Næringslivets sikkerhetsråd

Mørketallsundersøkelsen 2018

Informasjonssikkerhet, personvern og datakriminalitet

Gjennomført av Opinion AS for Næringslivets Sikkerhetsråd

Forord

Norge er et av verdens mest digitaliserte land, noe som i tillegg til muligheter også gir oss nye sårbarheter og utfordringer. Det er satset mye på innovasjon og utvikling, men ikke like mye på utdanning og kompetanse innen IT-sikkerhet. Dette er et gap som må tettes.

Undersøkelsen skal ikke bare kartlegge sikkerhetstilstanden og IT-sikkerhetshendelser, men også bidra til kompetanseheving og hjelp i det forebyggende sikkerhetsarbeidet. Vi har lagt vekt på forebyggende aktiviteter og tiltak i rapporten.

Mørketallsundersøkelsen 2018 er den 11. undersøkelsen fra Næringslivets Sikkerhetsråd. Gjennom den henter vi inn fakta om IT-sikkerhetstilstanden i privat og offentlig næringsliv, og undersøkelsen har en sentral plass i vår opplysnings- og informasjonsstrategi.

Undersøkelsen viser at virksomhetene har liten oversikt over kostnadene knyttet til sikkerhetshendelser, kostnader som er estimert til et titalls milliarder kroner hvert år.

Både Mørketallsundersøkelsen 2016 og 2018 viser at IT-sikkerhetshendelser i stor grad oppdages ved en tilfeldighet. Et av de positive funnene i årets undersøkelse er at det å ha styringssystemer og drive systematisk forebyggende sikkerhetsarbeid gir virksomhetene bedre oppdagelsesevne. Det gjør at de raskere kan iverksette kostnadsreduserende tiltak, samtidig som det bidrar til et mer robust og bevisst digitalt samfunn.

Vi håper derfor at årets undersøkelse og rapport vil bidra til økt sikkerhetsforståelse, større oppdagelsesevne og godt forebyggende sikkerhetsarbeid.

Takk til alle som har støttet undersøkelsen og gitt sine bidrag til rapporten.

Jack Fischer Eriksen
Direktør i Næringslivets Sikkerhetsråd


NASJONAL
SIKKERHETSMYNDIGHET


POLITIET
POLITIDIREKTORATET


telenor


Nordea


coop


ONE VOICE


Microsoft


KPMG


VISMA


THOMMESSEN


mnemonic

Innhold

Sammendrag

Organisering av it-driften er i stor grad som i 2016. Det er 17 prosent av virksomhetene som fullt og helt outsourcer it-driften, 31 prosent outsourcer delvis, mens nær halvparten (48 prosent) organiserer it-driften internt. Videre er det seks av ti virksomheter som har et styringssystem eller rammeverk for informasjonssikkerhet. Også det på nivå med 2016. Mens outsourcing er mer vanlig blant de små bedriftene, er det å ha styringssystem mer vanlig blant de store.

Virus- og malwareinfeksjon er den sikkerhetshendelsen som rammer flest virksomheter. 21 prosent av virksomhetene har blitt utsatt for det i løpet av 2017. Sammenlignet med 2016 er det en klar økning i andelen virksomheter som utsettes for phishing, forsøk på hacking og faktisk hacking, DDoS-angrep eller trussel om det, og bedrageri. Av de som ble utsatt for sikkerhetsbrudd i 2017 mener 67 prosent at hendelsene skyldtes tilfeldigheter eller uflaks, mens 55 prosent mener det var på grunn av menneskelige feil. De virksomhetene som har et styringssystem ser i mindre grad tilfeldigheter og uflaks som en årsak til hendelsen enn de som ikke har slike system.

Også når det gjelder årsaken til at sikkerhetsbruddet ble oppdaget er det forskjell på virksomheter med og uten styringssystem for informasjonssikkerhet. Totalt er det 40 prosent som mener hendelsen ble oppdaget ved en tilfeldighet. Blant de virksomhetene som ikke har et styringssystem er det 50 prosent som oppdaget hendelsen ved en tilfeldighet. I virksomheter med styringssystem er det 37 prosent som oppdaget det ved en tilfeldighet. Bedrifter med styringssystem oppdager hendelsene i større grad ved rutinemessig intern sikkerhetsmonitorering (44 prosent). Dette nevnes av kun 28 prosent av virksomhetene uten styringssystem.

Hos 61 prosent av virksomhetene som er utsatt for sikkerhetshendelser blir ledelsen involvert i saken. Videre er det 31 prosent som har rapportert hendelsen til selskapets styre. Hos 19 prosent av virksomhetene med sikkerhetshendelse har følgene vært økonomisk tap. Hos 9 prosent av virksomhetene har hendelsen ført til organisasjonsendringer. Hendelsene blir i størst grad rapportert til administrator av det aktuelle tekniske system (72 prosent), mens 3 prosent rapporterer til NorCERT og 2 prosent til sektor CERT.

Nær halvparten (48 prosent) av virksomhetene har gjort endringer eller forbedringer i arbeidet med personvern og informasjonssikkerhet som følge av innføringen av nytt personvernregelverk (GDPR).

Seks av ti virksomheter har i løpet av det siste året gjennomført aktiviteter for å øke de ansattes sikkerhetsbevissthet. Dette er langt mer vanlig i store virksomheter enn i små og i virksomheter som har styringssystem for informasjonssikkerhet enn hos de som ikke har det.

Om undersøkelsen

Bakgrunn
Opinion har gjennomført Mørketallsundersøkelsen 2018 på oppdrag fra Næringslivets Sikkerhetsråd. Før undersøkelsen i 2016 ble det gjort en del endringer i undersøkelsens spørsmål og datainnsamlingsmetode. Sammenligninger blir derfor ikke gjort med resultater fra 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 Bisnodes database som henter informasjon fra Enhetsregisteret. Sammenlignet med forrige undersøkelse i 2016 er det bevisst intervjuet flere store bedrifter. Det gjør at utvalget har en annen sammensetning enn forrige undersøkelse, og at vi ved sammenligninger har kontrollert for disse utvalgsulikhetene og tolket forskjeller med forsiktighet.

Det er gjennomført 1500 intervju i undersøkelsen.

Datainnsamling
Datainnsamling er gjennomført ved hjelp av telefonintervjuer (CATI), i perioden 1. til 19. februar 2018.

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 1500 respondenter eller intervjuer (n=1500) kan vi med 95 prosent sannsynlighet si at det riktige resultatet ligger innenfor ± 1,1 og ± 2,5 prosentpoeng, avhengig av prosentresultatets størrelse. Usikkerheten er størst ved et prosentresultat på 50 prosent og minst ved prosentresultater på 5 prosent/95 prosent.

Definisjon av rammeverk for informasjonssikkerhet

Med rammeverk for informasjonssikkerhet menes intern kontroll ved etablerte rutiner, styring, tydelige ansvarsforhold og rapportering for å håndtere informasjonssikkerhet som dekker hele virksomhetens verdikjede. Rammeverk bør tilpasses virksomheten, f.eks. i henhold til sektor som helse, kraft og kommune. Herunder også i henhold til beste praksis, ISO standard, beredskapsforskriften, sikkerhetslov, personopplysningsloven (herunder GDPR), og internasjonale forordninger og direktiver som NIS. Se også føringer fra Nasjonal sikkerhetsmyndighet på deres nettsider. [1)]

Fakta om test og kontroll av bedriftens sikkerhetssituasjon

Avtalt test og kontroll av bedriftens sikkerhetssituasjon kan avsløre sårbarheter og gi dokumentasjon for å innføre nødvendige tiltak og bør vurderes som et årlig sikringstiltak. For mer informasjon, se nettsiden til Nasjonal sikkerhetsmyndighet.

[1)] Europaparlamentets og Rådets direktiv (EU) 2016/1148 av 6. juli 2016 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU.

Karakteristikker

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

Sektor	Antall (n)	Andel Intervju
Privat	947	63 %
Offentlig	553	37 %
Totalt	1500	100,0 %

Geografi

Under er en oversikt over respondentenes fylkesvise tilhørighet:

Fylke	Antall Intervju (n)	Andel Intervju
Østfold	66	4,4 %
Akershus	130	8,7 %
Oslo	187	12,5 %
Hedmark	71	4,7 %
Oppland	74	4,9 %
Buskerud	82	5,5 %
Vestfold	59	3,9 %
Telemark	64	4,3 %
Aust-Agder	36	2,4 %
Vest-Agder	45	3,0 %
Rogaland	106	7,1 %
Hordaland	148	9,9 %
Sogn og Fjordane	47	3,1 %
Møre og Romsdal	90	6,0 %
Sør-Trøndelag	66	4,4 %
Nord-Trøndelag	45	3,0 %
Nordland	106	7,1 %
Troms	54	3,6 %
Finnmark	24	1,6 %
Totalt	1500	100 %

Virksomhetsstørrelse

Undersøkelsen omfatter virksomheter i følgende størrelsesgrupper:

Virksomhets-størrelse	Antall Intervju (n)	Andel Intervju
5 til 19 ansatte	728	48,5 %
20 til 99 ansatte	508	33,9 %
100 ansatte eller flere	264	17,6 %
Totalt	1500	100 %

Bransje

Undersøkelsen omfatter virksomheter i følgende bransjer:

Bransje	Antall Intervju (n)	Andel Intervju
Primær	15	1,0 %
Industri etc.	170	11,3 %
Bygg og anleggsvirksomhet	97	6,5 %
Varehandel etc.	310	20,7 %
Transport/lagring	45	3,0 %
Overnattings-/serveringsvirksomhet	58	3,9 %
Tjenesteytende næringer	252	16,8 %
Offentlig administrasjon	81	5,4 %
Undervisning	278	18,5 %
Helse og sosial	194	12,9 %
Totalt	1500	100 %

1. Organisering av it-driften

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

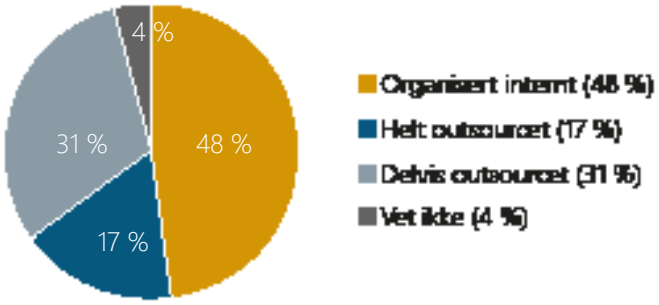
1. Organisering av it-driften

1.1 Outsourcing

17 prosent av virksomhetene har outsourcet it-driften helt. 31 prosent av virksomhetene har delvis outsourcet, mens 48 prosent har organisert it-driften internt.

Spørsmål: Er virksomhetens it-drift organisert ved at den er helt outsourcet, delvis outsourcet eller er all drift organisert internt? (n=1500)

Figur 1



Det er mer vanlig blant bedrifter med mindre enn 100 ansatte å sette ut hele it-driften enn tilfellet er for virksomheter med 100 ansatte eller flere. Blant virksomheter med 100 ansatte eller flere er det 12 prosent som har helt outsourcet. Det er på linje med 2016 undersøkelsen da 13 prosent av de store virksomhetene sa det samme. Blant virksomheter med 5 til 19 ansatte og 20 til 99 ansatte er det henholdsvis 19 og 18 prosent som har outsourcet hele it-driften. Også det er på nivå med 2016 da andelene var henholdsvis 22 og 23 prosent.

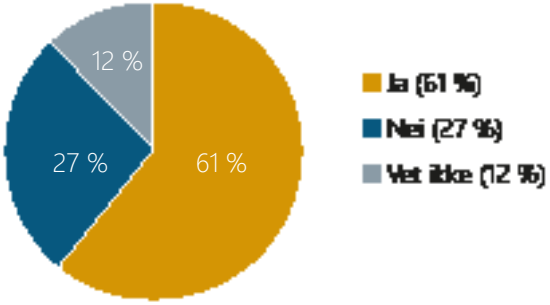
Blant de som benytter seg av outsourcing helt eller delvis er det 15 prosent som benytter outsourcingtjenester i utlandet. Dette er like vanlig enten det er snakk om store eller små virksomheter. Videre er det 82 prosent av de som bruker outsourcingtjenester i utlandet som vet hvor dataene fysisk er lagret, mens 18 prosent vet det ikke.

