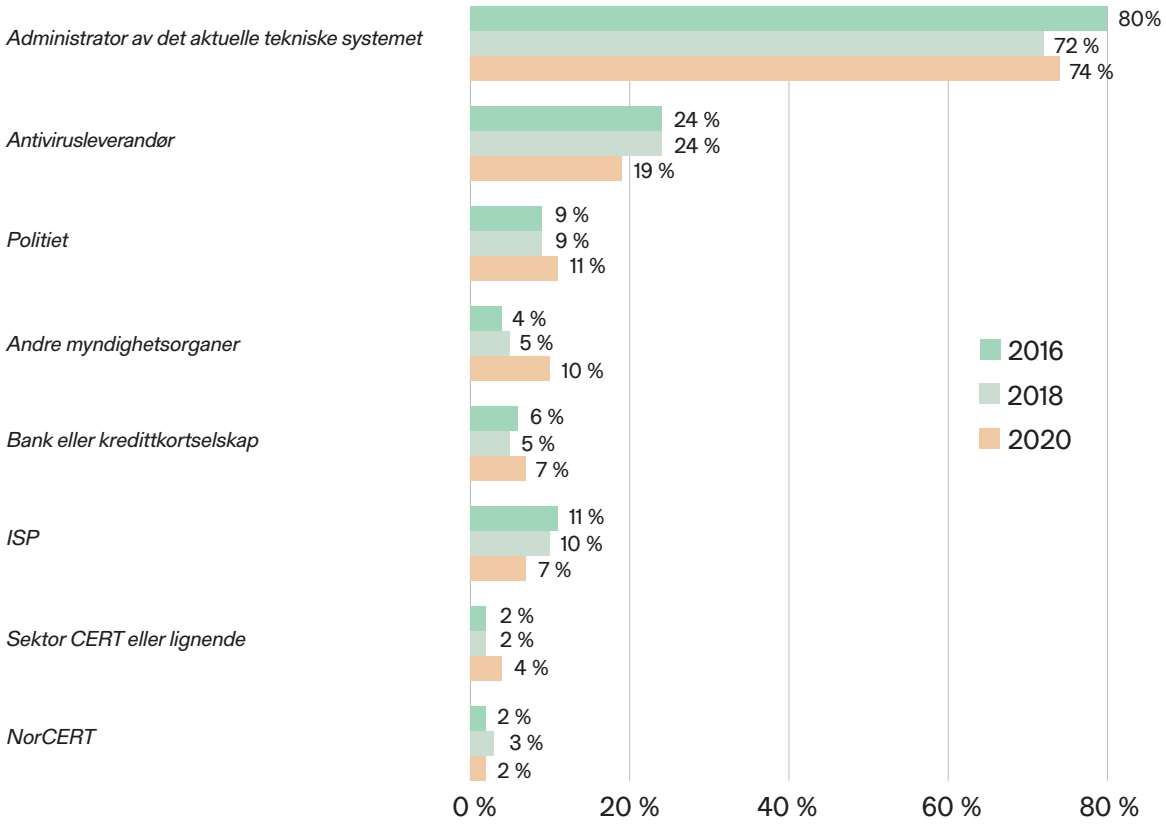
Spørsmål: Ble hendelsen rapportert til noen av følgende? (n=454)



Figur 18

Det er ikke klare mønstre når det gjelder type virksomheter. Store virksomheter rapporterer i mindre grad til antivirusleverandør enn små virksomheter. Store virksomheter rapporterer i større grad til andre myndighetsorganer, det samme gjelder offentlige virksomheter og de med rammeverk for informasjonssikkerhet. Når det gjelder sektor CERT og NorCERT rapporterer offentlige virksomheter i større grad til sektor CERT, men de svarer også vet ikke i større grad enn private.

Sammenlignet med 2018 er det et stabilt bilde på spørsmål om hvem hendelsen rapporteres til.



Figur 19

4.3 Hendelsens kostnad

Blant de som er utsatt for hendelser og som klarer å tallfeste hva hendelsen har kostet økonomisk, inkludert de som vet at den ikke har hatt noen økonomisk kostnad, er det i snitt en kostnad på nær 85 000 kroner for den mest alvorlige hendelsen i 2019. De som er hardest rammet, estimerer en kostnad på 5 millioner. Det er ikke signifikant forskjell mellom virksomheter som har eller ikke har styringssystem for informasjonssikkerhet, eller mellom virksomheter i ulike størrelsesgrupper.

5.

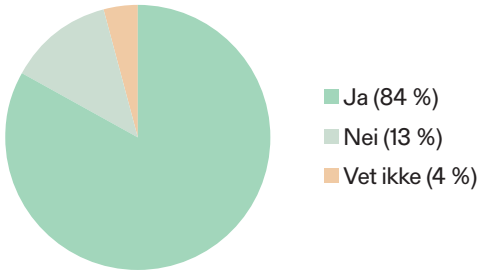
Personvernregel-verk og sikkerhets-bevissthet

Dette kapitlet handler om endringer i arbeid
med personvern og informasjonssikkerhet
i forbindelse med GDPR og aktiviteter
for økt sikkerhetsbevissthet blant ansatte.

5.1 Endringer som følge av GDPR

I 84 prosent av virksomhetene har innføringen av nytt personvernregelverk (GDPR) ført til at organisasjonen har gjort endringer og/eller forbedringer i arbeidet med personvern og informasjonssikkerhet.

Spørsmål: Nytt personvernregelverk (GDPR) trådte i kraft fra juli 2018. Har dette medført at organisasjonen har gjort endringer/forbedringer i arbeidet med personvern og informasjonssikkerhet? (n=1601)



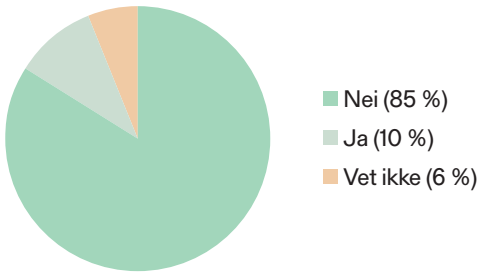
Figur 20

79 prosent av de minste virksomhetene (5-19 ansatte) har gjort dette, mens for de med 20 til 99 og 100+ ansatte er tallene henholdsvis 87 og 92 prosent.. Forskjellen mellom de minste virksomhetene og de to andre størrelses- gruppene er signifikant. Offentlige virksomheter har endret/forbedret arbeidet med personvern i noe større grad enn private (89 mot 81 prosent) og de med rammeverk for informasjonssikkerhet i større grad enn de uten rammeverk (90 mot 67 prosent).

5.2 Opplevd brudd på personopplysningssikkerheten

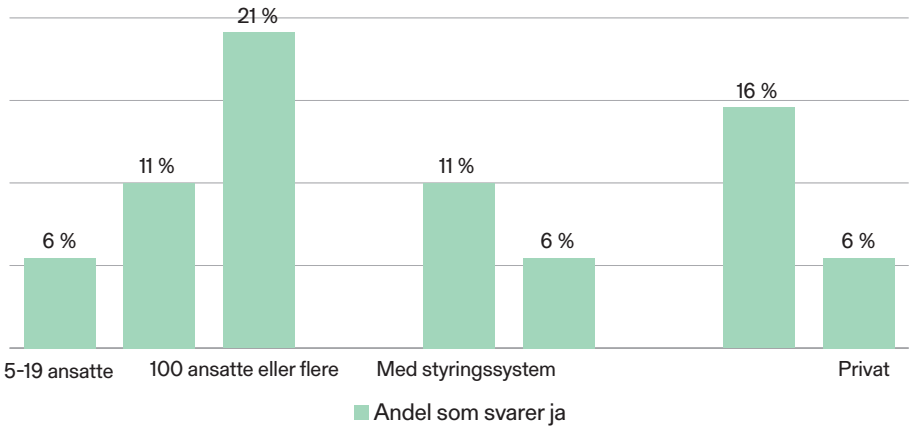
10 prosent har i løpet av det siste året opplevd brudd på personopplysningssikkerheten.

Spørsmål: Har virksomheten i løpet av de siste 12 månedene opplevd brudd på personopplysningssikkerheten, også kalt GDPR-avvik? (n=1601)



Figur 21

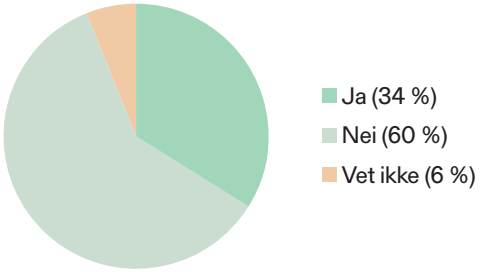
Store virksomheter har opplevd dette i langt større grad enn små. Mens 21 prosent av virksomheter med 100+ ansatte har opplevd GDPR-avvik, er det 6 prosent av de minste virksomhetene som har opplevd det. Virksomheter i offentlig sektor har opplevd det i større grad enn private (16 mot 6 prosent), og virksomheter med et rammeverk for informasjonssikkerhet har opplevd det i større grad enn de uten rammeverk (11 mot 6 prosent).



Figur 22

Blant de som har opplevd GDPR-avvik er det 34 prosent som har rapportert avviket til Datatilsynet.

Spørsmål: Er brudd på personopplysningssikkerheten (GDPR-avvikene) virksomheten har vært utsatt for siste 12 måneder blitt rapportert til Datatilsynet? (n=153)

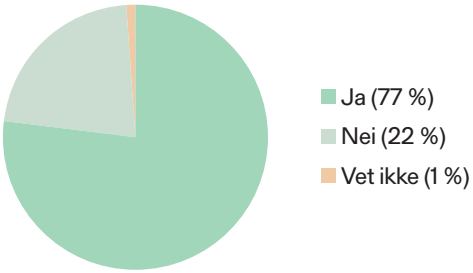


Figur 23

5.3 Økt bevissthet rundt sikkerhet blant ansatte

77 prosent av virksomhetene har i løpet av det siste året gjennomført tiltak for å øke de ansattes bevissthet rundt sikkerhet.

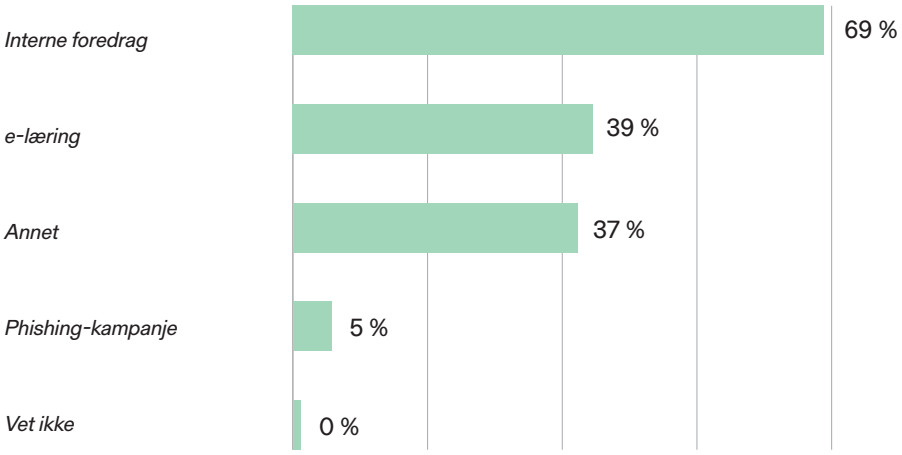
Spørsmål: Har virksomheten gjennomført aktiviteter som øker ansattes bevissthet rundt sikkerhet i løpet av det siste året? (n=1601)



Figur 24

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

Spørsmål: Hvilken type aktiviteter som øker ansattes bevissthet rundt sikkerhet er gjennomført i løpet av det siste året? (n=1231)



Figur 25

E-læring er noe mer vanlig tiltak blant de som har rammeverk for informasjonssikkerhet, blant offentlige og i virksomheter med mer enn 19 ansatte. Videre er phishing-kampanje mer vanlig blant store (100+ ansatte) enn blant mindre og i de med rammeverk for informasjonssikkerhet. Utover det er det ingen klare forskjeller mellom ulike typer virksomheter.

5.4 Mørketall og korona

Mørketallsundersøkelsen ble gjennomført i februar 2020, men spørsmålene rettet seg mot hendelser i 2019. Etter at regjeringen innførte strenge tiltak mot koronasmitte 13. mars 2020, måtte et stort antall arbeidstakere ha hjemmekontor. Dette reiste mange spørsmål om IT-sikkerheten, samt sårbarheten for svindelforsøk.

Derfor besluttet Næringslivets Sikkerhetsråd å gjennomføre en ekstra undersøkelse begrenset til hendelser i februar og mars 2020.

Undersøkelsen ble gjennomført av Opinion for Næringslivets Sikkerhetsråd. Det er gjennomført 900 intervju med norske virksomheter med 5 ansatte eller flere. Målgruppen for undersøkelsen og metode for datainnsamling er identisk med Mørketallsundersøkelsen.

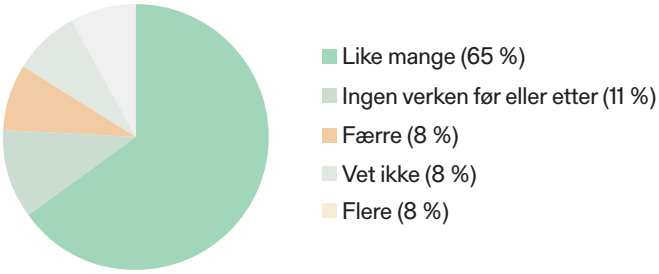
Datainnsamlingen er gjennomført i perioden 24. mars til 8. april 2020, og data er vektet på geografi og størrelse. Med 900 intervjuer må tallene tolkes med en feilmargin på +/- 1,4 til 3,3 prosentpoeng.

Flere eller færre sikkerhetshendelser?

Like mange opplever færre som flere sikkerhetshendelser

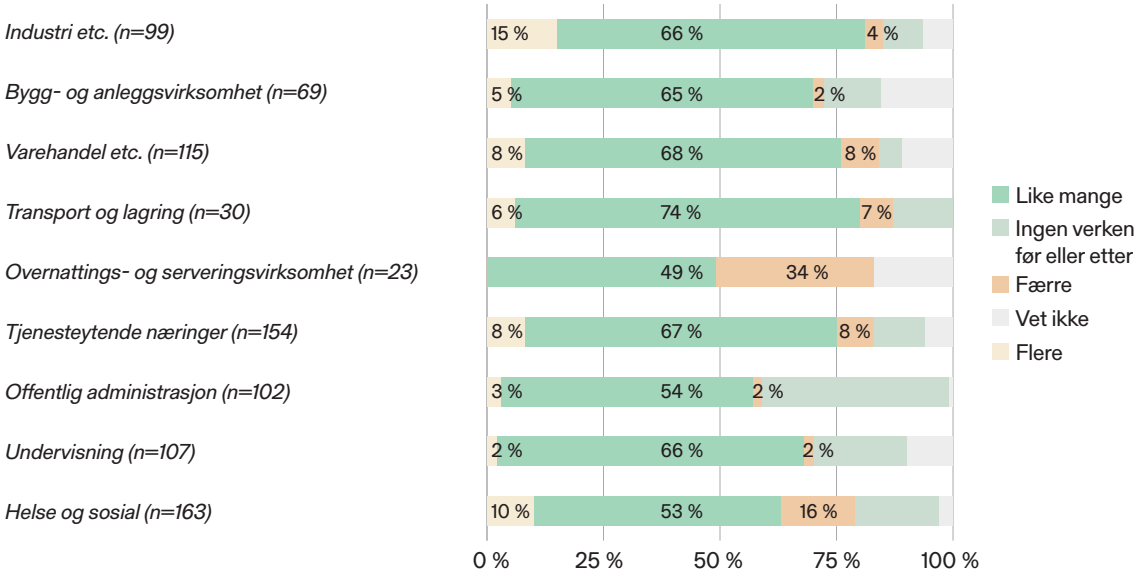
Det er 8 prosent som i løpet av koronakrisen har opplevd flere it-sikkerhetshendelser, men det er samtidig 8 prosent som har opplevd færre hendelser.

Det er ikke forskjell på virksomheter av ulik størrelse på dette spørsmålet, men det er noen klare forskjeller mellom ulike bransjer (se figur 27).



Figur 26

Overnatting og servering skiller seg klart fra andre bransjer ved å oppleve færre hendelser under koronakrisen. Hele 34 prosent av virksomhetene i overnatting/servering har opplevd færre hendelser (merk. relativt få respondenter i denne bransjen (23). Også helse og sosial svarer at de har opplevd færre hendelser (16 prosent). Blant bransjene som i størst grad har opplevd flere hendelser finner vi industri der 15 prosent har opplevd flere hendelser.



Figur 27

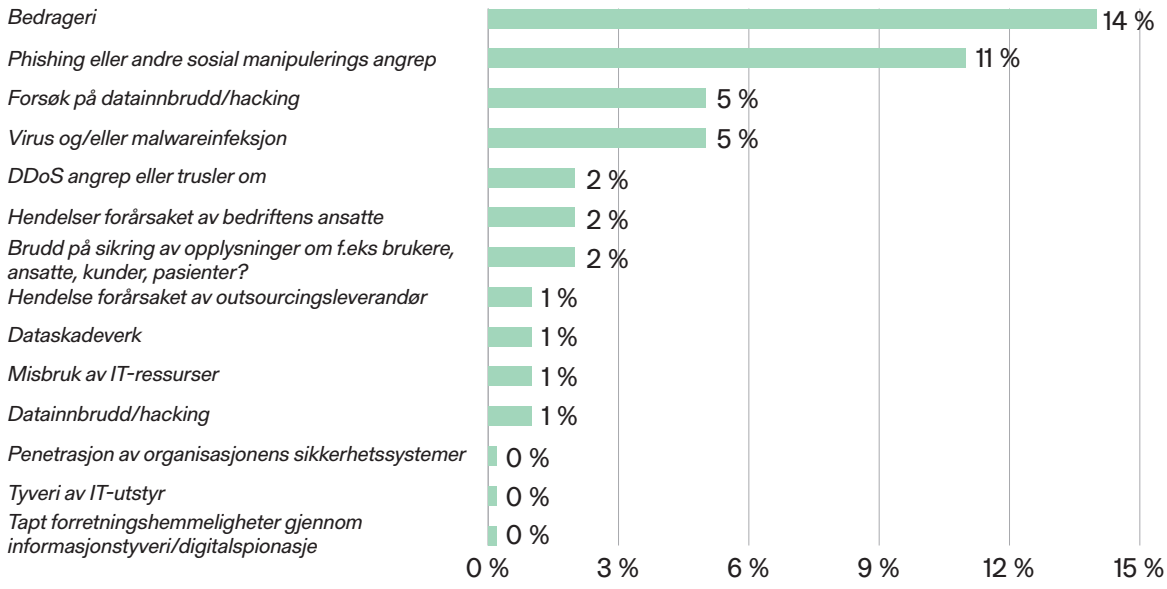
14 prosent utsatt for bedrageri

Den mest vanlige hendelsen å bli utsatt for er bedrageri som 14 prosent har opplevd, fulgt av phishing med 11 prosent.

Hacking, tyveri av it-utstyr og tap av forretningshemmeligheter er virksomhetene i liten grad utsatt for.

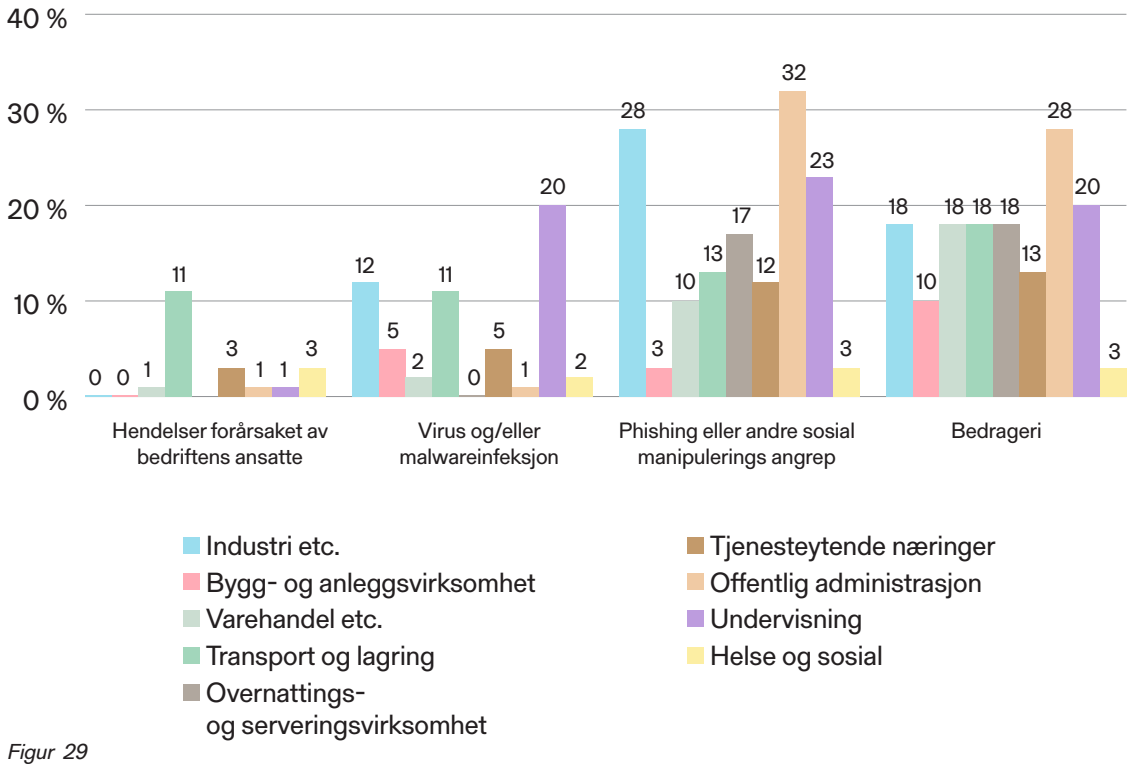
Store og små virksomheter er like utsatt for de ulike typene hendelser, mens det er enkelte bransjeforskjeller. Phishing er mest vanlig i industri, offentlig administrasjon og undervisning. Hendelser forårsaket av de ansatte er mer vanlig i transportbransjen. Virus/malware er undervisning mest utsatt for, mens bedrageri er noe mer vanlig å bli utsatt for blant virksomheter i offentlig administrasjon.

Type hendelse



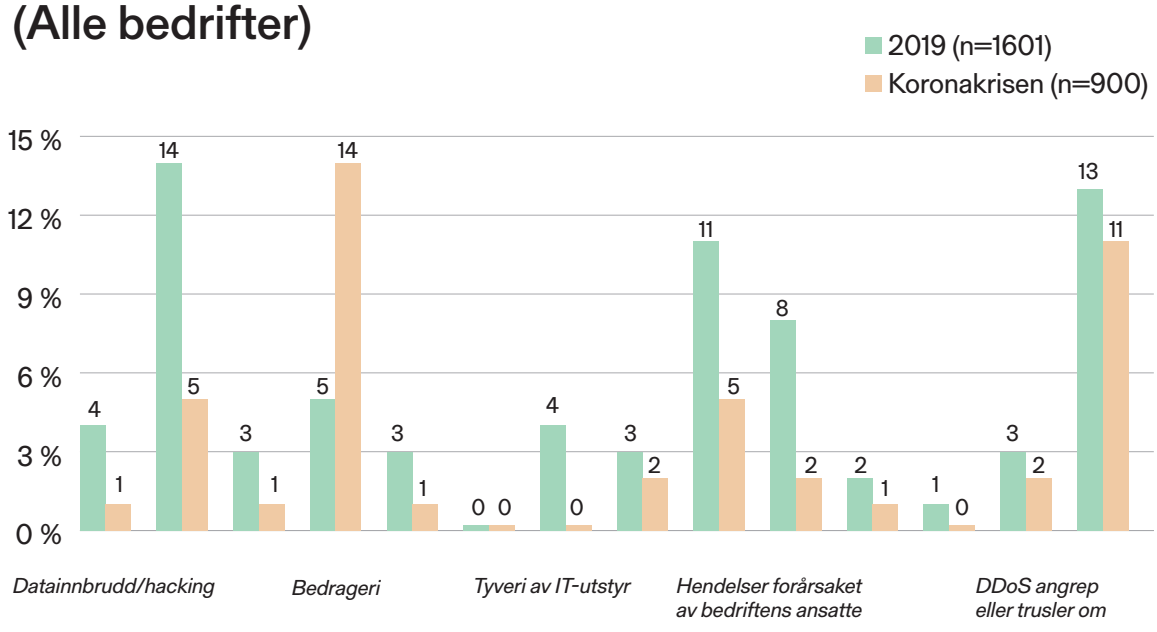
Figur 28

Type hendelser i ulike bransjer (Utvalgte hendelser)



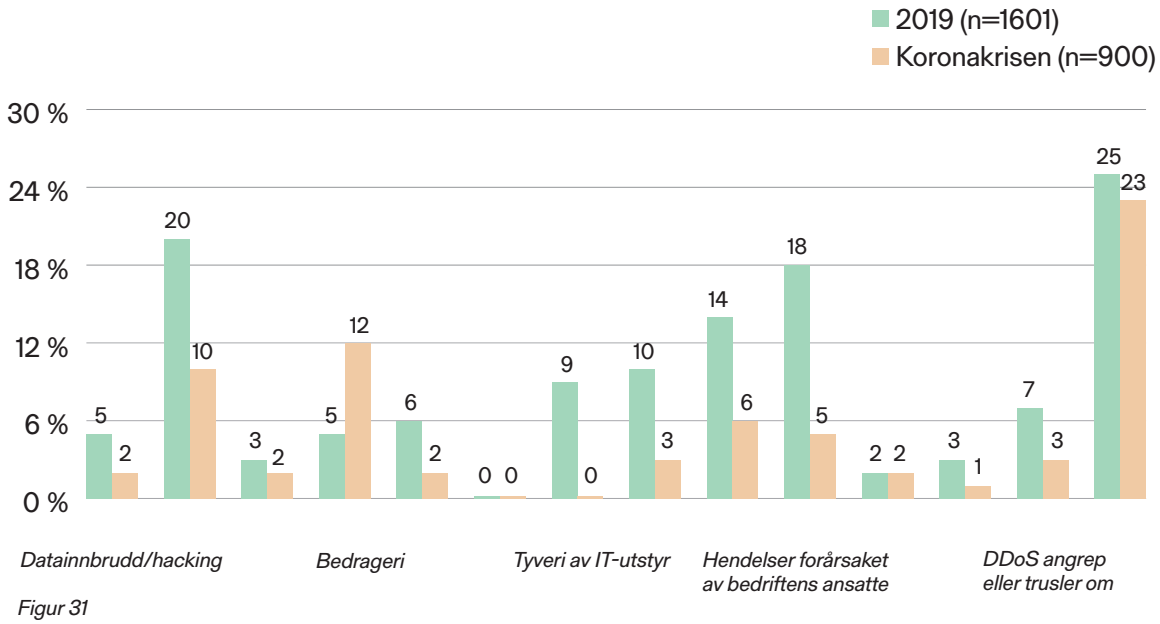
Figur 29

Type hendelser under koronakrisen vs. hele 2019 (Alle bedrifter)



Figur 30

Type hendelser under koronakrisen vs. hele 2019 (Virksomheter med 100 ansatte eller flere)

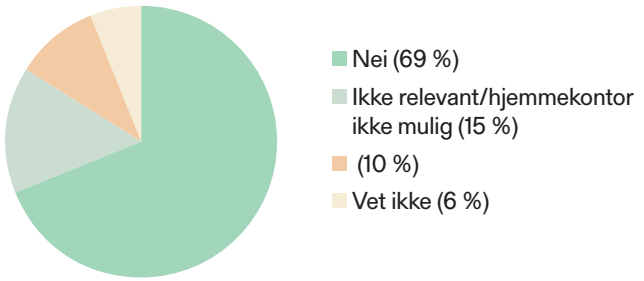


Figur 31

Svekket sikkerhet ved bruk av hjemmekontor?