1.2 Styringssystem og rammeverk

Seks 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=1500)

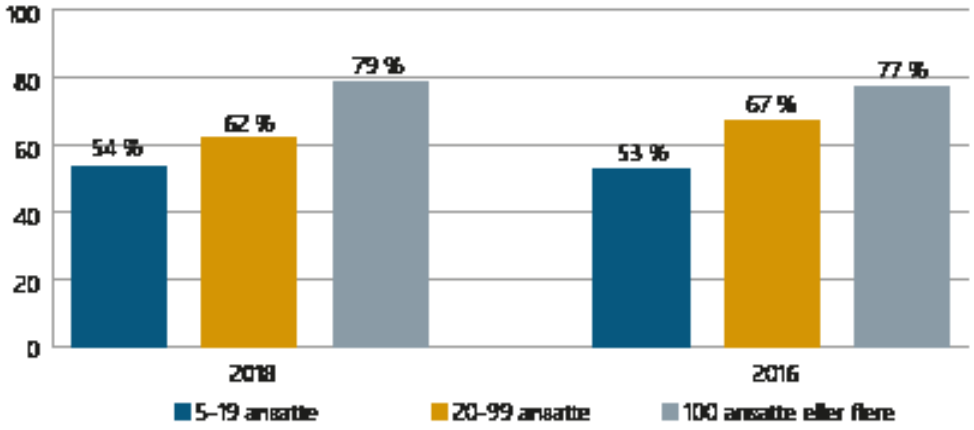
Figur 2



Det er store forskjeller mellom de minste og de største virksomhetene på dette spørsmålet. Mens 54 prosent av virksomheter med 5 til 19 ansatte har det, er det 62 prosent av de med 20 til 99 ansatte og

79 prosent av de med 100 ansatte eller flere som har rammeverk eller styringssystem for informasjonssikkerhet. Resultatene er på samme nivå som i 2016. Figur 3 viser andeler i hver størrelseskategori som har rammeverk/styringssystem i henholdsvis 2018 og 2016.

Figur 3

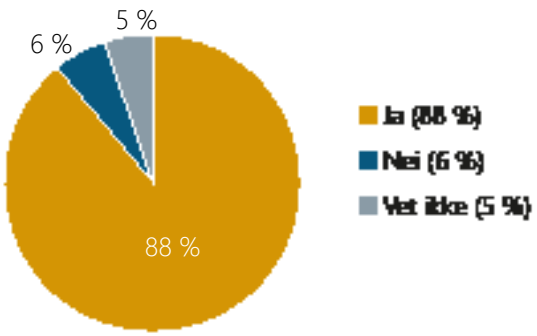


I spørsmålet ligger det selvsagt et tolkningsrom for respondenten. Det er ikke usannsynlig at definisjonen av hva et rammeverk eller styringssystem er, hvor omfattende det er og hvor godt implementert det er kan variere fra respondent til respondent. Likevel skal vi se at de bedriftene som sier de har et rammeverk eller styringssystem på en rekke 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. Nær ni av ti er av den oppfatningen.

Spørsmål: Opplever du at rammeverk/styringssystem for sikkerhet blir etterlevd i din organisasjon? (n=912 – de som har rammeverk/styringssystem)

Figur 4



Store virksomheter opplever i mindre grad enn små at styringssystemet etterleves. 12 prosent av virksomheter med 100 ansatte eller flere svarer nei, mot 4 prosent i de med 5 til 19 ansatte.

2. Hendelser

I dette kapitlet tar vi for oss hvilke informasjonssikkerhetshendelser virksomhetene er utsatt for, hendelser med negativ påvirkning og hva som anses som de mest alvorlige hendelsene.

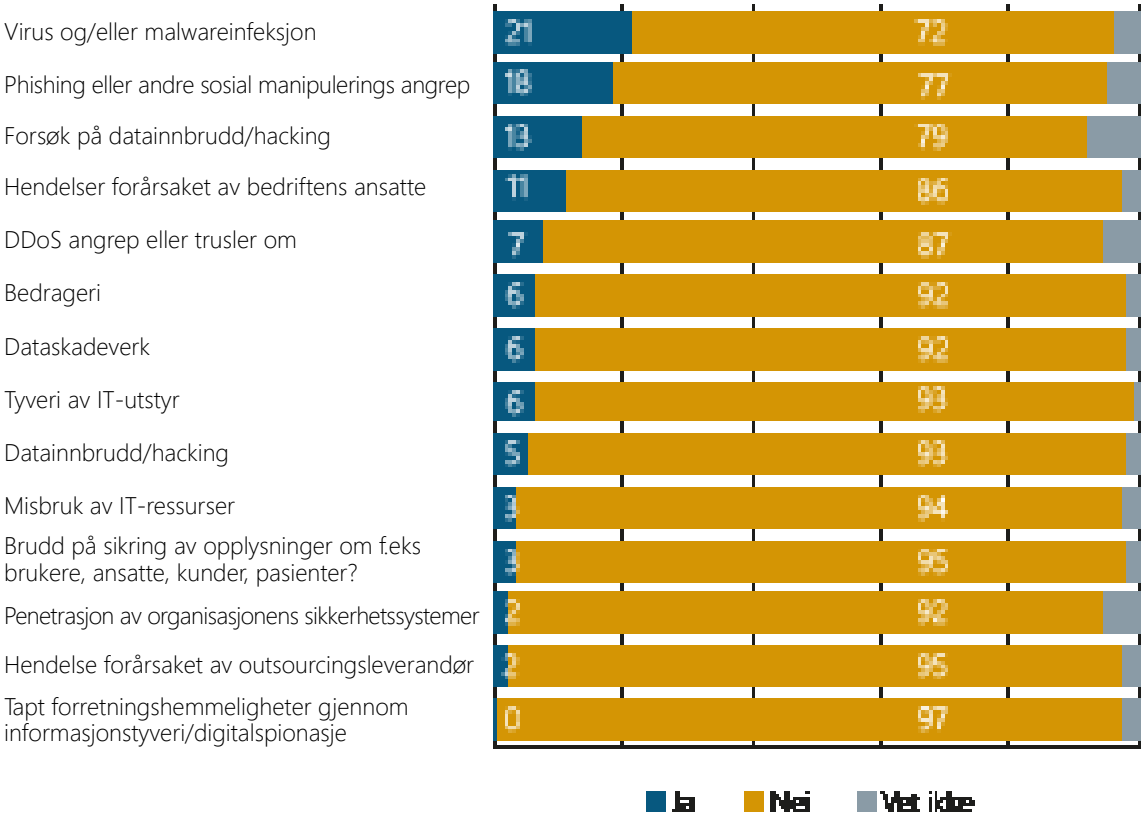
2. Hendelser

2.1 Informasjonssikkerhetshendelser

Virus- og/eller malwareinfeksjon samt phishing eller andre manipuleringsangrep er de mest vanlige hendelsene. Henholdsvis 21 og 18 prosent av virksomhetene har opplevd dette. Videre er 13 prosent blitt rammet av forsøk på datainnbrudd/hacking og 11 prosent av hendelsene som er forårsaket av ansatte. Hendelser forårsaket av outsourcingleverandør er på den andre siden langt mindre utbredt, mens ingen oppgir at de har tapt forretningshemmeligheter på grunn av digital spionasje.

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 2017? (n=1500)

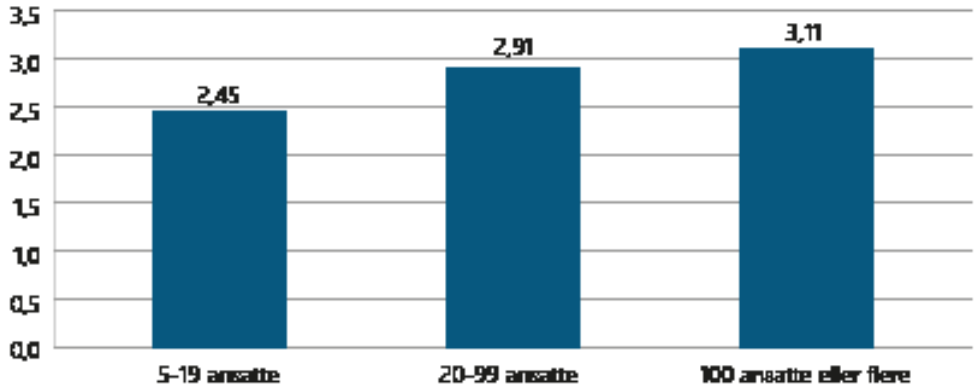
Figur 5



Blant de som har opplevd en hendelse har man i snitt opplevd 2,8 forskjellige typer hendelser. Ikke unaturlig er det mer vanlig med slike hendelser jo større virksomheten er. (Vi snakker her om antallet ulike hendelser, ikke antall hendelser totalt.)

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

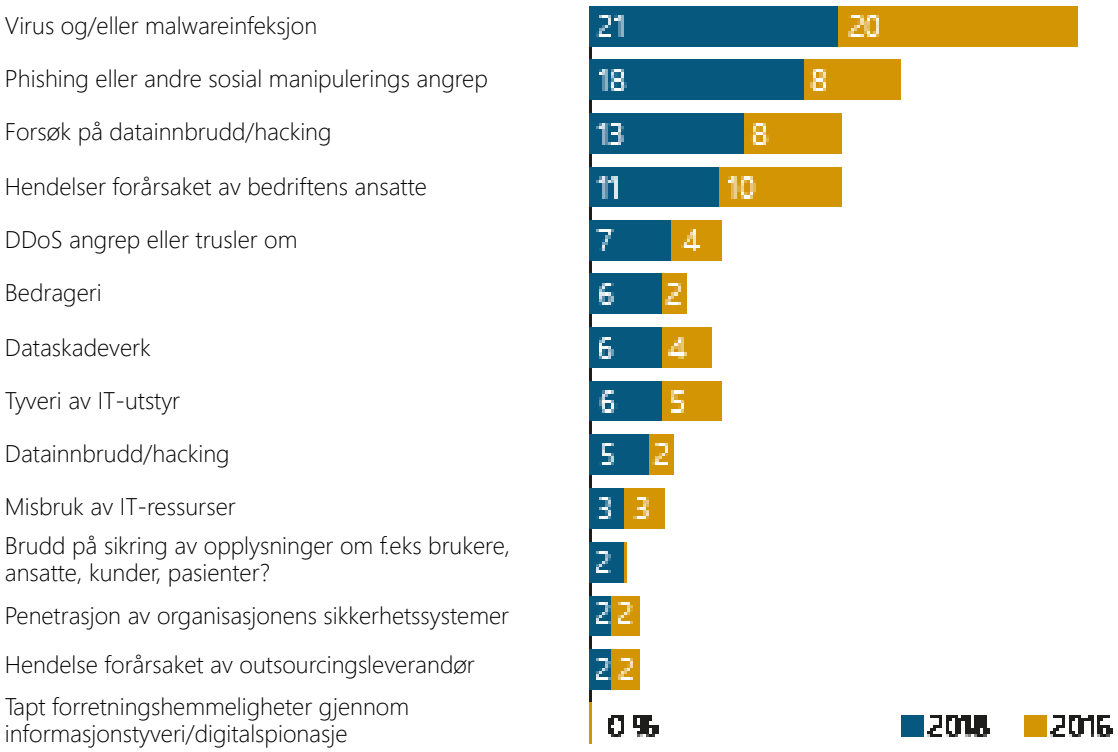
Figur 6



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

Sammenlignet med 2016 er det spesielt phishing, datainnbrudd/hacking, DDoS-angrep eller trussel om dette, samt bedrageri som har økt.