En av ti opplever svekket sikkerhet

10 prosent opplever at økt bruk at hjemmekontor under koronakrisen har bidratt til å svekke it-sikkerheten. Det er imidlertid 15 prosent av virksomhetene der hjemmekontor ikke er mulig. Ser vi fordelingen uten disse virksomhetene, er det 12 prosent som opplever at økt bruk av hjemmekontor har bidratt til svekket sikkerhet.



Figur 32

Samtidig er det 69 prosent som ikke har opplevd svekket sikkerhet. Ser vi bort fra virksomheter som ikke har mulighet til å ha hjemmekontor, er det 81 prosent som ikke har opplevd svekket sikkerhet.

Virksomheter i alle størrelsesgrupper opplever dette i like stor grad. Når det gjelder bransje er det i størst grad offentlig administrasjon og undervisning der man har opplevd svekket it-sikkerhet. Henholdsvis 28 og 24 prosent av virksomhetene i disse bransjene har opplevd svekket sikkerhet .

6.

Analyse

Skrevet av:
Professor Harald Øverby,
førsteamanuensis Lasse Øverlier,
professor Katrin Franke,
og doktorgradsstipendiat Livinus Obiora Nweke

6.1 Styringssystem for informasjonssikkerhet

Det er fortsatt en økning i antall virksomheter som har et rammeverk eller et styringssystem for informasjonssikkerhet, hvor 69% av virksomhetene har implementert dette i 2020. Styringssystem for informasjonssikkerhet er fortsatt mest vanlig i større virksomheter. Dette er normalt, siden større virksomheter generelt er avhengige av interne styringssystemer for å operere. Det er derfor overraskende at så mange som 14% av de større virksomhetene (flere enn 100 ansatte) fortsatt ikke har et styringssystem eller rammeverk for informasjonssikkerhet. Dette på tross av tydelige anbefalinger fra både NSMs Grunnprinsipper for IKT-sikkerhet og standarder som ISO27001, NIST Cybersecurity Framework og ITIL. I tillegg er alle virksomheter som behandler personopplysninger etter personvernregelverk pliktige til å ha et styringssystem for informasjonssikkerhet.

En markert tendens blant respondentene til Mørketallsundersøkelsen er at små virksomheter har mindre kontroll på sine data enn større virksomheter. Andelen virksomheter som rapporterer om kontroll på sine data er nokså lik med andelen som benytter et rammeverk eller styringssystem for informasjonssikkerhet.

Videre indikerer Mørketallsundersøkelsen en stagnasjon i internasjonal outsourcing av IT-drift. Årsaken til denne stagnasjonen er trolig sammensatt, men kan forklares gjennom: innføringen av personvernregelverket og økt bevissthet omkring teknisk og juridisk tilgang til data og informasjon, gjentagende negativ medieoppmerksomhet knyttet til hendelser, og uheldige situasjoner i forbindelse med internasjonal outsourcing. Kanskje mer konkurransedyktige leverandører av skytjenester innenlands også kan ha bidratt til dette. En kuriositet er at virksomheter med intern IT-organisering i markert lavere grad (62%) involverer virksomhetens ledelse i sikkerhetshendelser sammenlignet med de som helt (70%) eller delvis (73%) outsourcer driften av IT-tjenestene.

6.2 Personvernforordningen (General Data Privacy Regulation - GDPR)

Innføringen av personvernregelverket i 2018 har for de fleste virksomheter i Norge medført endringer i form av økt regulatorisk fokus på personvern. Et av personvernprinsippene omhandler nettopp informasjonssikkerhet. Det har vært antatt at dette også ville kunne ha en positiv effekt på arbeidet med informasjonssikkerhet i norske virksomheter, og 84% av respondentene i Mørketallsundersøkelsen sier at de har gjort endringer eller forbedringer i arbeidet med personvern og informasjonssikkerhet.

I gjennomsnitt har 10% av de forespurte virksomhetene opplevd brudd på personopplysningsloven. Forskjellene mellom privat og offentlig sektor er store: Kun seks prosent av private virksomheter opplever brudd på personopplysningsloven, mens 16% av offentlige virksomheter rapporterer om det samme. En årsak til dette kan være at offentlige virksomheter i snitt er større enn de private virksomhetene. Brudd på personopplysningsloven ser også ut til å være mindre vanlig for de virksomhetene som har et styringssystem for informasjonssikkerhet.

6.3 Sikkerhetshendelser

14% av virksomhetene rapporterer at de har hatt informasjonssikkerhetshendelser som har medført økonomisk tap eller svekket markedsposisjon. Dette vurderes som et lavt tall og kan indikere at informasjonssikkerhetsarbeidet i virksomhetene generelt er bra eller at omfanget av angrep er beskjedent.

De tre mest vanlige sikkerhetshendelsene i 2020 hadde—for en gitt virksomhet—en frekvens på 14% (forsøk på datainnbrudd/hacking), 13% (phishing eller andre typer sosial manipulering), og 11% (virus og/eller malwareinfeksjon). Disse tallene er overraskende lave; rundt 1 av 7 virksomheter opplevde forsøk på datainnbrudd eller hacking, og rundt 1 av 9 virksomheter opplevde virus og/eller malwareinfeksjon. En årsak til dette kan være at antallet hendelser er generelt lavt eller at systemene for å forhindre slike hendelser er svært gode. Det kan også være underrapportering av hendelser eller mangel på oversikt over hendelser i virksomheten. De store virksomhetene (flere enn 100 ansatte) rapporterer 3.62 sikkerhetshendelser for 2020. Dette tallet vurderes også som ganske lavt.

Fra undersøkelsen i 2018 til 2020 har antallet som rapporterer om hendelser knyttet til virus og/eller malware gått ned fra 21% til 11%. Dette kan være en indikasjon på færre nye virus og/eller malware eller at beskyttelsen mot slike typer angrep—for eksempel anti-virus programvare—har blitt forbedret de siste to årene. Men, tilsvarende undersøkelser i utlandet fra Mandiant[1)] og SANS[2)] rapporterer om at kun 9% av angrepene gir alarmer og at 68% av ransomware forblir uoppdaget. Vi må derfor anta at det høyst sannsynlig foregår et betydelig antall uoppdagede angrep mot norske virksomheter.

6.4 Sikkerhetsbrudd

Det fremkommer fra undersøkelsen at 42% av sikkerhetsbrudd oppdages ved en tilfeldighet og 44% oppdages av rutinemessig intern sikkerhetsovervåkning. At så mange av sikkerhetsbruddene oppdages ved ren tilfeldighet vurderes som urovekkende. Dette er en enda tydeligere tendens i små virksomheter (52%). Systematisk arbeid med informasjonssikkerhet i tillegg til rammeverk og gode rutiner burde kunne bidra til at sikkerhetsbrudd fanges opp i større grad. Resultatet fra undersøkelsen viser likevel at sikkerhetsbrudd kan være svært varierte og vanskelig å fange opp av et sikkerhetssystem. De virksomhetene som har et styringssystem for informasjonssikkerhet, opplever at færre sikkerhetsbrudd oppdages ved en tilfeldighet. Tallene er 38% for de virksomhetene som har styringssystem og 59% for de virksomhetene som ikke har styringssystem.

Gitt den høye andelen av sikkerhetsbrudd som oppdages ved en tilfeldighet kan det stilles spørsmål ved om det er korrekt at så mye som 84% av bruddene oppdages innen en dag etter at de oppsto, som indikerer at virksomhetene har gode mekanismer for å oppdage nye forsøk på sikkerhetsbrudd raskt. Også sett opp mot andre rapporter er dette et usedvanlig kort tidsvindu. En undersøkelse[3)] fra IBM i 2019 gjort på amerikanske virksomheter viser at gjennomsnittlig tid for å oppdage et faktisk datainnbrudd er rundt 200 dager med tilhørende kostnader i størrelsesorden titalls-millioner. Når over 80% av respondentene i Mørketallsundersøkelsen rapporterer at innbruddet ikke førte til økonomiske tap, ser vi indikasjoner på stor usikkerhet knyttet til virksomhetenes evne til å avdekke, håndtere og vurdere både kostnadene og konsekvensene av sikkerhetshendelsene på virksomhetsnivå.

1) https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html
2) https://www.domaintools.com/resources/survey-reports/sans-2020-cyber-threat-intelligence-survey
3) https://www.ibm.com/security/data-breach

De fleste av sikkerhetsbruddene i en virksomhet rapporteres internt, enten til selskapets ledelse eller styre. På begge disse punktene er det en positiv utvikling fra 2018, men fortsatt rapporterer under 50% av virksomhetene informasjonssikkerhetshendelser til sitt styre. Mørketallsundersøkelsen viser en vedvarende lav rapporteringsgrad av informasjonssikkerhetshendelser til politi, banker eller andre myndighetsorganer, og reflekterer ikke den økningen i meldinger om avvik i forhold til personvernregelverket som Datatilsynet beskriver i sin årsmelding for 2019. Lav rapporteringsgrad av hendelser til myndighetsorganer er uheldig, særlig på grunn av at rapportering av slike hendelser kan gi verdifull informasjon om pågående angrep eller metoder for å beskytte seg mot pågående angrep. Her ligger det trolig et potensiale for virksomhetene som kanskje ikke er klar over den pågående kraftsamlingen på myndighetssiden. I oppfølgingen av Nasjonal strategi for digital sikkerhet (2019) er både etableringen av nasjonale sentre som NC3 og NCSC og fremhevingen av de sektorielle CERTene signaler på myndighetenes intensjon om å bidra med kapasitet og kompetanse i og mellom sektorer i tråd med internasjonale anbefalinger[4)].

6.5 Covid-19

Tilleggsundersøkelsen som ble gjort tidlig i Covid-19 pandemien (24.mars–8.april) viser ingen signifikant økning i antall rapporterte sikkerhetshendelser under koronakrisen. Men, det er forskjeller mellom bransjene: På den ene siden rapporterer særlig industri, men også helse og sosial, varehandel og tjenesteytende næringer, om en økning i antallet sikkerhetshendelser. Her kan vi anta at blant annet økt bruk av hjemmekontor, stor arbeidsbelastning og kanskje også overføring av personell mellom ulike enheter kan ha skapt utnyttbare sårbarheter. På den andre siden ser vi at for overnattings- og serveringsvirksomheter rapporterer 34% av respondentene om færre sikkerhetshendelser enn tidligere. Dette har sammenheng med nedstengningen av landet, og at de fleste overnattings- og serveringsvirksomheter har stengt sin virksomhet og dermed er mindre aktive på nett.

Når det gjelder hjemmekontor er det vanskelig å konkludere med at denne arbeidsformen i seg selv har ført til svekket informasjonssikkerhet. 7 av 10 respondenter sier at sikkerheten ikke har blitt svekket som følge av hjemmekontor. Situasjonen er likevel noe ulik over type organisasjon: For ansatte i offentlig administrasjon og undervisning rapporterer hhv. 28% og 24% at sikkerheten har blitt svekket. Dette kan ha sammenheng med økt bruk av videokonferanser, fjerntilgang og VPN, utstrakt bruk av mobile enheter og muligens enheter som ikke er administrert av virksomheten. Når det gjelder typer informasjonssikkerhetshendelser tidlig i Covid-19 perioden, så legger vi spesielt merke til bedrageri rettet mot offentlig administrasjon, phishing og andre former for sosial manipulering rettet mot offentlig administrasjon, industri og undervisning, samt virus og/eller malware rettet mot undervisningssektoren. En observasjon er at rapporterte hendelser forårsaket av virksomhetens egne ansatte faktisk ser ut til å være lavere under Covid-19 sammenlignet med normalsituasjonen.

Datatilsynet har, i denne perioden, hatt en økning av rapportering av brudd på personopplysningssikkerheten relatert til phishing og spear phishing.

4) https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le

OPPSUMMERT

- Mørketallsundersøkelsen 2020 viser en generelt positiv utvikling i Norske virksomheters systematiske arbeid med informasjonssikkerhet siden forrige undersøkelse.

- Mørketallsundersøkelsen 2020 indikerer at de fleste virksomheter har implementert personvernforordningen, og virksomhetene rapporterer — i forhold til det store volum av personopplysninger som forvaltes — generelt få brudd på forordningen som ble innført i 2018.

- Mørketallsundersøkelsen 2020 viser at en skremmende stor andel av informasjonssikkerhetshendelsene fortsatt avdekkes ved en tilfeldighet.

- Mørketallsundersøkelsen 2020 dokumenterer en relativt beskjeden effekt på rapporterte informasjonssikkerhetshendelser i kjølvannet av Covid-19, men med noen sektorer som skiller seg ut. Mellom 33 prosent (offentlig administrasjon) og 41 prosent (undervisning) innen offentlig administrasjon, helse og undervisning oppgir at de oppdaget sikkerhetsbrudd ved en tilfeldighet. Når i overkant av en tredjedel av offentlige virksomheter oppdager sikkerhetsbrudd ved en tilfeldighet, kan man stille spørsmål ved hvor effektiv etterlevelsen av rammeverk for informasjonssikkerhet er i praksis, samt hvilken effekt mangel på eksisterende prosesser eller etterlevelse av rutiner har på sikkerhetsarbeidet.

7.

Risikobildet/ trender

7.1 Nasjonalt cybersikkerhetssenter – NSM

COVID-19 situasjonen har påvirket det digitale domenet gjennom 2020 på flere områder. Nasjonal sikkerhetsmyndighet (NSM) ved Nasjonalt cybersikkerhetssenter (NCSC) erfarte at ulike aktører utnytter et mulighetsrom som oppstår i det digitale rom knyttet til svindelforsøk og digitale operasjoner på nett med COVID-19 tematikk. Økte sårbarhetsflater og sikkerhetshull knyttet til utstrakt bruk av midlertidige hjemmekontorløsninger, som utnyttelse av sårbarheter i fjernaksessløsninger, førte til behov for økt årvåkenhet og bevisstgjøring rundt IKT-sikkerhet. NCSC har utgitt flere varsler, råd og tiltak knyttet til COVID-19 situasjonen på våre hjemmesider gjennom 2020.

COVID-19 situasjonen har likevel ikke endret hovedlinjene i det digitale risikobildet mot Norge. NCSC opplever et jevnt trykk av digitale operasjoner mot norske mål, inkludert virksomheter som ivaretar viktige samfunnsfunksjoner. Aktivitetsnivået som er observert gjennom 2020 samsvarer i hovedsak med normalbildet i det digitale rom. Både statstilknyttede og kriminelle aktører utfører digitale operasjoner mot norske mål.

NSM vurderer at statsforvaltningen og en rekke sektorer i Norge er utsatt for digitale operasjoner, blant annet virksomheter innen sektorene forsvar, rom, maritim, petroleum og kraft er risikoutsatt. Det samme bildet gjelder for miljøer innen samferdsel, forskning og høyere utdanning, ekom og helse.

Aktørene utfører rekognosering og informasjonsinnhenting mot mål i Norge, men også andre typer digitale operasjoner. Virksomheter utsettes for eksempel for utpressingsforsøk ved bruk av løsepengevirus, der aktører lammer digitale systemer og krever løsepenger for å låse opp krypteringen. I mange tilfeller er løsepengevirusangrep utført av aktører med høy digital kompetanse, på eget initiativ eller på oppdrag fra andre.

Under COVID-19 så NCSC en økning i rapportering av løsepengevirus mot norske virksomheter, noe som delvis kunne skyldes at omfanget av internetteksponerte tjenester var høyere grunnet utstrakt bruk av hjemmekontorløsninger. Økningen kan også skyldes at verktøy og metoder aktørene benytter er i stadig utvikling. NCSC forventer en fortsatt økning i løsepengevirus mot norske virksomheter i tiden fremover.

Svindelforsøk i form av direktørsvindel, datainnbrudd og misbruk av infrastruktur til utvinning av kryptovaluta rammer også mange norske virksomheter. I tillegg er det tilfeller hvor intetanende norske virksomheter blir kompromittert og brukt som en del av komplekse infrastrukturer i operasjoner mot mål i andre land.

Programvare- og tjenesteleverandører kan utnyttes av trusselaktører for å få innpass i systemene til selskapets kunder. NSM observerer også 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.

Metoder og verktøy som brukes for å komme inn i norske virksomheter er i stadig utvikling, men utviklingstrekkene er i stor grad gjenkjennbare. Trusselaktørene benytter kjente sårbarheter for å trenge inn i systemer og nettverk, ofte via internetteksponerte tjenester hos virksomheten. Bred kartlegging av sårbarheter og innsamling av åpen informasjon om en virksomhet og deres ansatte kan benyttes for å skreddersy e-poster som brukes i målrettede operasjoner mot virksomheten. Denne informasjonen kan benyttes for å skaffe påloggingsdetaljer via målrettede e-post-kampanjer som deretter utnyttes til å få tilgang til systemene.

Omfanget av operative hendelser håndtert hos NCSC i samarbeid med virksomheter som rammes spenner bredt i type aktivitet og alvorlighetsgrad. NCSC har gjort seg flere erfaringer fra hendelseshåndtering i 2020. Sakene er ofte komplekse, hvor håndtering krever mye ressurser.

Norske virksomheter blir mer sikkerhetsbevisste – de identifiserer tiltak og iverksetter disse i større grad. Likevel, i møte med virksomheter der NCSC bistår i hendelseshåndtering er det ofte gjentakende utfordringer som gjør håndteringen tidkrevende og komplisert. NCSCs oppfatning er at visse risikoreduserende tiltak mangler delvis eller helt hos enkelte virksomheter.

En helhetlig tilnærming til sikkerhetsnivået inkluderer både prosessuelle, organisatoriske og tekniske tiltak. NSM mener at et bevisst forhold til sikkerhet og sikkerhetskultur på tvers av disse ulike grupperingene kan redusere sikkerhetsrisikoen. Dette bør gjelde for alle virksomheter, også de mindre. Norske virksomheter må bli mer robuste i møte med uønskede digitale hendelser. Enkle grep nytter og kan stoppe de aller fleste dataangrep, slik som NSMs Grunnprinsipper for IKT-sikkerhet[5]. NSMs Grunnprinsipper versjon 2.0. ble lansert i 2020 for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Dette er viktig for å ivareta god grunnsikring av digitale verdier og vil igjen føre til redusert skadeomfang dersom en hendelse inntreffer.

7.2 Nasjonalt Cyberkrimsenter - Kripos

Gjerningspersoner som begår IKT-kriminalitet, skiller seg ikke nevneverdig ut fra andre kriminelle i den forstand at de har en tendens til å operere etter en metode inntil den ikke fungerer lengre. En følge av dette er at kriminalitetsbildet i 2019 og inn i 2020 i det digitale domenet er preget av kjente fenomener som drives etter kjente metoder. De forebyggende tiltakene for å begrense sannsynligheten for å bli et offer er i all hovedsak de samme som før.

IKT-kriminalitet er et internasjonalt problem hvor gjerningspersonene med enkelhet kan operere på tvers av kontinenter og landegrenser. Organiserte kriminelle har tilegnet seg kapabiliteter og kapasiteter som tidligere var forbeholdt statlige og statssponsede aktører. Trusselen denne type kriminalitet representerer overfor samfunnet er høy og konstant.

Politiet vil trekke frem to fenomener som særlig representerer en trussel for norske virksomheter. Løsepengevirus trekkes frem som den største digitale trusselen mot norske virksomheter etterfulgt av bedragerier hvor kriminelle endrer betalingsdetaljer. Betalingsdetaljene endres etter at de kriminelle har tilegnet seg informasjon gjennom uautorisert tilgang til datasystemer eller sosial manipulasjon.

Løsepengevirus er en skadevare som krypterer fornærmedes datasystemer etterfulgt av krav om penger for å utlevere en digitalnøkkel som benyttes for å dekryptere systemet. Størrelsen på betalingskravet er ofte tilpasset fornærmedes antatte betalingsevne. Løsepengene kreves betalt i kryptovaluta for at selve transaksjonen skal være motstandsdyktig mot sporing.

Løsepengevirus representerer en vedvarende trussel, og det er et høyt antall virksomheter på verdensbasis som blir rammet. Utviklingen går i retning av at kriminalitetsformen gir større utbytte til gjerningspersonene i tillegg til at den påfører fornærmede større økonomisk skade enn tidligere. De økonomiske skadene opp-

5) https://www.nsm.stat.no/globalassets/dokumenter/grunnprinsipper-for-ikt-sikkerhet-2.0/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

står i form av tapt produksjonstid og kostnader til gjenopprettelse av datasystemer. Virksomheter som utsettes for denne type kriminalitet spenner over alt fra globale selskaper til små og mellomstore bedrifter.

Det er kjent at noen aktører primært opererer som tilbydere av løsepengevirus som en tjeneste, på engelsk ransomware as a service (RaaS). Disse aktørene må nødvendigvis ha meget høy IT-kompetanse, både for å utvikle funksjonell programvare, ivareta anonymisering og annen operasjonell sikkerhet. Slike aktører utvikler og oppdaterer selve programvaren som benyttes, for så å selge den som en tjeneste til en affiliert aktør som velger ut hvilke mål de ønsker å rette løsepengeviruset mot. Fortjenesten fra slike løsepengevirusoperasjoner fordeles mellom aktørene.

I tillegg ser vi den siste tiden at flere og flere ulike løsepengevirusaktører, lekker informasjon om hendelser med trussel om å auksjonere bort stjålne data fra de rammede bedriftene om løsepenger ikke utbetales. Dette viser en utvikling i retning av mer avanserte flerstadie-hendelser. Det innebærer at aktøren ikke kun låser bedriftens systemer, men også først tar kontroll over og penetrer dypt i nettverket for å sikre seg mest mulig av bedriftens potensielt verdifulle og/eller sensitive data. Denne modusen virker å være benyttet for å legge ytterligere press på bedriften til å betale, samt øke den potensielle inntjeningen ved å kunne selge stjålet data til det høyeste budet.

Bedragerier foranlediget av at gjerningspersonene får endret fakturaopplysninger og deretter tilegner seg et økonomisk utbytte representerer en stor trussel mot næringslivet. Dette er en form for kriminalitet som rammer alt fra små lokale virksomheter til store internasjonale selskaper.

I sin simpleste form påvirker de kriminelle virksomhetens medarbeidere pr telefon eller epost til å endre betalingsdetaljer gjennom sosial manipulasjon. I de mer teknisk avanserte tilfellene tilegner de kriminelle seg uautorisert adgang til datasystemer og epostkontoer for å skaffe informasjon som benyttes til å utføre bedrageriene. Det er avdekket saker hvor gjerningspersonene har hatt adgang til systemene i flere måneder og implementert videresendingsregler i epostkontoer som medfører at de får tilsendt sensitiv informasjon som benyttes til å utføre bedrageriene. Politiet er kjent med saker hvor utbyttet fra bedrageriet varierer fra noen tusen til 150 millioner kroner. Phishing eposter med skadevare eller med lenker til sider hvor fornærmede blir lurt til å gi fra seg påloggingsdetaljer er den mest utbredte metoden for å få uautorisert aksess til virksomheters datasystemer. Trusselen fra phishing eposter er konstant.

Videre ser politiet at kjente sårbarheter i datasystemer ofte blir utnyttet til kriminelle formål. Dette er sårbarheter det finnes oppdateringer til som ville ha eliminert sikkerhetshullene. En av de mest rapporterte sårbarhetene som utnyttes i dag er den samme som ble brukt i forbindelse med WannaCry kampanjen. Det ble lansert en oppdatering for å fjerne sårbarheten i 2017.

Det er kjent at det eksisterer databaser som inneholder brukernavn og passord som er stjålet i forbindelse med datainnbrudd hos ulike virksomheter. Da mange benytter samme brukernavn og passord på tvers av ulike tjenester kan brukerdetaljer fra slike databaser benyttes av kriminelle til å skaffe seg uautorisert adgang til virksomheters datasystemer.

Til slutt vil vi trekke frem behovet for skjermede backuper av både system og data. Det kan være avgjørende for at en rammet bedrift vil kunne starte opp igjen rask når man først er rammet av løsepengevirus, uten å måtte betale løsepenger.

Økt bevissthet og varsomhet blant virksomhetenes ansatte relatert til å aktivisere lenker i eposter er viktige forebyggende tiltak for å redusere risikoen for å bli utsatt for digital kriminalitet. Innføring av to-faktor autentisering samt å redusere adgangen til å aktivere videresending av eposter anbefales. Videre er det viktig å sørge for at datasystemene har de siste sikkerhetsoppdateringene samt at virksomhetens ansatte har gode passordrutiner og ikke benytter samme brukernavn og passord på tvers av ulike tjenester.

7.3 Situasjonsbildet fra Nordisk FinansCERT

Avanserte bankranere

Det finnes flere grupperinger internasjonalt som benytter målrettede dataangrep for å bryte seg inn hos banker og stjele penger. Disse har en viss suksess – men så langt ikke i Norden. Vi ser en liten håndfull slike aktører som jevnlig prøver seg også i Norge, uten at de har lykkes i 2019.

Løsepengevirus

Saker som Hydro-saken (et målrettet løsepengevirus-angrep) har hatt stort fokus også i finansnæringen i 2019. Trusselen oppleves som stor, og næringen jobber aktivt med tiltak som reduserer muligheten for innbrudd, samtidig som man er forberedt på å måtte reetablere raskt ved et angrep. Det var én slik hendelse i finansnæringen høsten 2019, der virksomheten raskt valgte å reetablere fra backup.

Utilsiktet eksponering av data

I 2019 var det flere hendelser som gjaldt utilsiktet eksponering av data. I de fleste tilfellene involverte disse hendelsene skylagring, 3.partsleverandører og elementer av menneskelige feil.