Figur 7



2. Hendelser

2.2 Hendelse med negative konsekvenser

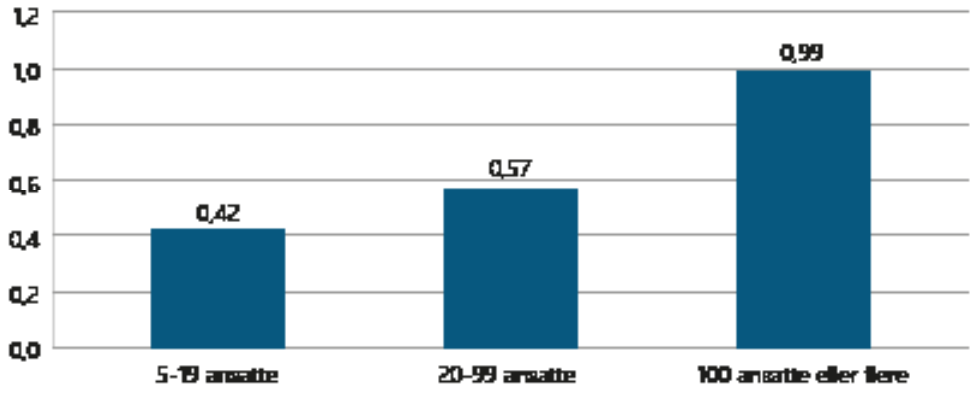
På spørsmål om informasjonssikkerhetshendelser som påvirket virksomheten negativt i form av økonomisk tap eller svekket markedsposisjon er det 19 prosent av virksomhetene som vet at de har hatt slike hendelser og som klarer å tallfeste hvor mange.

Blant de som har opplevd hendelser som har hatt negative konsekvenser med økonomisk tap eller svekket markedsposisjon har man i gjennomsnitt opplevd 3 slike hendelser i løpet av 2017. Median er 2 hendelser, så det typiske er 2 til 3 hendelser blant de som er utsatt for det.

Hvis vi antar at de virksomhetene som ikke oppgir et antall heller ikke er utsatt for slike hendelser er gjennomsnittet i hele populasjonen (virksomheter med 5 eller flere ansatte) 0,6 hendelser med negative konsekvenser i løpet av 2017. Virksomheter med 100 ansatte eller flere opplevde i snitt ett tilfelle av sikkerhetshendelser med økonomisk tap eller svekket markedsposisjon. Det er signifikant høyere enn virksomheter med under 100 ansatte (0,4 i virksomheter med 5 til 19 ansatte og 0,6 i virksomheter med 20 til 99 ansatte).

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

Figur 8



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

Spørsmål: Hva var den mest alvorlige hendelsen i 2017?

Figur 9

Virus eller malwareinfeksjon er også den hendelsen som oftest forekommer, og en rekke av de virksomhetene som nevner dette som det mest alvorlige har kun opplevd virus/malwareinfeksjon.

Ser vi kun på virksomheter som totalt sett har opplevd minst fire informasjonssikkerhetshendelser blir bildet et litt annet, og DDoS-angrep blir en mer dominerende hendelse.

Figur 10

Når det gjelder grunnen til at man opplever en hendelse som den mest alvorlige er det økonomisk tap, nedetid, tap av arbeidstid og produksjon som nevnes oftest.

3. Årsaker

Det er tilfeldigheter som avgjør om virksomhetene i Norge oppdager hendelser og det er menneskelig feil og uflaks som er årsaken til at virksomhetene rammes.

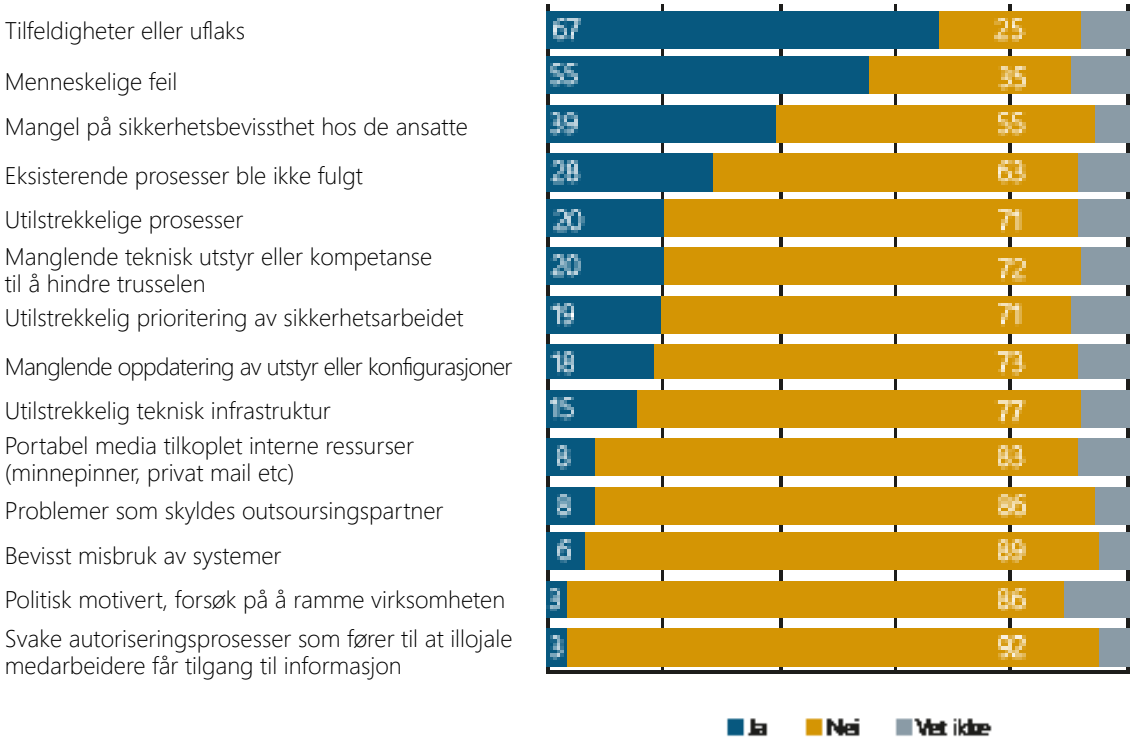
3. Årsaker

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=572)

Figur 11



Blant de som har opplevd hendelser er det 67 prosent som mener årsaken var tilfeldigheter eller uflaks, mens over halvparten også tilskriver sikkerhetsbruddet menneskelige feil.

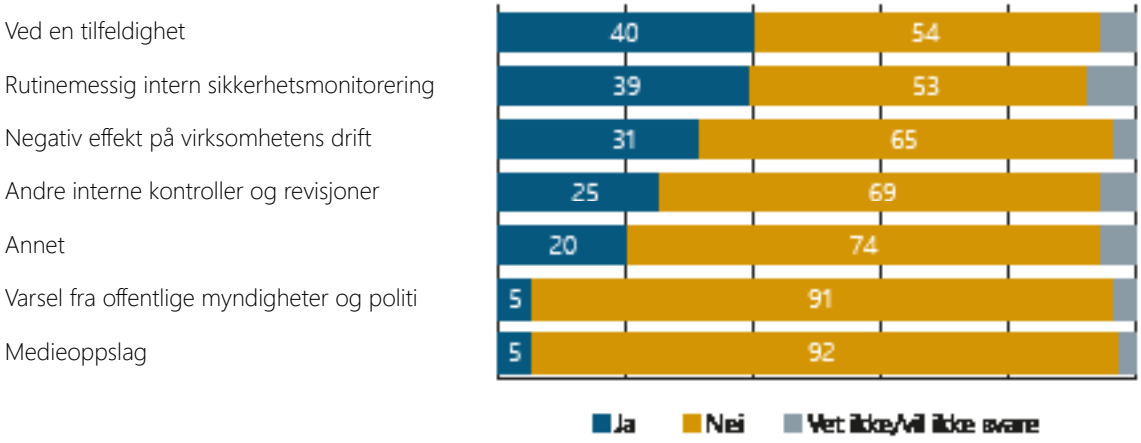
Tilfeldigheter og uflaks er i mindre grad en årsak blant de som har et rammeverk eller styringssystem for informasjonssikkerhet. 74 prosent av virksomheter som har opplevd hendelser og er uten styringssystem mener at det skyldes tilfeldigheter eller uflaks, mens det er 65 prosent av de med styringssystem som sier det samme. I tillegg mener de uten styringssystem i større grad at hendelsen skyldtes manglende teknisk utstyr eller kompetanse til å hindre trusselen. Mens det totalt er 20 prosent som oppgir denne årsaken er det 25 prosent blant de uten styringssystem og 17 prosent blant de med styringssystem.

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

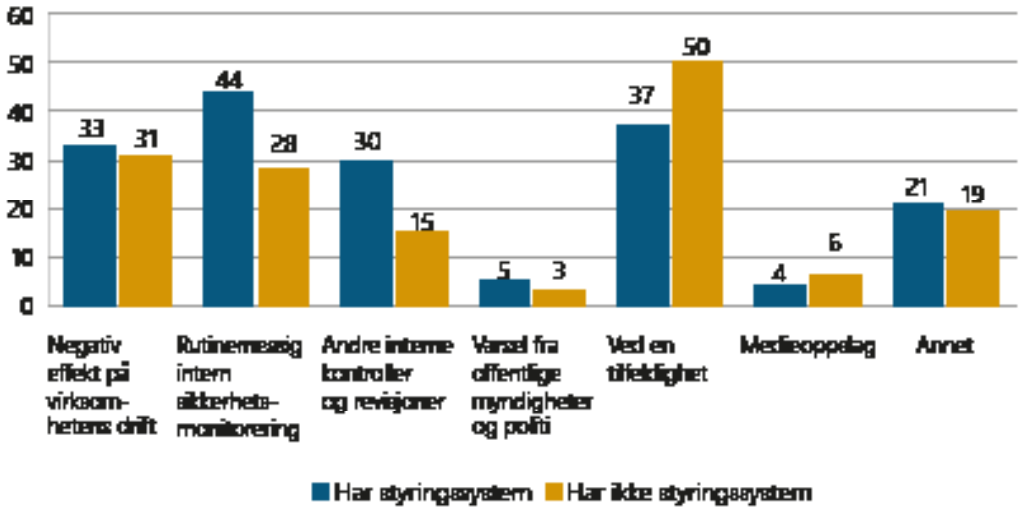
Spørsmål: Var noe av følgende årsak til at hendelsen ble oppdaget? (n=572)

Figur 12



Det er forskjell på virksomheter med og uten styringssystem for informasjonssikkerhet når det gjelder årsaker til at hendelsen ble oppdaget.

Figur 13



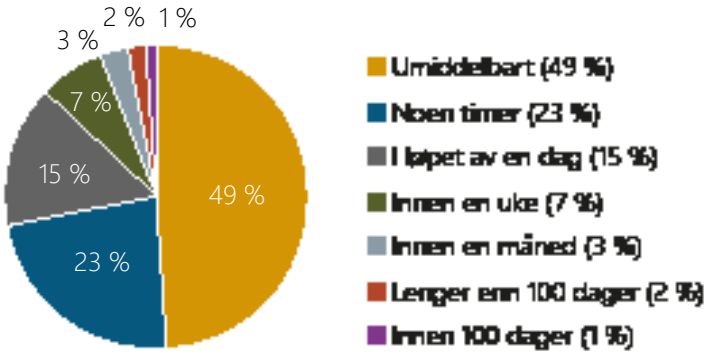
3. Årsaker

Virksomheter som har styringssystem oppdager i større grad sikkerhetsbrudd som følge av rutinemessig intern sikkerhetsmonitorering og andre interne kontroller og revisjoner enn virksomheter uten styringssystem. Bedrifter uten styringssystem oppdager på sin side sikkerhetsbruddene i større grad som en følge av tilfeldigheter enn tilfellet er for virksomhetene som har styringssystem.

Halvparten av virksomhetene oppdaget hendelsen umiddelbart (svarer for siste/mest alvorlige hendelse). Ytterligere 24 prosent oppdaget den i løpet av noen timer og 15 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.

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

Figur 14



Det kan være utfordrende å beskytte seg mot farer du ikke ser.

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.