Nettbank og betalingssvindel

Antall falske nettsteder som forsøker å stjele informasjon om BankID eller kredittkort som NFCERT håndterte doblet seg fra 2018 til 2019. Sidene utgir seg typisk for å være banken, Vipps, Nets eller andre kjente merkevarer som Netflix og Apple. Ofrene mottar epost eller SMS med lenke til fiske-nettstedet. Påloggingsinformasjonen som blir fisket blir brukt umiddelbart til å logge seg inn i Nettbank og gjennomføre betaling. Dette lykkes i liten grad.

De klassiske banktrojanerne så vi lite til - kun «Retefe» var litt aktiv i Norge i april/mai før aktøren gikk til andre markeder.

Stjeling av Office365-pålogging

I begynnelsen av 2020 har det vært en økning av fisking som er mer målrettet mot bedrifter i Norge. Ved å sende eposter, eller dele lenker på annet vis – f.eks. via LinkedIn - fisker de påloggingsinformasjon til Office365. Med tilgang vil angriperne kunne lese og sende epost, og kan sørge for at de får tilsendt kopi av viktig epost. Det er sett tilfeller der slik tilgang senere brukes til å manipulere bedriften til å sende penger til svindlerne i stedet for til sine partnere, eller til å sende ut endring på fakturaer med nytt mottakernummer.

Også virksomhetene i finansnæringen er utsatt for slik fisking. Virksomhetene har fokus på det og har raskt oppdaget og håndtert slike hendelser. Vi kjenner ikke til noen vellykkede angrep i vår sektor der informasjon eller penger har blitt stjålet.

Vishing (Voice Phishing)

Lokale kriminelle som ringer og utgir seg for å være f.eks. banken traff Norge høsten 2019. Dette har i flere år vært et stort problem i Europa og Norden. I Norge ble fenomenet kjent som «Olga-Svindel». Ofrene blir lurt til å gi fra seg BankID påloggingsinformasjon til svindlerne, som så forsyner seg med pengene de har stående i banken. Tett samarbeid mellom bankene og politi førte til arrestasjoner i 2019, og fenomenet ble borte en periode, men vi har i 2020 sett at det starter opp på nytt.

7.4 Telenor

Password-spraying og credential-stuffing

"Password-spraying" og "credential stuffing" er to beslektede angrepsformer som stadig blir mer populære blant trusselaktørene. Sammen med phishing, er disse angreps-metodene ofte brukt for å kompromittere både privatbrukere og firmaer.

Passwordspraying innebærer at de kriminelle først får tilgang til en liste med brukere på en tjeneste. Deretter prøver de å logge på med hvert enkelt brukernavn i listen, sammen med et vanlig passord, for eksempel "Qwerty123." Etter å ha prøvd alle disse kombinasjonene prøver de det neste passordet på listen mot alle brukerne. Dersom angriperne har kjennskap til tjenestens passord-policy, tilpasser de passordene de prøver til denne. Det trengs bare at én enkelt ansatt har et svært vanlig passord før bedriften blir kompromittert.

Credential-stuffing er en lignende type angrep, men i stedet for mye brukte passord benytter angriperne seg av tidligere lekkede passord fra kompromitterte tjenester. Siden over halvparten av brukere generelt gjenbruker passord mellom tjenester, lyktes det ofte angriperne å komme inn. Angriperne prøver gjerne passord-kombinasjoner fra hundrevis av servere samtidig og i sakte tempo for ikke å vekke mistanke.

Begge angrepsmetodene beskrevet over fører til at angriperne får tilgang til tjenesten gjennom en ellers lovlig bruker og kan derfor være vanskelig å oppdage, på lik linje med phishing. For å motvirke denne typen angrep er det viktig med to-faktor-autentisering.

Ny løsepenge-taktikk: Dobbel utpressing

Ransomware var svært aktuell også i 2018 da forrige utgave av Mørketallsundersøkelsen ble gitt ut. Flere norske firmaer har blitt rammet, men mest kjent er nok Norsk Hydro. Angriperne kommer seg gjerne inn i nettverket ved hjelp av phishing eller password-spraying som nevnt over. Noen ganger benytter de også svakheter i tjenester som bedriften har eksponert direkte mot Internett. Når angriperne først er på innsiden, benytter de i størst mulig grad vanlige nettverksadministrator-verktøy for rekognosering og spredning i nettet, kjent som "Living-off-the-Land" i cyber-security. Dette gjør at angriperne blir vanskeligere å oppdage.

I de siste månedene har bandene bak denne typen angrep lagt til en ny teknikk som legger enda mer press på rammede bedrifter: Før de krypterer alt de kommer over av servere og klienter, henter de ut mest mulig bedriftssensitive data. Utpresserne truer så med å offentliggjøre disse dataene dersom bedriften ikke betaler løsepenger. I de siste ukene har én kriminell aktør til og med begynt med offentlige auksjoner av dataene!

DDoS-angrep

DDoS-angrep i Telenors nettverk øker stadig i antall, men angrepene rammer i stor grad privatpersoner og utdanningsinstitusjoner. Det har vært en nedgang i trusselbrev der en truer med DDoS-angrep dersom offeret ikke betaler løsepenger. Fortsatt er det såkalte volumetriske angrep som er aller mest vanlig, altså angrep som prøver å fylle opp Internett-forbindelsen med store mengder pakker/trafikk. Angrepene blir gjerne gjennomført ved å reflektere pakker via feilkonfigurerte DNS, LDAP og SSDP-servere.

I mai var det 970 registrerte DDoS-angrep i Telenors nettverk. 136 av disse angrepene var så store at de ble aktivt mitigert. Et typisk angrep var på 1.33Gbps og varte i 25 minutter. Det største angrepet registrert i mai var på 54.5Gbps.

Smishing, vishing og spoofing

Phishing,Smishing og Vishing er alle varianter av samme type svindel. Det som skiller de fra hverandre er plattformen eller metoden svindlerne benytter for å få offeret på kroken. Fellesnevneren for disse svindelmetodene er at de alle benytter seg av sosial manipulasjon. Det betyr at svindlerne spiller på våre grunnleggende følelser som fristelser, frykt, tillit og opplevelsen av følt tidspress for å komme inn på oss, og få oss til å handle irrasjonelt.

Formålet med disse svindelmetodene er å fiske ut informasjon fra offeret, gjerne i form av kredittkortinformasjon eller annen personsensitiv informasjon.

Smishing, eller "SMS phishing" er SMS-meldinger, gjerne med linker til nettsteder som svindlerne har kontroll over. Avsender-nummeret/navnet er gjerne forfalsket/spoofet til å være et navn eller merkevare som mottaker kjenner og som dermed skal vekke tillit hos mottaker.

Vishing, eller "Voice phishing" er en annen variant der svindlerne bruker telefoni/tale til å svindle offeret. Det finnes flere varianter av denne svindeltypen, alt fra de helt enkle der svindleren ringer med skjult nummer og utgir seg fra å være en annen enn den de er, til de mer avanserte der man benytter seg av spoofing.

Spoofing (manipulering av nummeret som ringer opp) er noe som har økt i omfang de siste årene, spesielt i forbindelse med såkalt «Microsoft-svindel», der vilkårlige, norske mobilnummer brukes som oppringningsnummer for å få folk til å svare telefonen, siden folk har blitt mer skeptiske til å svare anrop fra utenlandske eller skjulte nummer. Teknikken bruker også i mer målrettede svindelforsøk der svindlerne bruker nummer som tilhører for eksempel norske banker og ringer utvalgte kunder, også kjent som "Olga-svindel".

Daglig blokkerer Telenors Fraud & Crime-avdeling flere hundre tusen svindelanrop. Dette inkluderer både Wangiri-anrop og spoofede samtaler fra utlandet, typisk falske support-anrop.

8.

Erfaringer

8.1 Erfaringer fra Telenor

Myndighetene i Norge gir vesentlig innsikt i forhold som påvirker oss. I årets vurderinger fra myndighetene legger vi spesielt merke til følgende:

«Trusselbildet Norge står overfor ved overgangen til 2020 er et resultat av strukturelle endringer som har pågått over mange år» (Kilde: Etterretningstjenestens trusselvurdering FOKUS 2020.) «Trusselbildet vil i stor grad være uendret fra 2019. Utenlandske etterretningstjenester forventes i 2020 å rette sin spionasje mot politiske myndigheter, mot naturressurser og næringsliv, mot forsvar og beredskap, samt mot forskning og utvikling.» (Kilde: PST trusselvurdering 2020.)

På bakgrunn av blant annet PSTs og Etterretningstjenestens trusselvurderinger erkjenner vi at vi er et mål for avanserte aktører. Både på grunn av vår rolle i Totalforsvaret, vår samfunnskritiske infrastruktur, vår nasjonale symbolverdi og våre kunder i alle bransjer og sektorer. Denne kunnskapen sett i sammenheng med myndighetenes vurderinger, legger vi til grunn i våre risikovurderinger.

8.2 Erfaringer fra Coop

Coop erfarer på generell basis en nedgang i antall sikkerhetshendelser. På den annen side er hendelsene som inntreffer stadig mer målrettet og sofistikert, og øker i kompleksitet. Hva gjør dette / fører det til?

Svindel

Coop, i likhet med mange andre virksomheter, har i en årrekke opplevd at merkenavn blir misbrukt i svindelkampanjer. Disse distribueres via e-post, SMS og falske annonser i sosiale medier. Svindelkampanjene er ofte rettet mot kunder, uavhengig av deres kundeforhold, der svindelaktørene har som formål å sanke inn personopplysninger og lure til seg penger, for eksempel gjennom dyre abonnementsløsninger.

Coop sin sikkerhetsgruppe har aktivt jobbet for å kunne håndtere svindelforsøk, og har utarbeidet interne rutiner for å oppdage og håndtere svindelsaker. I tillegg har Coop inngått samarbeid med flere store teleoperatører, for å kunne stanse SMS-kampanjer. Dette har gitt gode resultater, noe som understreker hvor viktig åpenhet og samarbeid er i kampen for å bekjempe nettkriminalitet.

Phishing

Coop merker en kraftig økning i mottak av phishing e-poster, spesielt parallelt med en satsing på diverse skytjenester. Spesielt observeres forsøk på spear phishing. Det betyr at kunder mottar en tilsynelatende legitim e-post, med et innhold som refererer til Coop. Deretter sendes mottaker til en falsk påloggingsside, der Coops logo og visningsnavn er forfalsket. I tillegg har Coop sett flere eksempler hvor legitime, men kompromitterte e-postkontoer benyttes til å sende ut phishing-kampanjer det siste året. Svindelaktørene forsøker også i større grad å angripe autentiseringsmekanismene i skytjenestene, da slike tjenester ligger tilgjengelig for alle med tilgang til internett.

Coop vil med dette påpeke viktigheten av å sette opp multifaktor autentisering for alle skytjenester. Det er ikke bare de store skyteknologi leverandørene som leverer skytjenester. Det finnes også mange SMB-er som er leverandører av skytjenester, og det uten å nødvendigvis ha sikkerhetsmodenheten på plass. Kunder som satser på funksjonelle løsninger i skyen, tenker ikke nødvendigvis på sikkerhetsmekanismer rundt løsningen, og stoler fullt og helt på leverandøren/samarbeidspartner.

Vi anbefaler at man har med sikkerhetskrav til leverandører allerede i anskaffelsesprosessen, og at man velger leverandører som har en tilfredsstillende grad av sikkerhetsmodenhet og ikke bare har fokus på funksjonelle krav. Still derfor relevante sikkerhetskrav til leverandørene, og kontroller at leverandøren faktisk etterlever de avtalte kravene.

Direktørsvindel

Coop ser en betydelig reduksjon på antallet forsøk på direktørsvindel, dog er det nye forsøk innimellom. De kriminelle benytter ulike fremgangsmåter i forsøk på å lure til seg store økonomiske verdier. En variant er der de kriminelle utgir seg for å være en beslutningstaker i organisasjonen. Typisk tar de kontakt med HR eller lønningsavdelingen om at vedkommende har byttet bank, og ber om at utbetaling av lønn må overføres til et nytt lønnskontonummer. For å unngå denne type svindel, er det viktig at virksomhetene utarbeider gode rutiner for og kontroll over utbetalinger.

Avslutningsvis ønsker Coop å oppfordre private virksomheter til å bruke Politiets næringslivskontakter så mye som mulig. De er en meget god kanal for å dele informasjon og kunnskap, som bør brukes for alt det er verdt. Vi i Coop har et godt samarbeid med våre kontakter, og anbefaler dette også for andre. Et tett samarbeid med myndigheter og næringsliv er uten tvil en viktig faktor for å vinne kampen mot nettkriminalitet.

Foto: Unsplash

8.3 Erfaringer fra Visma

Visma er begeistret for Mørketallsundersøkelsen og mener den er svært viktig for virksomheter. Vismas klare anbefaling er å analysere den i egen kontekst, og iverksette de tiltak man finner nødvendig for å forbedre egen sikkerhet. Visma anbefaler videre også å gjøre samme øvelse med de viktige trusselvurderingene fra politi og forsvar, og bruke erfaringer fra hendelser som deles i offentligheten for å lære.

Årets Mørketallsundersøkelse har, etter hva Visma erfarer, et skremmende resultat, og dette gjelder det svært høye antallet respondenter som svarer et tydelig NEI til at de har hatt sikkerhetsmessige hendelser i 2019, sammen med at et urovekkende stort antall respondenter svarte NEI på at de har opplevd forsøk på cyber-relaterte angrep. Våre data indikerer at enhver "internet exposed service" blir angrepet hver eneste dag, og flere av disse angrepene er såpass sofistikerte at de bør etterforskes og rapporteres videre i form av anmeldelser til politi. De mest nyanserte analysene viser et antall angrep på mellom 6-8 som er såpass avanserte at det er verdt å adressere de på månedlig basis. Om bevisstheten om disse angrepene blir mer utbredt i samfunnet, bør derfor antallet som svarer NEI på de cyber relaterte hendelsene reduseres til 0 i løpet av noen år. Utfordringen vi opplever er at det ikke alltid er enkelt å oppdage angrepene og skille trusselaktørene fra hverandre. De aller fleste angrepsforsøkene mislykkes og det er derfor lett å konkludere med "ingen skade skjedd, la oss gå videre". Vi analyser peker i retning av at de menneskene som håndterer denne informasjonen i virksomheten ikke avkreves slike svar fra sin ledelse. Derfor er det ikke rimelig å anta at dette vil forandres stort uten medvirkning fra ledelsen i virksomhetene. Vi samarbeider godt med politiet og vil fremheve betydningen av næringslivskontaktene idstriktene. Disse har vært en svært viktig rolle i å bevisstgjøre Visma, og har gjort det mye enklere å samarbeide med politiet de gangene det har vært slike behov. Visma ser ikke den samme evnen og viljen til samarbeide i alle land hvor vi er etablert i og anbefaler alle medlemmer i NSR å søke tettere og bedre samarbeid med sin lokale næringslivskontakt. For oss som næringslivsaktør fremstår pr i dag norsk politi som et eksempel til etterfølgelse for sine søsken i andre land, og vi håper disse vil få samme modning i samarbeidet med næringslivet i årene framover.

Vi har også observert en endring i nasjonalstatsaktørenes handlemønster under Covid-19. Med dette mener Visma nasjonale overvåkningsaktører, som samler informasjon fra andre land. Det er ikke Vismas oppfatning at situasjonen i Norge har endret seg radikalt under Covid-19, men det globale bildet ser ut til å ha endret seg noe. I våre systemer observeres det at aktører som normalt sett er svært lite eksponerte har blitt synlige under Covid-19. Dette er aktører som anses som aktive primært under kriser/krig i enkeltland. Disse aktørene, som kommer fra svært mange land, ser ut til å bruke eksotiske virkemidler som sjelden er sett i det åpne tidligere. Vismas analyser bekrefter stort sett de åpne trusselvurderingene fra myndigheter i våre markeder i Europa.

Hjemmekontorfunnene bekreftes i liten grad i våre interne undersøkelser. Det virker som de fleste ansatte er tilfredse og opplever at deres arbeidshverdag og produktivitet har økt som følge av endringene. Vi har gjennom flere år investert i dette feltet og opplevde få, om noen utfordringer ved overgangen til hjemmekontor. Vi gikk fra 184 lokasjoner til 11000 over natten og har klart denne operasjonen uten større utfordringer. Sikkerhetsmessig, er dette hva vi er designet for, og hjemmekontoret/den distribuerte arbeidsplass har vært en integrert del av beredskaps- og kriseplanene i mange år. Vismas råd til andre virksomheter er å bruke denne Covid-19 mulighet til å skape digitale arbeidsflater som ikke er avhengige av fysiske lokasjoner i samme grad som tidligere. Et større fokus på sikring av applikasjonene og tilhørende data er en fremtidssikring og bør inn i kriseplaner og beredskapsplaner for flere. Et sterkt fokus på nettverkssikring og sikring av bygningsmasse kan fremstå som kontraproduktivt om en ikke av særskilte årsaker MÅ gjøre det for å få virksomheten til å fungere.

8.4 Erfaringer fra Atea

Atea ønsker å anerkjenne jobben Næringslivets Sikkerhetsråd gjør i det norske samfunnet. Med alle foreninger, stiftelser, tilsyn og myndigheter som konkurrerer om rådgiverposisjonen for norske virksomheter, er det fint å ha en tilnærmet uhildet organisasjon som norske virksomheter, uavhengig av størrelse, kan snu seg til for å få gode råd.

Atea er aktiv sparringspartner med flere virksomheter og organisasjoner, både private og offentlige, eksempelvis NSR og NSM. Som godkjent hendelseshåndterer av Nasjonal Sikkerhetsmyndighet, ser vårt Incident Response Team det samme mønsteret som Mørketallsundersøkelsen viser. Når «menneskelig feil» og «tilfeldighet/uflaks» er den vanligste årsaken til at et sikkerhetsbrudd oppstår og/eller blir oppdaget, så er det et tydelig behov for å forbedre rammeverket for informasjonssikkerhet i norske virksomheter. Derfor var Nasjonal Sikkerhetsmyndighets Grunnprinsipper versjon 2.0 hovedtema og årets røde tråd under Ateas Sikkerhetsdager 2020. Siden det ikke finnes noen egne lover og regler for IT-sikkerhet som treffer alle norske virksomheter, oppfordrer vi alle virksomheter til å følge Grunnprinsippene.

Atea har siden 2014 kjørt over 80 sikkerhetsdager, som er en opplysningskampanje som tar for seg gjeldende samtids trusselbilde. I tillegg har vi tilbudt kundene våre gratis sikkerhetskurs under sikkerhetsmåneden oktober, men anbefaler selvfølgelig at virksomheter kjører bevisstgjøringsprogrammer kontinuerlig gjennom hele året.

Videre stiller Atea seg i rekken med NSM og NorSIS som anbefaler at virksomheter som ikke har kompetanse og ressurser til å håndtere egen IT-sikkerhet, outsourcer dette til en kommersiell aktør som er spesialisert på IT-sikkerhet. Men vi ønsker å være tydelige på at det å outsource IT-driften sin, ikke fritar virksomheten for ansvar. Det er avgjørende å stille tydelige og konkrete krav til sin driftsleverandør, spesielt når det kommer til IT-sikkerhet. Dette er noe vi som driftsleverandør håper å se mer av i tiden fremover.

Mørketallsundersøkelsen viser at det kun er 34 prosent av de som har opplevd brudd på personvernsloven som har rapportert dette til Datatilsynet, dermed er det en stor andel av virksomhetene som ikke har rapportert inn bruddet. Atea og våre hendelseshåndterere er klare på at alle brudd på personopplysningssikkerheten skal rapporteres inn, og vi stiller oss undrende til hvorfor dette ikke blir gjort. Om virksomheten ikke har satt seg inn i hvordan dette gjøres, følelsen av maktesløshet, at man har vært naive, om det kan skade fremtidig butikk og rykte vet vi ikke, men Ateas hendelseshåndterere har hørt alle variablene opp til flere ganger.

I følge Statistisk Sentralbyrå er det registrert ca. 590.000 norske virksomheter og av disse er det kun 845 som har 250 eller flere ansatte. Dette viser tydelig at Norge er et SMB-land, men vår erfaring tilsier at IT-produsenter tilbyr løsninger og produkter som er skalert for et marked med større andel enterprisevirksomheter. Økonomisk kan dette by på flere utfordringer for de små og mellomstore bedriftene ved at sikkerhetsbehovet er likt for alle virksomheter, uavhengig av størrelse, i tillegg til at kravene fra Datatilsynet i forbindelse med GDPR (General Data Protection Regulation) er lik for alle.

8.5 Erfaringer fra Datatilsynet

Datatilsynet er både tilsyn og ombud. Vår oppgave er å føre kontroll med at personvernregelverket etterleves, og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem. Datatilsynet er et uavhengig forvaltningsorgan under Kommunal- og moderniseringsdepartementet (KMD). Det at vi er uavhengige betyr at vi ikke skal instrueres i enkeltsaker og hvordan vi skal prioritere vår innsats overfor ulike sektorer mm.

Datatilsynets erfaringer baserer seg på spørsmål til vår veiledningstjeneste, meldinger om brudd på personopplysningssikkerheten fra virksomheter, tips fra virksomheter og enkeltpersoner, erfaringer fra tilsyn og generell saksbehandling. På grunnlag av dette kan vi forsøke å danne oss et bilde av trender i samfunnet.

Økende digitalisering av samfunnstjenester, kombinert med innsamling av enkeltindividers informasjon, tror vi har bidratt til at den enkelte er mer bevisst sine rettigheter og friheter, men også plikter etter personvernforordningen. I 2019 mottok Datatilsynet 1916 meldinger om brudd på personopplysningssikkerheten, noe som innebærer en betydelig økning sett i forhold til tidligere år. årsaken er strenge krav til at brudd på personopplysningssikkerheten skal meldes inn til Datatilsynet.

Personvern- og informasjonssikkerhetskompetanse

Henvendelsene til Datatilsynets veiledningstjeneste er jevnt fordelt fra privatpersoner og fra virksomheter. Ut ifra de spørsmålene vi mottar har Datatilsynet grunn til å anta at virksomheter og privatpersoner har fått mer kunnskap om personvern, siden spørsmålene er mer reflekterte og vel funderte enn de var før da personvernforordningen ble innført. Likevel vil vi oppfordre til å holde fokus på opplæring i personvern og informasjonssikkerhet på alle plan i samfunnet, siden dette blir viktigere og viktigere i tråd med den stadig eskalerende digitaliseringen i samfunnet.

Krav om digitalisering har medført at det noen ganger går litt for fort når det tas i bruk programmer for å bli mer digitale, aktuelle og effektive. Vi mener at Helse Sør-Øst saken[6)] har bidratt til å sette fokus på nødvendigheten av gode risikovurderinger, og forståelse av hvorfor dette er viktig. Samtidig ser vi at norske virksomheter, private så vel som offentlige, trenger mer kompetanse på vurdering av personvernkonsekvenser. Som en kuriositet vil vi nevne at de færreste tjenester og programmer er «gratis», betalingen er ofte leverandørens tilgang til de registrertes personopplysninger. Flere av de bruddene på personopplysningssikkerheten som rapporteres til Datatilsynet har dels sitt opphav i manglende eller for svake risikovurderinger.

Skal vi oppnå en god beskyttelse av den personlige integriteten også i fremtiden, må personvern være inkorporert i alle løsninger. Nøkkelpersoner for at fremtiden skal være personvernvennlig, er medarbeidere i utviklingsteamene, men ikke minst også ledelsen og de som bestiller og anskaffer løsninger. Utviklerne er helt sentrale fordi det er de som faktisk bygger applikasjoner, tjenester, roboter, algoritmer for automatiske beslutninger, kunstig intelligens osv. Vi tror at det er viktig å fortsette og styrke kunnskapen om innebygd personvern og personvern som standardinnstilling hos disse yrkesgruppene.

6) https://www.datatilsynet.no/aktuelt/2017/ni-helseforetak-er-varslet-om-gebyr/

Fødselsnummer

Flere henvendelser til Datatilsynet og meldinger om brudd på personopplysningssikkerheten omhandler fødselsnummeret på avveier. Fødselsnummer skal bare behandles når det er saklig behov for og metoden er nødvendig, for å oppnå slik identifisering. Selv om fødselsnummer ikke er omfattet av særlige kategorier personopplysninger, gjelder plikten om tilfredsstillende personopplysningssikkerhet. Med kravet om å offentliggjøre postjournaler ser vi økende publisering av fødselsnummer på internett. Vi tror årsaken til dette er mangel på opplæring i personvern og informasjonssikkerhet av ansatte og innleide, men også manglende internkontroll og -revisjon.

Hemmelig adresse

Flere i Norge lever på hemmelig adresse, fordi de trenger særskilt beskyttelse mot vold og trusler. For kortere eller lengre tid kan enkeltpersoner ha behov for å flytte til en ukjent adresse slik at vedkommende blir vanskeligere å finne for den som truer vedkommende. Prosessen er et omfattende tiltak og krever mye ressurser. Kompromittering av kontaktinformasjon tilhørende de som har fått tildelt hemmelig adresse kode 6 eller fortrolig adresse kode 7 er svært alvorlig for de det gjelder. Datatilsynet ser derfor tilsvarende alvorlig på denne typen brudd på personopplysningssikkerheten knyttet til sårbare enkeltpersoner og grupper. Årsaken til slike brudd tror vi er at den behandlingsansvarlige ikke er tilstrekkelig bevisst sitt ansvar for å beskytte disse personopplysningene, samt at det kan være en uoversiktlig «verdikjede», der svikt ett sted ikke blir oppdaget pga. et manglende helhetsbilde.

Databehandlere

Databehandler skal kun arbeide på instruks fra den behandlingsansvarlige, og dette formaliseres ofte i form av en kontrakt. Vi ser at ulike skytjenester tas i bruk i takt med digitaliseringen. Ofte kan en skyleverandør tilby mer verktøy, kompetanse og også informasjonssikkerhet for lavere kostnader enn at den behandlingsansvarlige drifter dette hos seg selv. Utfordringen med skytjenester er når behandlingsansvarlig ikke selv kan sette premissene i avtalene, dette gjelder spesielt når tjenester kjøpes av de store IKT-selskap. Behandlingsansvarlig opplever å være «i hendene» på databehandlerne ved å måtte aksepterer en kontrakt som strir mot de registrertes personvern. Det er nødvendig å minne om at behandlingsansvarlig står ansvarlig for pliktene i personvernforordningen, selvsagt også når de kjøper ulike skytjenester.

Et mer kontrollerende samfunn?

En jevn strøm av spørsmål til Datatilsynet omhandler arbeidslivet, og kommer fra både arbeidstakere og representanter fra arbeidsgiversiden. Spørsmål er relatert til kontroll og overvåkning på arbeidsplasser og arbeidsutøvelsen, samt bygninger. Dette inkluderer GPS-sporing av kjøretøy og flåtestyring.