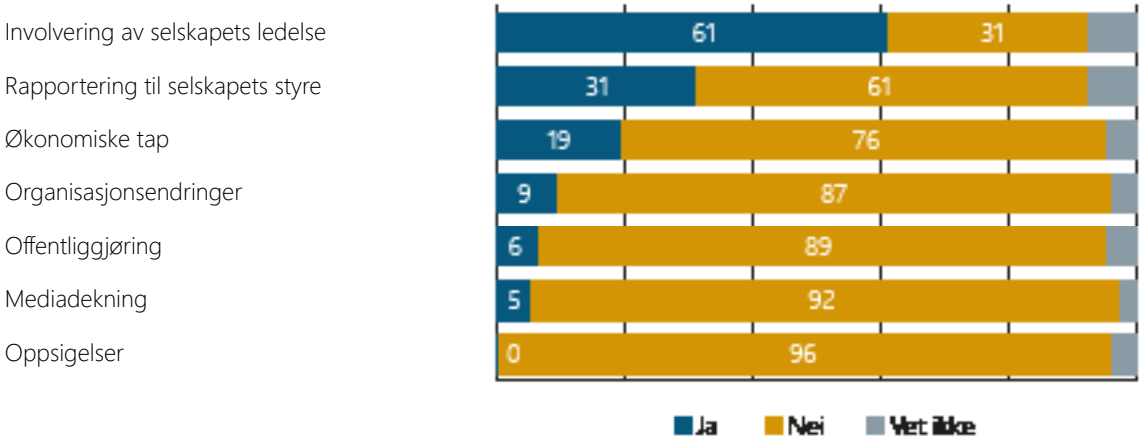
4. Følger og håndtering av hendelser

4.1 Følger av hendelsen

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

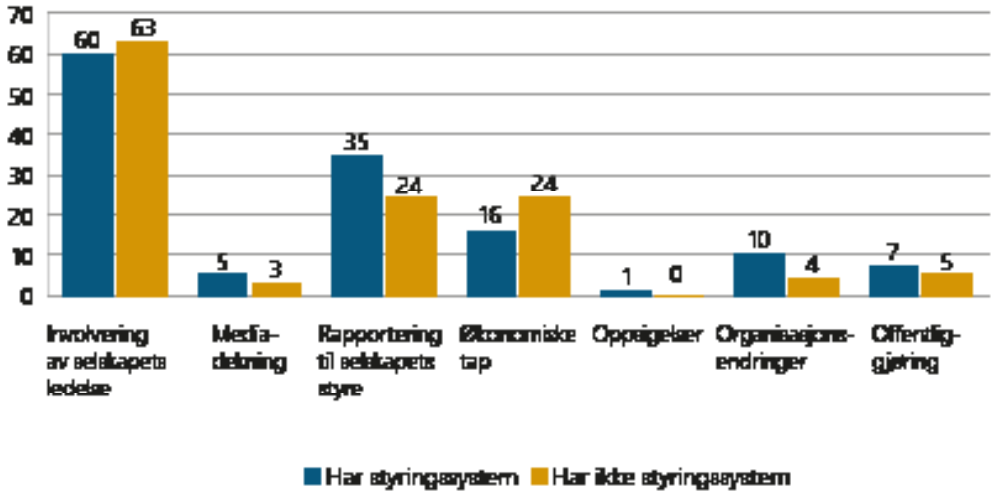
Spørsmål: Førte denne spesifikke hendelsen til følgende? (n=572)
– respondenten svarer ut fra siste hendelse/mest alvorlige hendelse.

Figur 15



Både involvering av selskapets styre og involvering av ledelsen er mer vanlig i mindre virksomheter enn i store, mens det også er forskjell mellom virksomheter som enten har eller ikke har styringssystem for informasjonssikkerhet. De som har et styringssystem har mer rapportering til styret, i større grad organisasjonsendringer og i mindre grad økonomisk tap.

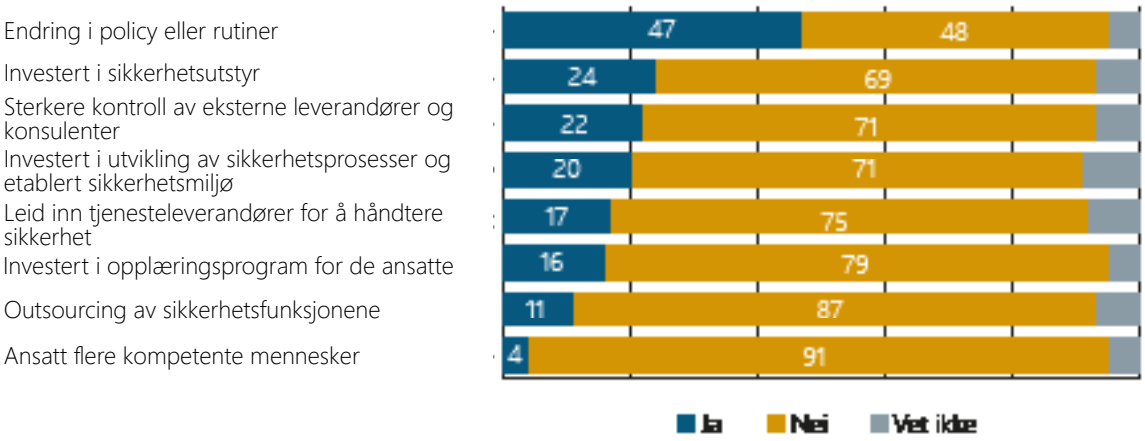
Figur 16



I tillegg til følgene nevnt tidligere har sikkerhetshendelsene også ført til endringer i en del av de utsatte organisasjonene, der 47 prosent har endret policy og rutiner.

Spørsmål: Som et resultat av hendelsen, ble noen av følgende endringer gjort i organisasjonen? (n=572)

Figur 17



Små virksomheter har gjort endringer ved å henvende seg til ekspertise utenfor egen organisasjon i større grad enn store (100 ansatte eller flere). Mens det er henholdsvis 22 og 14 prosent av de minste virksomhetene som har leid inn leverandør for å håndtere sikkerhet og outsourcet sikkerhetsfunksjoner, er det 9 og 5 prosent av virksomhetene med 100 ansatte eller flere som har gjort det samme. De små virksomhetene har i tillegg i større grad enn store investert i sikkerhetsutstyr og innført sterkere kontroll av eksterne konsulenter. De store virksomhetene har på sin side i større grad investert i opplæring for de ansatte. Virksomheter som har et styringssystem for informasjonssikkerhet har i større grad enn andre investert i utvikling av sikkerhetsprosesser og etablert et sikkerhetsmiljø. Mens 24 prosent av virksomhetene med styringssystem har gjort dette, er det 11 prosent av de uten styringssystem som har gjort det samme.

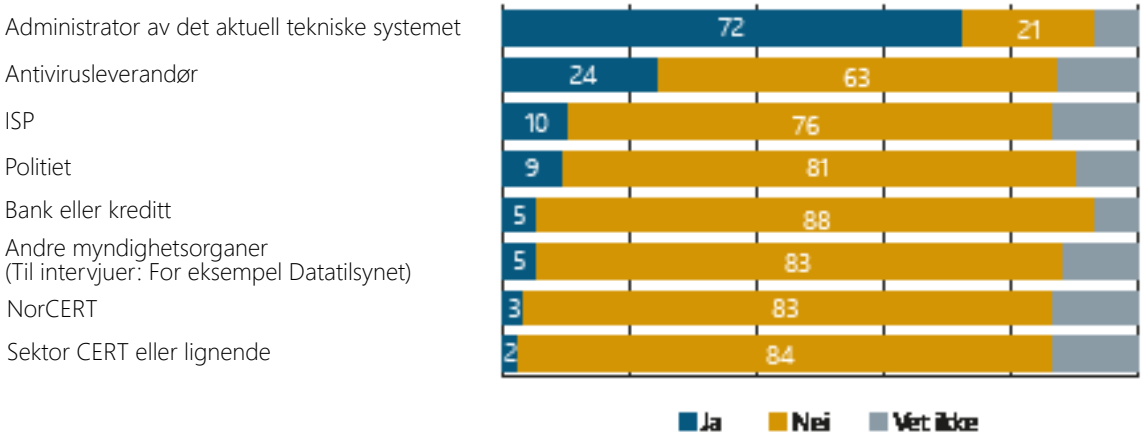
4. Følger og håndtering av hendelser

4.2 Rapportering

72 prosent av virksomheter som har opplevd sikkerhetshendelser har rapportert hendelsen til administrator av det aktuelle tekniske systemet, mens 9 prosent har rapportert hendelsen til politiet. Rapportering til NorCERT eller sektor CERT er det kun 3 og 2 prosent som gjør.

Spørsmål: Ble hendelsen rapportert til noen av følgende? (n=572)

Figur 18

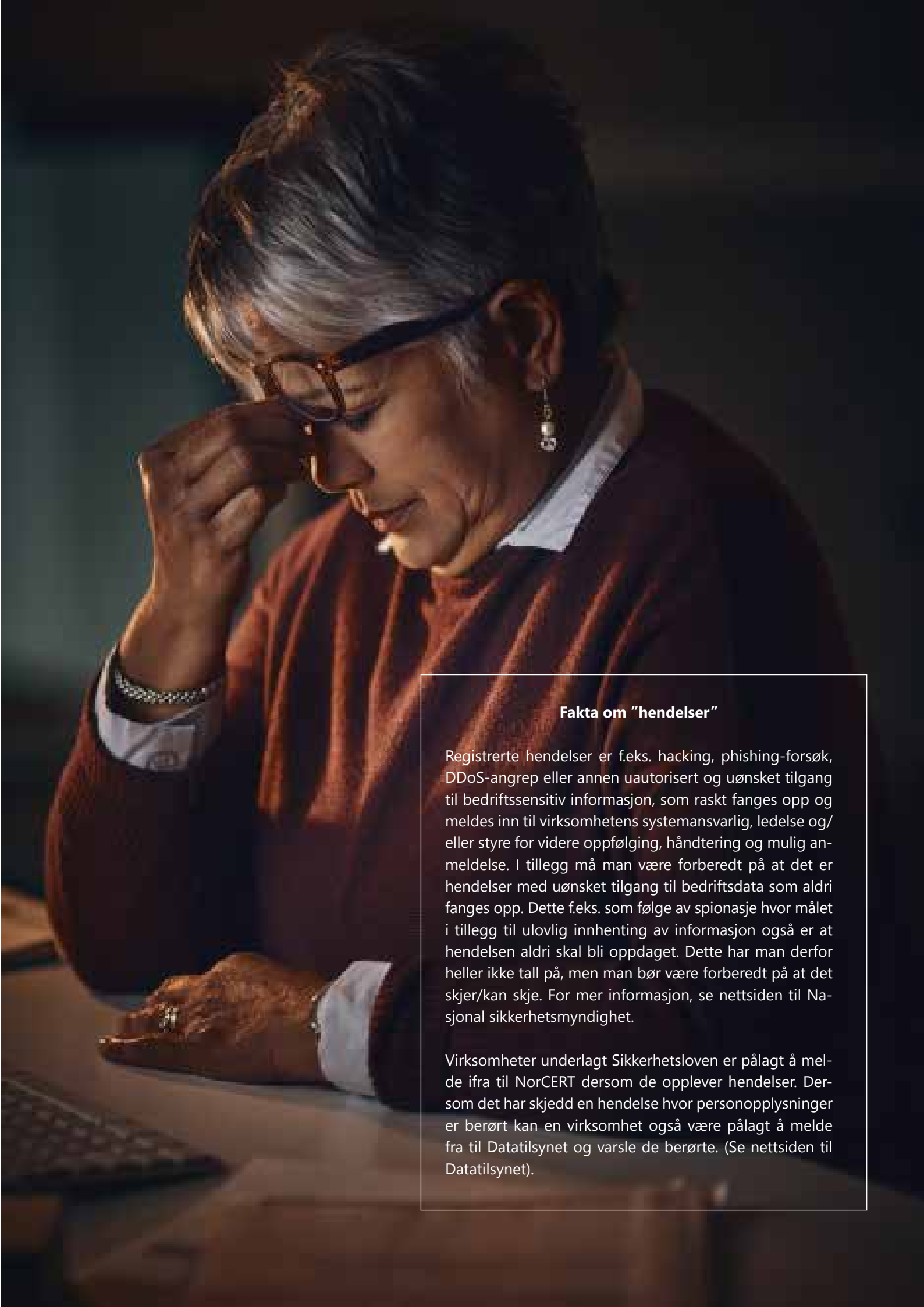


De som har et styringssystem har i større grad enn andre rapportert til administrator for systemet og ISP, men mønsteret er ikke like klart som på enkelte andre spørsmål. Det er også verdt å merke seg at de som har styringssystem i større grad ikke vet om de har rapportert hendelsen til NorCERT eller sektor CERT.

Virksomheter i ulike størrelsesgrupper følger det samme mønsteret. Eksempelvis er det ikke signifikant forskjell på små og store virksomheters rapportering til NorCERT eller sektor CERT. Rapportering til NorCERT varierer fra 2 til 4 prosent i ulike størrelsesgrupper, mens tilvarende for sektor CERT er 1 til 3 prosent.

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 drøyt 54 000 kroner for den mest alvorlige hendelsen i 2016. De som er hardest rammet estimerer en kostnad på 2 millioner. Det er ikke signifikant forskjell på virksomheter som har og ikke har styringssystem for informasjonssikkerhet, eller mellom virksomheter av ulik størrelse.



Fakta om "hendelser"

Registrerte hendelser er f.eks. hacking, phishing-forsøk, DDoS-angrep eller annen uautorisert og uønsket tilgang til bedriftssensitiv informasjon, som raskt fanges opp og meldes inn til virksomhetens systemansvarlig, ledelse og/eller styre for videre oppfølging, håndtering og mulig anmeldelse. I tillegg må man være forberedt på at det er hendelser med uønsket tilgang til bedriftsdata som aldri fanges opp. Dette f.eks. som følge av spionasje hvor målet i tillegg til ulovlig innhenting av informasjon også er at hendelsen aldri skal bli oppdaget. Dette har man derfor heller ikke tall på, men man bør være forberedt på at det skjer/kan skje. For mer informasjon, se nettsiden til Nasjonal sikkerhetsmyndighet.

Virksomheter underlagt Sikkerhetsloven er pålagt å melde ifra til NorCERT dersom de opplever hendelser. Dersom det har skjedd en hendelse hvor personopplysninger er berørt kan en virksomhet også være pålagt å melde fra til Datatilsynet og varsle de berørte. (Se nettsiden til Datatilsynet).

5. GDPR og sikkerhets-bevissthet

Dette kapitlet ser på endringer i arbeid med personvern og informasjonssikkerhet i forbindelse med at GDPR trår i kraft og aktiviteter for økt sikkerhetsbevissthet blant ansatte.

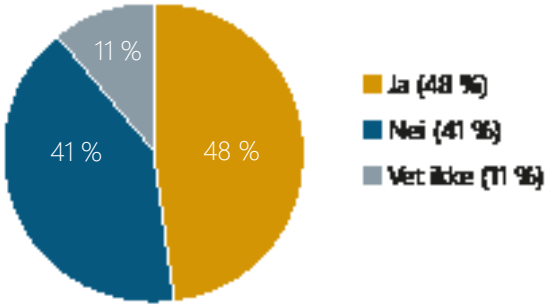
5. GDPR og sikkerhetsbevissthet

5.1 Endringer som følge av GDPR

Rundt halvparten av virksomhetene har gjort endringer i arbeidet med personvern og informasjonssikkerhet som følge av GDPR.

Spørsmål: Nytt personvernregelverk (GDPR) trer i kraft fra mai 2018. Har dette medført at organisasjonen har gjort endringer/forbedringer i arbeidet med personvern og informasjonssikkerhet? (n=1500)

Figur 19



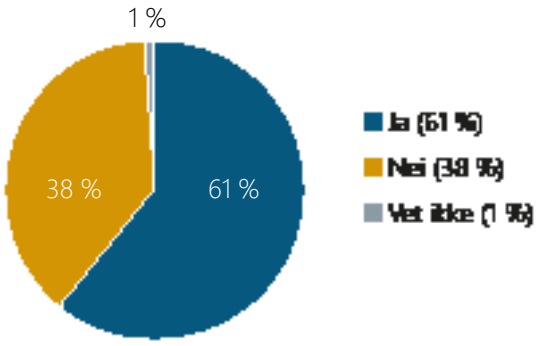
Mens det er 66 prosent av virksomheter med 100 ansatte eller flere som har gjort endringer, er det 40 prosent av de med 5 til 19 ansatte som sier det samme. Videre har 57 prosent av de med styringssystem gjort endringer, mens 31 prosent av de uten styringssystem har gjort det.

5.2 Økt sikkerhetsbevissthet

61 prosent har i løpet av det siste året gjennomført aktiviteter for å øke de ansattes bevissthet rundt sikkerhet.

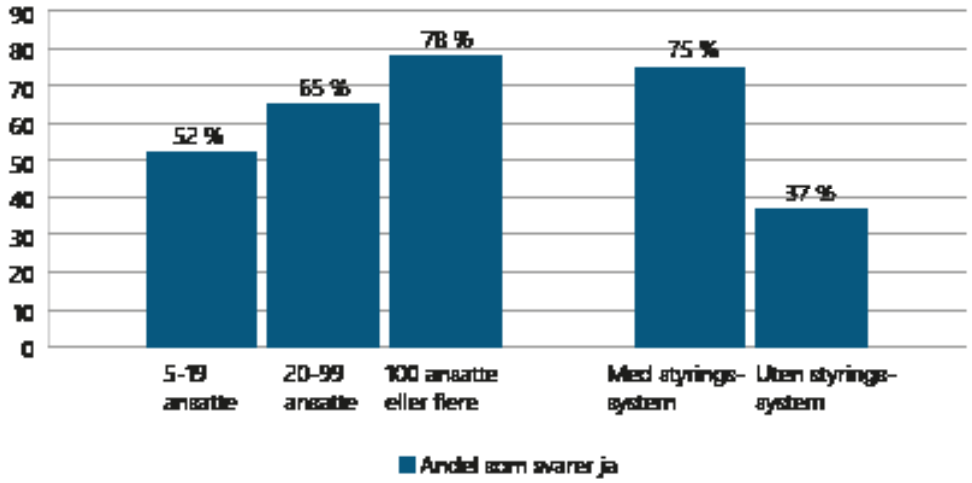
Spørsmål: Har virksomheten gjennomført aktiviteter som øker ansattes bevissthet rundt sikkerhet i løpet av det siste året? (n=1500)

Figur 20



Store virksomheter med 100 ansatte eller flere og de med styringssystem for informasjonssikkerhet er de som i størst grad har gjennomført slike aktiviteter. Mens det er 52 prosent av virksomheter i den minste størrelsesgruppen som har gjennomført aktiviteter, er det 78 prosent blant de store virksomhetene som har gjort det. Blant bedrifter med styringssystem for informasjonssikkerhet er det 75 prosent som har gjennomført aktiviteter, mens kun 37 prosent av de uten slike system har gjort det.

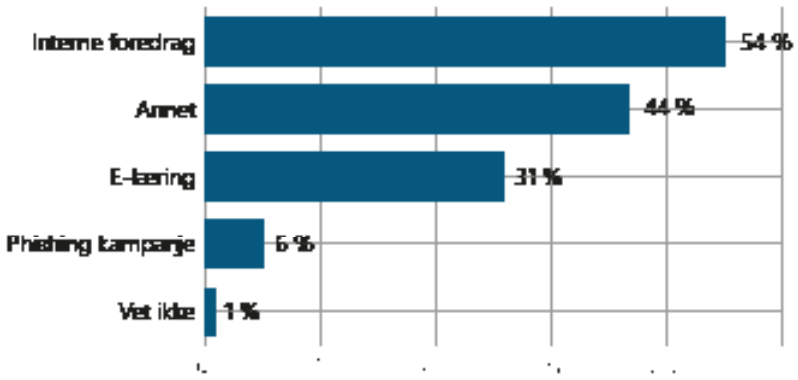
Figur 21



Blant de som har gjennomført aktiviteter er det interne foredrag som er det vanligste tiltaket.

Spørsmål: Hvilken type aktiviteter som øker ansattes bevissthet rundt sikkerhet er gjennomført i løpet av det siste året? (n=913)

Figur 22



6. Analyse

I dette kapitlet har vi analysert noen av funnene i undersøkelsen.

6. Analyse

6.1 Hovedfunn i virksomheter som oppgir å ha sikkerhetsrammeverk

6.1.1 I offentlig sektor

En høy prosentandel innen offentlige virksomheter har et rammeverk eller styringssystem for informasjonssikkerhet. Av de som rapporterer at de har rammeverk for sikkerhetssystemer oppgir 82 prosent (offentlig administrasjon) til 88 prosent (helse) av offentlige virksomheter at disse rutinene etterleves.

Undersøkelsen viser også at ved sikkerhetsbrudd rapporterer 22 prosent av offentlige helsevirksomheter at bruddet skjedde grunnet manglende prioritering av sikkerhetsarbeid.

En annen grunn til sikkerhetsbrudd som rapporteres blant de som har rammeverk for informasjonssikkerhet er utilstrekkelige prosesser.

Innen offentlig administrasjon melder 25 prosent av respondentene at manglende sikkerhetsprosesser førte til sikkerhetsbrudd. Enda flere respondenter, 40 prosent innen offentlig administrasjon, rapporterer at virksomheten har opplevd sikkerhetsbrudd grunnet manglende oppfølging av prosesser. I helsesektoren rapporterer 33 prosent det samme. **Dette er interessant ettersom det rapporteres høy grad av etterlevelse av sikkerhetsrammeverk, samtidig som manglende prosesser og rutiner blir oppgitt som en betydelig årsak til sikkerhetsbrudd.**

Funnene tyder på at til tross for at store andeler av det offentlige har styringssystemer og rammeverk for informasjonssikkerhet, og en betydelig andel rapporterer at disse etterleves i organisasjonene, er likevel oppfølging av disse sikkerhetstiltakene ikke tilstrekkelig for sikring av virksomhetene.

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.**

Til gjengjeld oppgir 40-50 prosent av de offentlige virksomhetene som har opplevd sikkerhetsbrudd at det ble oppdaget umiddelbart.

6.1.2 I privat sektor

Som forventet finner man større variasjon blant ulike bransjer i privat sektor. Innen bygg og anlegg, service, samt industri oppgir under 50 prosent at de har et sikkerhetsrammeverk på plass.

Bygg og anlegg har generelt lav modenhet innen informasjonssikkerhet. Opptil 20 prosent av virksomhetene oppgir at de ikke vet om de har et rammeverk for informasjonssikkerhet.

Av private virksomheter som har et sikkerhetsrammeverk eller styringssystem rapporterer en høy andel også at disse etterleves. Her skiller overnattings- og serveringsvirksomhet samt varehandel seg ut ved at over 90 prosent mener sikkerhetsrammeverk og rutiner rundt disse etterleves. Men ved opplevd sikkerhetsbrudd rapporteres det fra overnattings- og serveringsvirksomheter at 29 prosent mener brudd har oppstått grunnet manglende prioritering av sikkerhetsarbeid. **Dette henger ikke sammen med sektorens opplevde etterlevelse av eksisterende sikkerhetsrammeverk.**

Overordnet følger virksomheter i privat sektor prosesser for sikkerhetsbrudd o.l. i større grad enn i offentlig sektor.

Omkring en fjerdedel av virksomheter i privat sektor mener sikkerhetsbrudd skjer grunnet manglende etterlevelse og oppfølging av eksisterende prosesser.

Innen industri rapporterer 30 prosent av virksomheter at sikkerhetsbrudd oppstod grunnet manglende oppfølging av prosesser og 55 prosent at sikkerhetsbrudd ble oppdaget ved en tilfeldighet.

Ved sikkerhetsbrudd har industri, overnattings- og serveringsvirksomheter samt tjenesteytende næringer lavest modenhet for oppdagelse, hvor færre enn halvparten oppdager brudd umiddelbart etter hendelse. I andre sektorer melder mellom 50-70 prosent at de oppdaget sikkerhetsbrudd umiddelbart etter hendelse.

6.1.3 Oppsummert

Cybertrusler og -angrep har blitt en del av den digitale hverdagen vi alle må forholde oss til. Derfor blir det viktigere å ikke bare investere i sikkerhets- og forsvarsmekanismer, men også å forberede virksomheten på etterlevelse av rammeverk og retningslinjer, samt oppfølging ved hendelser.