Hjemmel for å kunne behandle personopplysninger baseres ofte på lovgrunnlag eller samtykke. Norge får stadig nye lover som gir det offentlige og myndighetene lov til å samle inn og behandle borgernes personopplysninger til ulike formål. Som borgere i Norge er den enkelte registret i mange nasjonale registre, og ofte svært detaljerte. Det er et spørsmål om staten har passert grensen for hva de bør vite om sine borgere og bør fokusere på å håndtere kun strengt nødvendige data..

I april la regjeringen fram et forslag til ny etterretningslov. Loven skal beskytte oss mot et økende antall cybertrusler fra utlandet og et stadig endret trusselbilde. Nesten all kommunikasjon mellom virksomheter og privatpersoner i Norge går via utlandet. Datatilsynet er svært bekymret for hvilke konsekvenser dette får for personvernet ved at e-tjenesten gis tilgang til så store mengder data om vår kommunikasjon og om våre liv.

Sosiale medier og internett florerer av bilder. Vi ser økt fokus på ulike type bruk med hensyn til bildegjenkjenning. Algoritmene kan med stor sannsynlighet predikere sykdom og legning utefra bare ***ett*** bilde. Mulighetene ny teknologi gir, kan medføre ulovlig behandling, diskriminering og profilering av enkeltpersoner.

Vi ser et økende tilbud av tekniske innretninger som gjør at man kan overvåke andre. Dette kan være programvare som installeres på og i ulike enheter, for å få oversikt over samtaler, ytringer, bevegelsesmønstre, arbeidsmønstre og oppførsel til den som bruker enheten. Ofte er disse innretningene enkle å ta i bruk og ofte medfølger demonstrasjonsvideoer. Villighet til å benytte slike tekniske innretningene kan være en indikasjon på at samfunnet kanskje i mindre grad enn tidligere ikke baseres på tillit hverandre. Dette kan også skyldes at mange rett og slett bare faller for fristelsen til å ta i bruk løsninger som er teknologisk fascinerende og brukervennlige, uten at den ansvarlige i tilstrekkelig grad reflekterer over hvilke konsekvenser dette kan ha for den individuelles rettigheter og friheter.

Aktuelle saker i 2019

Datatilsynet fattet tre avgjørelser om overtredelsesgebyr etter brudd på bestemmelser i personvernforordningen. Vi har i tillegg fattet sju andre vedtak om overtredelsesgebyr etter reglene i den gamle personopplysningsloven, siden forordningen ikke har tilbakevirkende kraft. Disse sakene gjelder ulovlig innsyn i e-post på arbeidsplassen, kredittvurderinger uten saklig behov og ulovlig publisering av bilder fra overvåkningskamera. De tre avgjørelsene som er avgjort etter reglene i personvernforordningen, har alle handlet om brudd på personopplysningssikkerheten (artikkel 32). Bergen kommune fikk et overtredelsesgebyr på 1,6 millioner NOK for at personvernsikkerheten i datasystemene som ble brukt i grunnskolen ikke var tilstrekkelig. Oslo fikk et gebyr på 500 000 NOK for å ha lagret pasientopplysninger utenfor journalsystemet ved sykehjemmet. Oslo kommune fikk også varslet gebyr på 1,2 millioner NOK for brudd på personopplysningssikkerheten i mobilapplikasjonen Skolemelding.

Verdens femte største teleselskap, 1&1 Telecom GmbH, fikk et gebyr på 9,55 millioner Euro for brudd på informasjonssikkerheten (artikkel 32). Manglende tekniske og organisatoriske tiltak gjorde det mulig for uautoriserte å hente informasjon fra kundens bestillingstjeneste.

Deutsche Wohnen fikk et gebyr på 14.5 million Euro for brudd på plikten den behandlingsansvarlige har innebygd personvern i løsningen (artikkel 25). Personopplysninger til leietakere ble lagret uten å sjekke om lagring var tillatt eller til og med nødvendig, etter formål var oppnådd.

Hotellkjeden Marriott fikk i overkant av I millioner NOK i gebyr for et sikkerhetsbrudd som antas kan ha ført til kompromittering av personopplysninger av 339 millioner kunder.
British Airways fikk 2 milliarder NOK i gebyr for manglende personopplysningssikkerhet som medførte tyveri av kundedata.

Covid 19

Under pandemien har Datatilsynet hatt større pågang fra virksomheter, spørsmål relatert til hjemmekontor, videoløsninger og ønske om kontroll over ansatte og elever. Datatilsynet opprettet en egen 24/7 beredskapstelefon hvor virksomhetenes personvernombud raskt kunne komme i kontakt med oss.

Noen ledere har gått langt i ønsket om å kontrollere at arbeidstaker virkelig gjør jobben sin på hjemmekontor. Det kan dreie seg om alt fra å gi seg selv som leder rettigheter til den enkelte ansattes epostkasse, til at alle eposter som sendes fra den ansatte skal sendes med kopi til leder. Vi har også sett eksempler på at lærere har bedt elevene om å laste ned programvare som gjør at elevens aktivitet i gymtimen vises i sanntid for læreren og andre som tilsvarende program, eller at det gjøres opptak av møter som berører sterkt personlige tema. Datatilsynet har fått spørsmål om automatisk videresending av eposter til ansattes privatepostadresse, hvilket svekker informasjonssikkerheten og kontrollen over virksomhetsinformasjon, herunder personopplysninger.

Vi har hatt henvendelser angående bruk av sosiale medier som kommunikasjonskanal for virksomheten. Det er selvsagt alvorlig dersom sosiale medier benyttes for å dele særlig kategorier opplysninger.

Datatilsynet har også hatt henvendelser om bruk av data fra basestasjoner for å varsle hytteeiere, forskningsprosjekt knyttet til smitte og hurtiginnføring av ulike typer løsninger og programmer. Vi har flere ganger måtte informere om at det som ikke var lov før pandemien, heller ikke er lov under pandemien. Datatilsynet har forholdt seg til ansvarlighetsprinsippet (artikkel 5(2)), og det er vil bli en jobb i ettertid å følge opp lovligheten av ulike aktiviteter i denne perioden.

I denne perioden har Datatilsynet også hatt en økning av rapportering av brudd på personopplysningssikkerheten relatert til phishing.

Smittestopp ble utviklet og tatt i bruk. Datatilsynet har ikke myndighet til å si ja eller nei til ulike apper, vi er et kontrollorgan som gjør tilsyn på behandling av personopplysninger. Datatilsynet besluttet å føre tilsyn med appen, og vurdere lovligheten ved av løsningen. Vi mener appen er en svært inngripende i den enkeltes personvern, relatert til EMK 8. I fredstid/normaltid ville Datatilsynet aldri akseptert slik inngripende behandling. Vi fokuserer også på dataminimeringsprinsippet, lagringstid og nytteverdien av innsamlet data gitt formålet. Formålet med kartlegging av befolkningens bevegelser er heller ikke spesifikt nok, det omfatter både å hindre smittespredning samt forskning.

Vi grunn til å tro at flere kontinuitets- og beredskapsplaner manglet eller ikke hadde tatt høyde for en risiko ved hjemmekontor og -skole når pandemien brøt ut. Disse planene vil forhåpentligvis etableres og oppdateres med føringer og regler for hjemmekontor. Flere har vært kreative under covit19-perioden, og ofte fordi virksomheten mangler føringer fra ledelsen. Eksemplene her er videoløsninger eller kommunikasjonsprogram som verken er testet med hensyn til personvern og informasjonssikkerhet.

9.

Forebyggende aktiviteter og tiltak

9.1 Styringssystemer og lederforankring

God digital sikkerhet forutsetter et systematisk arbeid som er forankret hos virksomhetens ledelse. Et fungerende styringssystem for informasjonssikkerhet vil redusere risikoen for uønskede hendelser og bidrar til at sikkerhetsbrudd i større grad oppdages av virksomheten selv. Et fungerende styringssystem for informasjonssikkerhet bidrar også til at virksomheter har bedre kontroll på sine data og reduserer risikoen for brudd på personopplysningsloven. NSM anbefaler at styringssystemet etableres med grunnlag i anerkjente standarder.

Sikkerhet må være en del av den helhetlige virksomhetsstyringen for å oppnå et forsvarlig sikkerhetsnivå.

I dag er virksomheter i privat og offentlig sektor avhengig av tilstrekkelig styring og kontroll på digital sikkerhet for å lede virksomheten på en god og forsvarlig måte. Det er virksomhetens leder som har ansvar for at det er etablert et styringssystem. Dette har blitt enda viktigere i møte med stadig mer komplekse verdikjeder og et næringsliv preget av internasjonalisering. I og med at virksomhetene knyttes sammen gjennom stadig nye avhengigheter, kan det resultere i at sårbarheter i én virksomhet får konsekvenser for andre virksomheter. Mangelfull sikkerhetsstyring og ledelse fører til at de viktigste risikoene ikke blir identifisert, håndtert og redusert.

Når styret i en virksomhet skal påse at selskapet har god internkontroll og hensiktsmessige systemer for risikostyring[7] bør dette omfatte styring og kontroll på området informasjonssikkerhet. Dette er anbefalinger som har til hensikt å øke antall virksomheter som rapporterer informasjonssikkerhetshendelser til sitt styre. Det er ønskelig at flere slike hendelser rapporteres til politi eller andre myndighetsorganer.

Sikkerhetsbevisste ledere

NSM har over flere år observert en klar sammenheng mellom sikkerhetsengasjerte ledere og sikkerhetstilstanden i virksomheten. Der ledelsen er fraværende i sikkerhetsspørsmål, blir avstanden til sikkerhetsarbeidet fort stor, og det blir vanskeligere å få besluttet, gjennomført og evaluert relevante tiltak. NSM erfarer at de mest alvorlige avvikene ved tilsyn gjerne forekommer i virksomheter hvor sikkerhet behandles som et fagområde som er litt på siden av virksomhetens fokus og av en adskilt gruppe mennesker.

7) Kapittel 10 «Risikostyring og intern kontroll» i «Den norske anbefalingen om eierstyring og selskapsledelse», Norsk utvalg for eierstyring og selskapsledelse, 17. oktober 2018. https://nues.no/eierstyring-og-selskapsledelse/

9.2 Digital sikkerhetskultur

NorSIS` bestemte inntrykk er at mange virksomheter tror informasjonssikkerhet er noe som ikke angår dem. Ifølge en undersøkelse vi fikk utført i 2019, oppga hele 22 prosent av norske virksomheter at det var lite sannsynlig at dataangrep vil lamme dem. Derfor er det også viktig å jobbe med holdninger.

Det handler grunnleggende sett om å ha en kultur for sikkerhet, og å la denne bli en naturlig del av hele virksomhetskulturen. Digital sikkerhetskultur er våre felles verdier, holdninger, normer, kunnskaper og handlinger for å kunne ta del i et digitalisert samfunn på en trygg måte.

Informasjonssikkerhetshendelser kan ramme alle

Det første steget for å få på plass en slik sikkerhetskultur er å erkjenne at dataangrep og andre sikkerhetshendelser kan ramme alle. Mange er nok av den formening at de ikke har verdier som er attraktive nok for slike målrettede angrep. Det stemmer ikke. De kan likevel bli brukt i både verdikjedeangrep mot andre aktører eller rammes av mer vilkårlige trusler som fakturasvindel, direktørsvindel eller løsepengevirus. Dernest må alle i virksomheten vite hva som skal gjøres når noe skjer. Det handler blant annet om hvem som skal varsles, samtidig som ledelsen må ha en plan for hvordan det skal løses.

Det er også viktig for enhver virksomhet å ha en intern åpenhet om sikring av egne verdier, og en kultur der alle oppfordres til å melde fra om hendelser som avviker fra normalen. Undersøkelser som NorSIS har gjennomført viser at fire av ti nordmenn synes det er ubehagelig å si fra om egne eller arbeidskollegaers brudd på IKT-regler. Det bør flere virksomheter ta på alvor.

9.3 NSMs Grunnprinsipper for IKT-sikkerhet

NSMs Grunnprinsipper for IKT-sikkerhet[8)] ble utgitt som versjon 2.0 i april 2020. Dette er et sett av prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. De representerer et utvalg som vi mener er mest relevante for norske virksomheter. De er utarbeidet i samarbeid med virksomheter som forvalter kritiske samfunnsfunksjoner og/eller kritisk infrastruktur, men de er relevante for alle offentlige og private virksomheter. Grunnprinsippene gjelder både virksomheter som i hovedsak forvalter sine egne IKT-systemer selv og virksomheter der flere IKT-tjenester forvaltes av en tredjepart. De er relevante uavhengig av om virksomheten er underlagt Sikkerhetsloven eller ikke.

Prinsippene er delt inn i fire kategorier. For hvert prinsipp er det beskrevet

- *Mål for prinsippet*
- *En begrunnelse for hvorfor dette prinsippet er viktig*
- *Anbefalte sikkerhetstiltak som en virksomhet bør etablere for å følge prinsippet*
- *Utdypende informasjon og lenker til andre kilder*

8) https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/grunnprinsipper-for-ikt-sikkerhet-2-0/

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 sikkerhets-overvåkning
- 3.3 Analyser data fra sikkerhets-overvåkning
- 3.4 Gjennomfør inntrengings-tester

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

9.4 Forsvar i dybden

Et forebyggende sikkerhetstiltak skal redusere risikoen for en uønsket hendelse, men for mange trusler er det nødvendig å etablere flere lag med sikkerhetstiltak for å oppnå et akseptabelt nivå på restrisikoen for en gitt uønsket hendelse. Ved risikovurdering vil gjennomgang av scenarioer[9)] gi anledning til å beskrive forsvar i dybden og bruk av både forebyggende og konsekvensreduserende sikkerhetstiltak.