Undersøkelsen viser at mange outsourcer IT-driften, og det rapporteres få sikkerhetsbrudd hos tredjepartsleverandører. Til tross for dette er det fortsatt viktig å forstå trusselen i virksomhetens verdikjede og å sørge for kontinuerlig oppfølging av sikkerhetsarbeid også hos samarbeidspartnere.

Virksomheter anerkjenner betydningen av cybersikkerhet og å sikre seg mot angrep, men dette kommer ikke godt til syne i rapportert oppfølging av sikkerhetsbrudd.

GDPR krever at organisasjoner har en plan for brudd på persondatasikkerhet, men mange virksomheter har fremdeles ikke etablert et sikkerhetsrammeverk og følger ikke policy og rutiner for oppfølging av sikkerhetsbrudd.

Det er økende behov for å sikre data og personvern. Dette blir også i større grad enn før belyst via offentlige diskusjoner, samt via nasjonale og internasjonale lover, reguleringer, forordninger og direktiver som GDPR og NIS.

Mange rapporterer at det er kontrasten mellom virksomhetenes arbeid og fokus på sikkerhetsrammeverk og manglende oppfølging av sikkerhetsrutiner og prosesser i hverdagen som er grunnen til sikkerhetsbrudd i virksomhetene.

6. Analyse

6.2 Rapportering og anmeldelser av sikkerhetshendelser

De virksomheter som investerer minst mulig i informasjonssikkerhet har trolig en økt sjanse for å bli rammet av datakriminalitet. I tillegg kan man være rammet over tid uten å vite om det. Det fremgår av undersøkelsen at virksomheter uten styringssystem oppdager hendelser mest tilfeldig. Virksomheter som innehar et styringssystem oppdager i større grad sikkerhetsbrudd som følge av at de har rutiner for aktiv jobbing med informasjonssikkerheten. Dette kan tyde på at mange virksomheter ikke investerer nok i informasjonssikkerhet.

Årsaker til at man ikke velger å investere i god informasjonssikkerhet kan være flere, slik som at man har en oppfatning av at sin virksomhet ikke er et attraktivt mål for trusselaktører. Eller at man tror sannsynligheten for å bli rammet er liten med tanke på alle virksomheter i verden som også kan være mulige mål. Det finnes en rapport[2)] hvor fire av ti beslutningstakere i virksomheter har oppgitt at de heller vil betale løsepenger til hackere enn å investere i datasikkerhet.

Som årsaker til sikkerhetsbrudd oppgir mange virksomheter at de dominerende faktorer er menneskelig feil, mangel på sikkerhetsbevissthet blant de ansatte og at eksisterende prosesser ikke ble fulgt. Dette kan også tyde på at man ikke velger å investere nok i informasjonssikkerhet. All den tid trusselaktørene ofte benytter sosial manipulasjon som et av sine hovedverktøy så er det et viktig tiltak innen informasjonssikkerhet å øke bevisstheten og kunnskapen blant de ansatte. Man kan ha høy logisk og systemteknisk sikkerhet, men mennesket vil likevel være det svakeste leddet i sikkerheten.

6.3 GDPR og sikkerhetsbevissthet

I år har vi fått et nytt personvernregelverk i Norge. Personvernforordningen (GDPR), som er en del av personopplysningsloven i Norge, er en EU-forordning som gjelder i hele EU/EØS. Med det nye regelverket er det kommet en del nye plikter for virksomhetene og styrkede rettigheter for borgerne.

Det er verdt å merke seg at personvernlovgivningen i Norge de siste 20 år har inneholdt mange av de samme kravene som den nye forordningen nå har tydeliggjort og konkretisert for å komme den økte digitaliseringen i samfunnet i møte. Etterlevelse av den nye lovgivningen vil sterkt bidra til økt sikkerhetsfokus og tryggere systemer.

I årets undersøkelse ble det stilt spørsmål om virksomheter har gjort endringer/forbedringer i arbeidet med personvern og informasjonssikkerhet. Vi ser av figur 19 at det er kun 40 prosent av de mindre virksomhetene som sier de har gjort endringer i forbindelse med GDPR. Det kan tyde på at mange virksomheter ikke kjenner til regelverket og ikke er klar over at de må etterleve det. Personvernregelverket gjelder for alle virksomheter som behandler personopplysninger - for eksempel innsamling, bruk, kommunikasjon, utlevering, lagring og bearbeiding av personopplysninger. Alle virksomhetene som har besvart undersøkelsen har minst fem ansatte og behandler da som minimum personopplysninger om sine ansatte, og de plikter med det å etterleve regelverket i likhet med virksomheter som har brukere, kunder, pasienter, klienter, elever osv.

Personvernregelverket stiller blant annet krav til at man vet hvor personopplysninger befinner seg. I punkt 1.1 Outsourcing ser vi at antallet virksomheter som outsourcer tjenester til utlandet nå er 15 prosent, noe som er en klar økning fra forrige undersøkelse der 8 prosent svarte det samme. Av de svarer nesten en femdel (18 prosent) at de

[2)] *NTT Security, Risk:Value Report.*

ikke vet hvor data fysisk er lagret. Dersom det er personopplysninger blant data som er outsourcet og man ikke vet hvor data fysisk er lagret kan det være at de ligger lagret i land utenfor EU/EØS. Da er det sannsynlig at det ikke er blitt gjort noen risikovurdering av leverandøren eller landet det er lagret i, og at man ikke har et lovlig grunnlag for å lagre personopplysninger der. I de tilfellene er dette brudd på personvernforordningen og brudd på personopplysningssikkerheten.

Personvernforordningen stiller krav til at virksomheter som oppdager brudd på personopplysningssikkerheten skal melde inn avvik til Datatilsynet innen 72 timer. Eksempler på hendelser som skal meldes inn til Datatilsynet er:

- Dokumenter er blitt tilgjengeliggjort på internett der det er opplysninger som er underlagt taushetsplikt eller som inneholder følsomme eller beskyttelsesverdige personopplysninger.
- Opplysninger om personer som bor på hemmelig adresse og som har blitt offentliggjort i opplysningstjenester eller distribuert til uvedkommende.
- Uvedkommende har fått tilgang til medlemsliste i politisk parti eller en religiøs menighet.
- Uvedkommende har endret personopplysninger som kan føre til skade for enkeltpersoner, f.eks. omdømmetap, diskriminering, fare for liv og helse.

Datatilsynet mottok i fjor 370 avviksmeldinger og omtrent samme antall halvveis i 2018. Her finnes det med stor sikkerhet store mørketall. Vi ser av figur 13 at 50 prosent av virksomheter uten styringssystem oppdaget hendelser ved en tilfeldighet. Med 72 timers krav om rapportering kan det være lurt å ikke være avhengig av tilfeldigheter og ukjent årsak til hendelser. Brudd på personvernforordningen kan gi bøter på opptil 4 prosent av brutto global omsetning eller 20 millioner Euro, det som er det høyeste.

7. Risikobildet/trender

I dette kapitlet presenterer vi risikobilder og trender sett fra ulike myndigheter og private aktører.

7. Risikobildet/trender

Nasjonal sikkerhetsmyndighet
NSM har som oppdrag å oppdage, varsle og bistå ved hendelseshåndtering i forbindelse med angrep mot samfunnskritisk infrastruktur eller samfunnsviktige funksjoner. Innenfor rammen av oppdraget har NSM gjennom flere år sett en jevn økning av målrettede datainnbrudd mot norske interesser, både offentlig og privat. I tillegg til økningen av målrettede angrep er det en økning av kriminelt motiverte handlinger i det norske cyberdomenet. En stor andel av disse angrepene er blitt mer avanserte enn tidligere.

Vanligste metode i målrettede angrep er bruk av infiserte epost ("Phishing" eller nettfiske). Eposten inneholder da et ondsinnet vedlegg eller lenke til en side som inneholder ondsinnet kode. I de fleste tilfeller er eposten utformet med relevant informasjon for mottakeren og sendes kun til et fåtall utvalgte brukere (spearphishing). Informasjonen om epostmottakeren blir hentet fra informasjon som angriper har tilgang til, enten fra åpne kilder eller tidligere kompromittert informasjon.

Foruten epost er skanning etterfulgt av utnyttelse av sårbare systemer den mest populære angrepsteknikken benyttet det siste året. I motsetning til nettfiske (phishing) er denne fremgangsmåten mindre avhengig av menneskelig interaksjon. Skanning etter sårbare versjoner av programvare i et nettverk er et populært valg for angripere. Hvis bedriften har manglende oppdateringsrutiner kan gamle versjoner av programvare gi angriper en billig vei inn i nettverket til bedriften. Manglende segmentering av nettverk gjør ofte at angripere kan flytte seg mellom ulike deler av virksomhetenes IKT-løsninger. NSM ser at angrep nesten alltid utnytter kjente sårbarheter. Unntaksvis ser NSM at «ikke kjente sårbarheter», såkalte 0-dags sårbarheter, blir utnyttet.

NSM ser også en trend der utdaterte webserverinstallasjoner hos mindre bedrifter med begrensede IT-ressurser blir kompromittert. De kompromitterte serverne blir så brukt som mellomledd i nye angrep mot andre mål, både nasjonalt og internasjonalt. Det er ikke bare sårbare versjoner av programvare som utnyttes. NSM observerer at angripere i større grad utnytter sårbare implementasjoner av systemer, og her menes en funksjon eller program som er sårbar for kompromittering på grunn av svakheter i designet til en tjeneste, eller grunnet feilkonfigurering. Slike systemer blir ofte utsatt for angrep som utnytter disse svakhetene til blant annet å lekke informasjon for å oppnå tilgang til systemet.

Angrep via leverandørkjede er en teknikk der en aktør velger å angripe verdikjeden til en bedrift i motsetning til et direkte angrep. NSM observerer at aktører i økende grad angriper svake ledd i verdikjedene.

En sterk negativ utvikling innenfor cyberkriminaliteten er graving (eng: «mining») etter kryptovaluta. Illegitim graving etter kryptovaluta (såkalt «kryptojacking») øker sterkt. og har derfor åpnet for en rekke nye problemstillinger innen forebyggende IT-sikkerhet.

NSM har ikke observert noen angrep utført av hacktivister som har fått store samfunnsmessige konsekvenser i Norge så langt, men lengre nedetid på tjenester og nettsider har forekommet.

NSM har observert en trend der angrep blir mer komplekse og hvor avanserte aktører beveger seg vekk fra phishing og over til andre teknikker. Dette kan medføre at det i mange tilfeller er blitt vanskeligere og krever mer å avdekke et datainnbrudd. NSM anbefaler sterkt at virksomheter fortsatt fokuserer på epostsikkerhet da nettfiske fortsatt er en angrepsteknikk som kan skade virk-

somheten i stor grad. I tillegg må virksomheter bygge generell motstandsevne for å kunne avdekke og stå imot ulike komplekse angrep.

Viktigst av alt bør være at virksomheter må ha kontroll på hele verdikjeden innen sitt IKT-miljø, og NSM Grunnprinsipper er laget for å hjelpe til i dette arbeidet. Her startes det med prosesser rundt identifikasjon og kartlegging av IKT-miljøet. Beskytte, bevare og oppdage er viktige elementer for å unngå å bli kompromittert, samt når uhellet er ute bør det finnes gode gjennomtestede rutiner for å håndtere og gjenopprette sitt IKT-miljø. NSM anbefaler at alle virksomheter anvender Grunnprinsippene som et minimum i sitt sikkerhetsarbeid.

Nasjonal motstandsdyktighet og beredskap i det digitale rom må styrkes. I løpet av høsten 2018 etableres derfor Nasjonalt cybersikkerhetssenter som en del av NSM. Senteret skal gjøre det digitale rom sikrere for norske aktører.