Flere typer angrep utnytter e-postmeldinger med skadevare eller med lenker til falske nettsteder som angrepsvektor. For nærmere beskrivelse av de tekniske sikkerhetstiltakene viser vi til NSMs Grunnprinsipper for IKT-sikkerhet. Det følgende er syv lag med sikkerhetstiltak som er relevante for flere scenarioer hvor trusselaktører utnytter e-post i et angrep mot virksomheten.

Vær oppmerksom på at en risikovurdering også skal behandle mulige konsekvenser for tredjepart. Dersom meldinger som sendes ut fra din virksomhet kan manipuleres av en trusselaktør kan det få konsekvenser for mottakeren av meldingen, og selv om mottakeren stopper dette angrepet kan det få konsekvenser for omdømmet til din egen virksomhet.

Foto: Unsplash

9) Se punkt 4.6 «Identifisering og valg av scenarioer» i «Risikovurdering for sikring», Håndbok, NSM, mars 2016. https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/risikovurdering-handbok/

1. **Beskytt e-post og nettleser**
   Flere forebyggende tekniske tiltak beskytter transport av e-post mellom servere for å redusere risiko for brudd på konfidensialitet, integritet og e-postmeldinger med falsk avsenderadresse. Disse tiltakene er beskrevet under grunnprinsipp 2.8 «Beskytt e-post og nettleser».

2. **Bruk skadevareskanning på e-postmeldinger og vedlegg**
   Bruk automatiserte verktøy for å analysere innkommende meldinger, meldingsvedlegg og klikkbare lenker i disse for å avdekke skadevare og andre trusler. Dette er beskrevet i tiltak 3.1.3 under grunnprinsipp 3.1 «Oppdag og fjern kjente sårbarheter og trusler».

3. **Merk usikre/mistenkelige meldinger**
   Det kan være til hjelp for brukerne dersom meldinger er tydelig merket dersom de ikke har vært sikret under transport mellom servere som beskrevet i punkt 1 av denne listen, eller dersom de er identifisert som mistenkelige av tiltaket som er beskrevet i punkt 2 av denne listen.

4. **Autentisering av brukere**
   En trusselaktør kan også skaffe seg adgang til e-postsystemet ved å utnytte en brukers tilgang og sende meldinger med skadevare fra den interne brukeren. På denne måten kan trusselaktøren omgå noen av de forebyggende sikkerhetstiltakene som er nevnt over i denne listen. NSMs grunnprinsipp 2.6 «Ha kontroll på identiteter og tilganger» beskriver relevante tiltak.

5. **Gi brukere opplæring og bedre risikoforståelse**
   Selv om det er etablert flere lag med forebyggende tekniske sikkerhetstiltak er det risiko for at meldinger med skadevare eller manipuleringsangrep havner i brukerens innboks. Sosial manipulasjon fungerer. Da er det viktig at brukerne har fått opplæring og har en sikkerhetsforståelse som reduserer risikoen for at de lar seg lure.

6. **Oppdag sikkerhetsbrudd**
   For trusselaktøren er det bare et spørsmål om tid. Uansett hvor mange lag med forebyggende sikkerhetstiltak som er etablert kan sikkerhetshendelser ramme alle virksomheter. Da er det vesentlig å ha etablert gode og effektive konsekvensreduserende tiltak. Rask deteksjon av sikkerhetsbrudd er det beste utgangspunktet for å redusere konsekvensene av et sikkerhetsbrudd. Grunnprinsippene 3.2 «Etabler sikkerhetsovervåkning» og 3.3 «Analyser data fra sikkerhetsovervåkning» beskriver relevante tiltak som kan etableres for å oppdage sikkerhetsbrudd.

7. **Håndter hendelser og gjenopprett normal driftssituasjon**
   Det siste punktet i gjennomgangen av scenarioer er håndtering av den uønskede hendelsen. Det gir mulighet til å forberede seg på mulige hendelser med en målsetning om at håndtering av denne typen hendelser kan gjennomføres effektivt. NSMs grunnprinsipper i kategori 4 «Håndtere og gjenopprette» om å håndtere ønskede hendelser, minimalisere skaden, fjerne hendelsesårsaken og gjenopprette integriteten til nettverk og IKT-systemer.

Eksempelet over er en generell scenariogjennomgang. En konkret scenario kan for eksempel være et angrep med «kryptolocker» og da vil det være naturlig å legge til et forebyggende sikkerhetstiltak for å etablere evne til gjenoppretting av data som er tema beskrevet i NSMs grunnprinsipp 2.9 «Etabler evne til gjenoppretting av data». Dette er et forebyggende tiltak som er en forutsetning for effektiv gjenoppretting av en normal driftssituasjon og å sikre virksomhetskontinuitet.

9.5 Passord og totrinnsbekreftelse[10)]

Passord utgjør fortsatt en betydelig sårbarhet.

- Virksomhetene glemmer ofte å bytte standardpassord på produkter.
- Passordene er for enkle og forutsigbare, noe som muliggjør passordgjetting.
- Passord gjenbrukes mellom personlige administrative konti og sluttbrukerkonti, mellom ulike tjenester og mellom forskjellige systemer, både interne og eksterne. Ett passord kan dermed gi tilgang til flere systemer.

Tiltak 2.3.7 i NSMs Grunnprinsipper for IKT-sikkerhet er å endre alle standardpassord på IKT-produktene før produksjonssetting. Tiltak 2.3.10 sier at dette også gjelder IoT-enheter. Tiltak 2.6.3 anbefaler å bruke et sentralt verktøy til å kontrollere passord-kvaliteten opp mot virksomhetens sikkerhetskrav. NSM har publisert råd og anbefalinger om passord[11)].

Passord utgjør fortsatt en betydelig sårbarhet

Totrinnsbekreftelse er trolig det aller viktigste sikkerhetstiltaket små og mellomstore bedrifter og enkeltpersoner bør ta i bruk for å sikre sine digitale kontoer. Likevel bruker under fire av ti nordmenn denne løsningen der den er tilgjengelig. Totrinnsbekreftelse fungerer ved at du logger inn med brukernavn og passord slik du pleier på din e-postkonto eller sosiale medier, men ved førstegangs pålogging fra en ny enhet må du også oppgi en engangskode. Denne koden får du gjerne tilsendt til din mobil per SMS eller via en app.

NorSIS ser ofte at innloggingsinformasjon til alt fra Facebook til virksomhetens sky- eller andre lagringsløsninger kommer på avveie, enten ved datainnbrudd eller at enkeltpersoner blir fralurt informasjonen gjennom phishingangrep. Med totrinnsbekreftelse blir det svært vanskelig å ta over en enkeltpersons eller virksomhets konto.

«Spesielt i SMB-markedet er det mange som ved skylagring verken sikrer klient (PC, mobil o.l.), bruker sikker totrinnsbekreftelse eller regulerer den enkelte ansattes tilgang til dataene og programmene de har behov for.»[12)]

Det er også viktig at tjenesteleverandører og andre tilbyr totrinnsbekreftelse for sine tjenester, enten det er til e-post kontoer eller andre personlige kontoer som for eksempel i nettbutikkløsninger.

10) Betegnelsen to-faktor autentisering er brukt om dette tiltaket tidligere i denne rapporten
11) Råd og anbefalinger om passord, 10. oktober 2019 https://www.nsm.stat.no/NCSC/NCSS-Radgivning/rad-og-anbefalinger-om-passord
12) Side 37 i «Trusler og trender 2019-2020», NorSIS, 4. februar 2020. https://norsis.no/trusler-og-trender-2019-2020/

9.6 Andre forebyggende sikkerhetstiltak

NSM utnytter kjente sårbarheter i applikasjoner og operativsystemer i sine inntrengingstester. I halvparten av testene sist år fant NSM enkeltkomponenter i virksomhetens infrastruktur som ikke lar seg oppdatere fordi supporten på produktet for lengst har opphørt. Mangelfull sikkerhetsoppdatering er en gjenganger.

Virksomhetene sliter med å holde IKT-infrastrukturen oppdatert

I NSMs Grunnprinsipper for IKT-sikkerhet handler prinsippene i kategori 2 om å beskytte og opprettholde. Flere av tiltakene i denne kategorien kan bidra til etablere en IKT-infrastruktur som kan holdes løpende oppdatert og dermed legge til rette for at en forsvarlig sikkerhetstilstand kan opprettholdes over tid. Dette er en omfattende oppgave for mange virksomheter. Hvilke punker det er hensiktsmessig å prioritere blir forskjellig fra virksomhet til virksomhet. Felles for alle er at det er viktig at dette arbeidet følges opp i virksomhetens styringssystem for informasjonssikkerhet. Sikkerheten må følges opp gjennom hele livsløpet til utstyr og tjenester.

Beskytt virksomhetens nettverk og kontroller dataflyt

Del opp virksomhetens nettverk etter virksomhetens risikoprofil. Det er viktig å ha oversikt over fysisk tilgjengelighet for svitsjer og kabler, og ha etablert tilgangskontroll på flest mulige nettverksporter. Dette er tiltakene 2.2.3, 2.4.3 og 2.4.1 i NSMs grunnprinsipper. En erfaring fra NSMs inntrengningstester er at sensorer plassert utenfor kontrollert område, kan benyttes som veien inn i virksomhetens infrastruktur. Det har vært mulig å få tilgang til sensitive data på det interne nettet via tilgang fra adgangskontrollsystem og sensorer utendørs.

NSM ser en økende grad av direkte innbrudd i sårbare internetteksponerte tjenester. Derfor vil vi anbefale at virksomheter å være oppmerksom på tiltakene i grunnprinsipp 3.1 «Oppdag og fjern kjente sårbarheter og trusler». Dersom en virksomhet vurderer å gjennomføre inntrengningstester, se grunnprinsipp 3.4 «Gjennomfør inntrengningstester». Det er hensiktsmessig å starte med tiltak 3.1.1 som er å jevnlig gjennomføre sårbarhetskartlegging og håndtere de sårbarhetene som blir avdekket, før man går videre med inntrengningstester.

IKT-sårbarheter kan gi fysisk adgang til virksomheten

Virksomheter benytter adgangskort basert på sårbar teknologi. NSM ser fortsatt utstrakt bruk av kort som er forholdsvis enkel å kopiere. Når dørlåser, adgangskontroll og alarmsystemer er digitale blir også dette en del av de systemer som må underlegges virksomhetens styring og kontroll av informasjonssikkerhet.

9.7 Opplæring

Kunnskap om trusler hos den enkelte medarbeider og leder i en virksomhet er viktigere enn noensinne. Spesielt den siste tiden har NorSIS sett en dreining fra angrep mot datamaskiner og nettverk til angrep rettet mot enkeltpersoner. Det dreier seg om alt fra rene svindelforsøk, som kan bli en dyrebar erfaring for en virksomhet, til phishing, løsepengevirus eller falske utpressingsforsøk. NorSIS erfaring er at stadig mer profesjonelle kriminelle blir bedre til å pakke inn truslene sine slik at de fremstår som ekte. Den uskyldige lenken en ansatt trykker på i en e-post kan lede til at ondsinnet programvare blir lastet ned og skape store utfordringer for hele virksomhetens IT-nettverk, og i forlengelsen, selve driften.

En ansatt som har gjennomgått en faglig og uavhengig opplæring som det NorSIS tilbyr står langt bedre rustet til å la være å trykke på lenken og bli «det svake leddet». Temaet for opplæringen er nettopp det å avdekke de vanlige fremgangsmetodene for denne typen sosial manipulering.

Det svakeste leddet i en verdikjede er den korteste veien til mest mulig fortjeneste for de kriminelle. Derfor angriper de det svake leddet i en verdikjede – en liten eller mellomstor virksomhet eller en enkelt ansatt– i stedet for å prøve seg på den store og godt sikrede virksomheten som denne lille leverer varer eller tjenester til.

NorSIS har allerede sett en vridning der kriminelle i økende grad angriper disse verdikjedene, de legitime kanalene og systemene, simpelthen fordi det er mindre motstand her enn i de ofte godt sikrede IKT-systemene. Spesielt er SMB-markedet ekstra sårbart. Manglende kompetanse og færre ressurser til å ha oversikt over systemene er hovedårsaken til at de er spesielt utsatte.

Det er også viktig at opplæringen er tilgjengelig for alle ansatte, ikke bare for dem med spesialkompetanse på feltet. I motsatt fall er risikoen at den digitale sikkerheten i virksomheten blir svekket, rett og slett fordi de ansatte oppfatter opplæringen som for vanskelig og krevende til at det er aktuelt å gjennomføre den.

Informasjonssikkerhetsutvalget

Tønnes Ingebrigtsen
mnemonic
(utvalgsleder)

Maria Bartnes
SINTEF Digital

Veronica Jarnskjold Buer
Datatilsyne

Peggy Heie
NorSIS

Bente Hoff
Nasjonalt cybersikkerhetssenter,
NSM

Anders R. Hovdum
Statens vegvesen

John Arild A. Johansen
Sopra Steria

Johnny Mathisen
Telenor

Ole Tom Seierstad
Microstoft

Soner Sevin
Coop

Thomas Stærk
Nasjonalt Cyberkrimsenter,
Kripos

Bjørn Watne
Storebrand

Vidar Østmo
Euronext VPS

Arne Røed-Simonsen
Næringslivets Sikkerhetsråd
(utvalgssekretær)

Forside: Istock

Næringslivets
sikkerhets-
råd

www.nsr-org.no