Telenor

Mot slutten av 2017 var det ransomware som var den trusselen som ble mest omtalt i datasikkerhetsverden. Norske virksomheter har heldigvis ofte en forholdsvis god grunnsikring, siden patching av i alle fall operativsystemet i bunn gjøres av de fleste. Piratkopiering av Windows er også lite utbredt. Dette gjorde at Norge stort sett gikk klar av de store spredningene av ransomware og programvare som slettet harddisker i 2017 (WannaCry/NotPetya). Denne malwaren spredde seg lokalt i nettverket gjennom svakheter i Windows. Microsoft hadde imidlertid allerede patchet svakhetene da spredningen startet, så fullt patchede maskiner var immune. Ingen av våre norske kunder ble rammet av disse angrepene.

Tidlig i 2018 var det malware som utvant kryptovaluta som tok over oppmerksomheten. Angriperne begynte å skanne etter sårbare systemer, spesielt webservere, og infiserte disse. Dette ble også en del norske virksomheter utsatt for, også flere av våre kunder. For angriperne er det en del fordeler med å bruke denne typen malware framover:

- Ofrene merker ofte ikke at de er infisert og at ressursene til PCene deres misbrukes.
- Ressursene kan dermed ofte misbrukes over lang tid.
- Pengene tjenes helt automatisk uten at offeret må overføre penger eller gjøre noe aktivt.
- Ingen kommunikasjon med offeret.
- Ransomware-angrep kan gjøre store skade for offeret og dermed føre til større straff eller til og med dårlig samvittighet for gjerningspersonene. Å stjele dataressurser er ikke destruktive i samme grad.

Generelt er det mindre generelle infeksjoner av PCer og servere i Norge nå enn tidligere. Exploit-kits som før infiserte datamaskiner via nettlesere har forsvunnet nesten helt. Folk blir heller lurt til å gi fra seg brukernavn/passord ved hjelp av phishing. Web mail er et svært populært mål enten bedriften drifter eposten selv eller de har satt den ut til skyen. Angriperne lurer ofte først noen få ansatte før de sender ut målrettede phishing-eposter fra offerets egen konto. Ofte blir det satt på videresending av epost fra rammede kontoer slik at angriperne kan stjele bedriftshemmeligheter eller forberede videre utnyttelse, som for eksempel direktørsvindel. Vi anbefaler å bruke to-faktor-autentisering på alle epost-kontoer for å begrense denne typen angrep.

Direktørsvindel har blitt enda mer sofistikert og målrettet i det siste. Bakmennene gjør seg mer flid med å kartlegge roller og relasjoner i bedriftene før de setter i gang angrepet og skriver på godt norsk. Disse angrepene kan ofte gi bakmennene meget store gevinster. Dette er en type svindel

7. Risikobildet/trender

svindel som det er vanskelig å lage tekniske barrierer mot. Her er det opplæring av ansatte og gode interne rutiner som er viktig.

Fortsatt er det datainnbrudd fra fremmede makter mot norske mål med det formål å drive spionasje og informasjonsinnhenting. I de aller fleste tilfellene er det e-post som er veien inn for angriperne. Det brukes gjerne phishing, eller Microsoft Office-filer med malware som vedlegg. Eksempler på virksomheter som har blitt rammet av dette i det siste er NUPI og Helse Sør-Øst. Mange norske bedrifter blir nok utsatt for industrispionasje uten at de er klar over det.

Det kommer fortsatt bølger med trusler om DDoS-angrep mot bedrifter. Bedriftene trues til å betale "beskyttelsespenger" for å hindre påståtte kommende angrep. Ofte kommer det "test-angrep" sammen med trusselen. Det er imidlertid ikke fullt så ofte at det kommer store angrep i etterkant av test-angrepet, selv om løsepengene ikke blir betalt. Antallet DDoS-angrep i Telenors nettverk totalt er noe fallende, men de aller fleste ofrene er privatbrukere. Hittil i år har vi hatt 1806 angrep. 599 av disse angrepene har blitt håndtert og mitigert av TSOC. Det største angrepet var på hele 101 Gbps og varte i én time. Typisk blir 4-10 av våre betalende kunder på DDoS-filtrering angrepet i løpet av en måned.

Kripos

Trusselaktiviteten mot norske virksomheter vil fortsatt bestå av kjent kriminalitet som direktørsvindel, phishing-kampanjer og tjenestenektangrep.

Kripos har blitt oppmerksom på at trusselaktørene har blitt mer teknisk kompetente og i større grad skaffer seg ulovlig tilgang (kompromittering) til e-post kontoer, etc. Ved å ha tilgang til e-post kontoer kan trusselaktøren fremstå med troverdighet som en person i virksomheten og således villede andre til å utføre handlinger de ønsker. Språket i korrespondansen med offer har også blitt bedre både på norsk og engelsk. I flere tilfeller fremstår språket som helt plettfritt, og trusselaktøren svarer raskt tilbake til offeret med god skriftlig fremtoning, noe som gjør at offeret ikke har mulighet til å bli advart med det som grunnlag. Summen av dette medfører at det er vanskeligere å avsløre at man blir utsatt for svindel, og det vil fremover sette virksomheters rutiner og sikkerhetssystemer på større prøve.

Kryptovaluta sin fremtreden har medført at trusselaktører benytter ulovlig tilegnet datakraft til utvinning. Det har også vært flere tilfeller hvor personer har blitt svindlet av falske kryptovaluta vekslere. Så lenge kryptovaluta har en viss verdi er det meget sannsynlig at enkelte aktører vil fortsette å svindle personer og at man utnytter andres datasystemer for å tjene penger på utvinning av kryptovaluta.

Krypteringsvirus gjør skillet mellom statlige aktører og organiserte kriminelle grupper mer komplisert. Krypteringsvirus kan brukes både som sabotasjemiddel og som middel for å kreve løsepenger. Trusselaktørene har blitt flinkere til å bygge på erfaringer fra tidligere løsepengeviruskampanjer, og de oppdaterer kontinuerlig sine verktøy og teknikker for å trenge inn i datasystemer. Det forventes derfor mer avanserte løsepengevirus- eller krypteringsviruskampanjer fremover.

Det utvikles stadig nye mobile løsninger i forbindelse med betalingstjenester og andre tjenestetilbud. Fra internasjonale samarbeidspartnere har det flere ganger blitt rapportert om skadevare tilpasset individbaserte enheter som inneholder angrepskode for utenlandske banker. Kripos har tidligere erfart at personer har kjøpt skadevare tilpasset individbaserte enheter som de hadde til hensikt å bruke i forbindelse med angrep mot en norsk bank. De ble pågrepet før angrepet ble

iverksatt. Det er sannsynlig at man fremover vil se trusselaktører som i større grad retter seg mot mobile enheter.

Det er fortsatt trusselaktivitet mot norske banker, og det har vært flere forsøk på målrettede angrep mot bankansatte og nettbankkunder. Det er meget sannsynlig at utviklingen i hovedsak skyldes at globale trusselaktører favner stadig større nedslagsfelt for sin virksomhet. Flere globale trusselaktører fremstår som avanserte eller velorganiserte. Det er meget sannsynlig at de har tilgang på store utviklingsressurser innenfor skadevare og har stor infrastruktur med kompromitterte servere tilgjengelig. Det forventes derfor at trusselen mot norske banker og bankkunder vil vedvare eller øke fremover.

mnemonic

De siste årene har vi observert at skadevare-kampanjer ofte forekommer i en syklus lik denne: en stor kampanje blir spredt bredt uten å være rettet mot ett spesifikt mål. Som en konsekvens ser vi mange bli infisert i tiden kampanjen foregår. Deretter stilner det noe igjen, helt til neste kampanje slår til noen måneder senere. Det hele gjentar seg igjen med noen få måneders mellomrom. Nå har vi ventet lenge på den neste store kampanjen, uten at den ser ut til å være på vei.

Mens omverden blir mer oppmerksom på trusler som løsepengevirus og annen skadevare søker kriminelle stadig nye og mer effektive måter å tjene penger på. Observasjoner fra vår SOC (Security Operations Center) viser et skifte i trusselbildet fra den brede, generiske spredningen av skadevare vi har sett de siste årene, til en økning i flere store, målrettede angrep. Denne tendensen viser seg mest synlig blant angrep mot større organisasjoner og selskaper.

Angrepene er målrettet ved at de blant annet går etter én spesifikk organisasjon, eller organisasjoner med et visst antall endepunkter, i ett spesifikt geografisk område eller industri. Generelt observerer vi at trusselaktørene bak slike angrep legger større vekt på å undersøke målet i forkant av angrepet. Vi ser også at disse trusselaktørene er utholdende og kan vende tilbake med ulike angrepsmetoder og teknikker basert på lærdom fra tidligere forsøk. Bak disse typene angrep ligger det mer arbeid og ressurser enn de generiske spredningskampanjene. Angrepene tar også i bruk løsepengevirus og annen skadevare i en mer målrettet form enn vi har sett de brukt tidligere.

En konsekvens av dette er flere større sikkerhetshendelser med potensielt større innvirkning på organisasjonen enn de mer generiske angrepene. De kan også være vanskeligere å detektere da de er skreddersydd for det spesifikke målet angriperen ønsker å oppnå. Selv om slike tunge, målrettede angrep for det meste er observert blant større organisasjoner og selskaper, ser vi ikke bort ifra at når angrepsmetoden utvikler seg vil den også bli benyttet for å gå etter mindre virksomheter.

Vi observerer at organisasjoner sakte, men sikkert endrer tankesettet sitt fra å forsøke å forhindre alle angrep til å akseptere at noen angrep vil kunne tre gjennom preventive sikkerhetskontroller. Som en del av dette ser vi at flere organisasjoner forbereder seg for slike situasjoner ved å forbedre hvordan de detekterer trusler, etablerer rutiner for hendelseshåndtering og generelt har en mer balansert tilnærming til preventive og responsive sikkerhetsstrategier.

Dette skiftet skyldes en rekke faktorer. Vi kan spekulere i at én faktor er nye reguleringer, inkludert GDPR og NIS-direktivet, som krever at organisasjoner har mer kontroll på sine data og systemer. Dette tvinger organisasjoner til å i det minste dis-

7. Risikobildet/trender

kutere og evaluere ulike informasjonssikkerhetssituasjoner. En annen faktor kan være at media nærmest daglig rapporterer om nye datainnbrudd og lekkasjer, og dermed gjør folk flest mer oppmerksom på IT-sikkerhet. Mediedekningen, som i flere tilfeller inkluderer kjente merkenavn og organisasjoner, samt flere rapporterte datainnbrudd og lekkasjer kan ha bidratt til at flere venner seg til tanken på at dette også vil kunne skje dem. Det kan også forklares ved at bransjen modnes og har utviklet seg over tid.

Selv om endringen skjer sakte er den mulig å observere gjennom de samarbeidene og diskusjonene vi har med bransjen, samt gjennom forespørslene vi mottar. Dette tror vi er et skritt i riktig retning.

Nordic Financial CERT – NFCERT

NFCERT er de norske, og etter hvert de nordiske, bankenes samarbeidsprosjekt, som har blitt en egen enhet - finansnæringens «brannkorps» mot internettkriminalitet i Norden.

NFCERT tilbyr en lukket kommunikasjonsplattform mellom de deltakende finansinstitusjonene slik at de kan varsle hverandre om data- og svindelangrep og utveksle erfaringer.

Oppsummert, basert på observasjoner fra operasjonelle hendelser og annen erfaringsbasert informasjon fra deltakerne, er det innen disse områdene trusselbildet er størst:

- Mobil- og nettbankbedrageri
- Tjenestenektangrep (DDoS)
- Målrettede angrep/datainnbrudd
- Svindel via e-post (inkl. phishing og malware)
- Løsepengevirus
- Kjente sårbarheter

Bank- og finansnæringen er under jevnlig og målrettet angrep innen områdene nevnt over. Angrepene har sitt utspring fra forskjellige internasjonale eller lokale grupperinger og varierer i styrke og frekvens. Det kan være at angrepene avtar eller tidvis stopper helt opp etter at f.eks. Europol arresterer individer med tiknytning til en spesiell gruppering kriminelle, men vi ser så at aktiviteten da ofte starter opp igjen etter et tidsrom på noen måneder etter en slik arrestasjon.

Trusselaktørene spenner bredt - fra rene amatører med begrenset gjennomføringsevne, via hackergrupper og organiserte kriminelle, til nasjonalt statsstøttede organisasjoner der sistnevnte aktør besitter stor kunnskap og høy motivasjon for å kunne utføre forskjellige typer angrep.

Store hendelser i 2017 viser med all tydelighet at finanssektoren ikke er immun. Stjålet kredittkortinformasjon blir jevnlig solgt på «Det mørke nettet», og etter avsløringen av at det amerikanske kredittvurderingsselskapet Equifax var utsatt for et datainnbrudd der data for opptil 146 millioner kunder ble kompromittert, reagerte aksjemarkedet ved å sende aksjene ned 33 prosent.

NFCERT så en relativt rolig slutt på året 2017 selv om vi har sett økt interesse og fokus fra trusselaktørene, og da spesielt rundt skadevare på mobile enheter. Dette er en trend som har økt i omfang inn i 2018, og det må påregnes at det vil være fortsatt fokus på dette området i tiden fremover. Finansinstitusjonene i Norden ligger inne som mål i ondsinnet programvare, og utviklingen av angrep og svindel er økende. I Norden har det ikke vært nye malwarebaserte angrep på banktjenester på en god stund, men nå er det mer skadelig programvare for salg på «det mørke nett» for både Android- og PC-plattformer, og vi tror vi vil se en økning i malwarebaserte angrep igjen utover året.

En annen bekymring er økningen i sårbarheter i maskinvare (ref. Meltdown og Spectre på de mest utbredte prosessorene) som kan utnyttes i bedriftens interne systemer. Patching eller utskifting av

sårbart utstyr tar vanligvis svært lang tid og gir trusselaktørene god tid til å utvikle verktøy for å utnytte denne type sårbarheter.

I begynnelsen av 2018 var det mer aktivitet mot banktjenester enn vi har sett på en stund. Phishing-kampanjene har fortsatt, og det er flere varianter malware direkte rettet mot finansinstitusjoner. Avanserte aktører har også vært aktive i Norden med målrettede angrep mot finansinstitusjonene ved å sende spam/e-post med ondsinnede vedlegg.

Inn i 2018 ser vi nå en økning i CEO- svindel igjen etter at trenden har vært nedadgående det siste halve året.

På den positive siden har det vært en relativt bratt nedgang i spredning av løsepengevirus ved inngangen til 2018. Det sier at det globale volumet av løsepengevirus er ned med mer enn 30 prosent sammenlignet med tidligere år. Vi har observert en betydelig reduksjon i aktiviteten fra våre medlemmer med saker som involverer løsepengevirus, noe som i praksis bekrefter den nedadgående trenden.

Mange virksomheter har lav oppdagelsesevne, og liten kunnskap om de økonomiske tapene ved en hendelse.

8. Mørketall

I dette kapitlet har vi innhentet beskrivelser og erfaringer om digital kriminalitet fra ulike virksomheter. Dette gir et bilde av hva de selv har blitt utsatt for, og hva de ser at andre blir utsatt for av ulik digital kriminalitet. Sett opp mot antallet hendelser som blir anmeldt, blir mørketallene store.

8. Mørketall

Erfaringer fra Kripos

Grunnen til at det er få hendelser som anmeldes til politiet kan bero på flere faktorer, både internt i virksomheten og eksternt. En intern faktor kan være bevisstheten rundt hva som er å anse som en kriminell hendelse som bør anmeldes.

Eksterne faktorer kan være omstendighetene rundt det å inngi anmeldelse. Slik mottak av anmeldelser er i dag så kan det for noen virksomheter fremstå som tungvint, noe som medfører at de ikke prioriterer å anmelde hendelsene. Ved tilgjengeliggjøring av anmeldelse på internett vil man kunne minske terskelen for at virksomheter anmelder hendelser. Man kan også legge til rette for å kunne laste opp filer som er relevante for saken i samme manøver som utfylling av anmeldelsen, slik at saken raskt belyses så godt som mulig. Man har fra Kripos sin side laget et veiledningsskjema for anmeldelse av datakriminalitet for å forenkle prosessen for både fornærmede og politiet. Dette skjemaet og informasjon om datakriminalitet ligger tilgjengelig på politiets internettsider.

Det virker å være en oppfatning blant en del virksomheter at politiet ikke har ressurser til å etterforske datakriminalitet, eller at en anmeldelse vil kunne medføre mye merarbeid for virksomheten. Politiet har de senere årene ved flere anledninger etterforsket og iretteført datakrimsaker hvor man har oppnådd gode dommer innen flere datakrimtyper. Samspillet mellom den fornærmede virksomhet og politiet har vært helt nødvendig for at man har kommet i mål med et godt resultat. Etter hvert som de kriminelle øker sin tekniske kompetanse vil det fordre at politiet og næringslivet spiller hverandre gode. Det er derfor fordelaktig hvis virksomhetene ser på det eventuelle merarbeidet som en del av sitt samfunnsansvar, for å være med på å spille politiet gode i bekjempelsen av datakriminalitet.

For at virksomhetene skal kunne lage gode mottiltak er man avhengig av å ha kunnskap både om den kriminelle og teknologien. Mange av kategoriene innenfor datakriminalitet genererer mange hendelser som igjen kunne medført mange anmeldelser fra næringslivet. Ved et godt samspill og regelmessig dialog kan politiet skaffe seg en god oversikt over det totale omfanget samtidig som man legger ned ressurser på saker hvor man har økt sjanse for å komme i mål og øke kunnskapen både om de kriminelle og teknologien. Noe som igjen kan fordre gode mottiltak som virksomhetene kan iverksette. Kripos har samarbeid med flere aktører som knytter politiet nærmere næringslivet samtidig som politidistriktene har egne næringslivskontakter. En fremtidig utfordring kan være å bli bedre på informasjonsutveksling mellom politiet og næringslivet så man får en økt kunnskap om datakriminaliteten og får flere gode resultater i rettssystemet.

Datakriminalitet er ressurskrevende å etterforske, og ved økt antall saker vil man få et større ressursuttak. Politiet tar datakriminalitet på alvor og vil at det skal bli en større del av porteføljen enn tidligere. Det vises ved etableringen av NC3, i tillegg til at hvert politidistrikt nå har etablert egen seksjon for digitalt politiarbeid. Politiet kan derimot forbedre sin formidlingsevne til næringslivet vedrørende hvilke kapasiteter man har innen datakriminalitet og hvilke resultater man tidligere har oppnådd. Dette for å gi økt motivasjon til at næringslivet prioriterer å anmelde en hendelse. Det skal også legges til at politiet ønsker å informere publikum om trusler og utfordringer innen IKT-kriminalitet, senest ved rapport publisert på politi.no i desember 2017.

Erfaringer fra Visma

Visma er en leverandør av programvare, outsourcingstjenester, innkjøpsløsninger, innfordringstjenester, butikkdataløsninger, samt IT-relatert utviklings- og konsulentvirksomhet.

Dagens angrepsmønstre mot våre tjenester er sammensatt. Det som Visma anser som "normal bakgrunnsstøy" er f.eks. Nasjonalstaters endeløse leting etter kjente sårbarheter, organisert kriminalitet og liknende aktiviteter fra hacktivister, frittstående "script kiddies" og andre som kjeder seg. Disse er stort sett automatiserte skanninger som har varierende avansert teknisk grad.

Det antallet som er normert for én av Vismas tjenester (Website/Webshop) er omlag 800.000 uregelmessigheter pr mnd. Dette kan sammenliknes med en "ukjent person" som tester døra utenfor huset for å se om den er åpen eller låst.

Vismas analyser viser at 6-10 av disse er såpass avanserte eller målrettet at de fremstår som et "forsøk på innbrudd", "forsøk på svindel" eller "forsøk på industrispionasje evt. nasjonalstaters forsøk på spionasje mot Visma eller deres kunder".

Visma leverer ca. 300 ulike tjenester, så dersom man anslår at angrepsraten og forsøkene på ulik kriminell aktivitet er lik for alle tjenestene, ville dette gitt grunnlag for mellom 1800 – 3000 anmeldelser pr. måned.

Mønsteret vi ser er at det er stor variasjon i hvor avanserte angrepene er. De beste angriperne ligger langt fremme teknisk og utfordrer vår evne til å "kjøpe sikkerhet" ved å kontinuerlig investere mer og mer for å beskytte tjenestene.

For Vismas minste kunder (de som driver sin egen frisørsalong, gatekjøkken, verksted, elektriker, rørlegger osv.) så har de sannsynligvis ikke kompetansen eller tid til å drive med like avansert sikringsarbeid som en stor tjenesteleverandør vil ha.

De beregninger som Visma har gjort er med utgangspunkt i Visma som fornærmet. Dersom man hadde regnet med Vismas kunder, så hadde tallet blitt enda større.

Erfaringer fra Nordea

Nordeas kunder utsettes daglig, i likhet med resten av Norges innbyggere, for ulike typer av svindelforsøk. Forsøkene går i bølger, noen ganger mer og noen ganger mindre, og vi vet at jo flere som faller for svindelen, desto større er risikoen for at svindelen øker i omfang. I vårt daglige arbeid støter vi på mørketallskomplikasjoner daglig. I stort så påvirker det Nordea på den måten at vi faktisk fullt ut vet hvordan risikobildet ser ut. Vi fører statistikk over de angrep vi vet om, både på norsk og nordisk nivå. Men vi vet ikke hvor stor andel av våre kunder som faktisk rapporterer svindelforsøk, eller fullbyrdet svindel (som har resultert i tap for privatpersoner og/eller virksomheter).

Vi jobber ut fra det vi ser, men ønsker et tydeligere virkelighetsbilde. I Norge i 2018 har vi sett mest investeringssvindel, kjærlighetssvindel og på tredjeplass, fakturasvindel. Dette er basert på den statistikk vi har registret, uten hensyn til eventuelle mørketall. Vi har sett dobbelt så mange investeringssvindler som kjærlighetssvindler i 2018, og ca. dobbelt så mange kjærlighetssvindler som fakturasvindler.

Direktørsvindel, i likhet med samtlige svindelmetoder, bærer med seg en følelse av skam. Vi vet om mange forsøk og vi vet om virksomheter som har tapt penger, men vi får også høre om virksomheter som verken rapporterer om forsøk på eller fullbyrdede Direktørsvindler. Når en virksomhet taper penger på grunn av Direktørsvindel, sier det en del om virksomhetens interne rutiner, rapporteringsregler og betalingsoppdrag, og man kan få en følelse av at de ansatte ikke vet hvordan de skal forholde seg i slike situasjoner. Dette gir en antagelse av at virksomheten ikke ønsker å

8. Mørketall

dele sin erfaring med svindel fordi man ikke er fornøyd med hvordan dette ble håndtert internt.

Om alle, både privatpersoner og virksomheter, la denne følelsen av å mislykkes til side, hadde vi sammen kunnet lære av hverandres feil og stått sterkere mot svindlerne.

Erfaringer fra Coop

Coop opplever, i likhet med mange andre større aktører innen detaljhandel, at merkenavn misbrukes i phishing-kampanjer. Phishing-kampanjene kommer i bølger og er i all hovedsak rettet mot kunder – uavhengig av deres kunderelasjon til Coop. Kampanjene utføres både via e-post og SMS, og formålet er alltid å innhente personopplysninger eller å lure mottaker til å utføre banktransaksjoner som beriker svindelaktøren. Utformingen på kampanjene utnytter bevisst mottakers tillitsforhold til Coop for å nå dette målet.

Coop har aktivt jobbet med å bygge opp kompetanse blant egne ansatte for å håndtere denne type svindelforsøk. En sentralt opprettet sikkerhetsgruppe i Coop er opprettet for å håndtere sikkerhetshendelser, samt å bidra til bevisstgjøring om datasikkerhet blant egne ansatte. Denne gruppen samarbeider med kundesentrene for å håndtere henvendelser fra butikker og kunder. Henvendelsene loggføres i eget sakssystem av kundesentrene, og sikkerhetsavdelingen følger opp disse. Dette gjør sikkerhetsavdelingen i stand til raskt å identifisere og skille de ulike svindelkampanjene. Rutiner for å forsøke å ta ned svindelsider er etablert, samt å anmelde svindelkampanjer som misbruker Coops merkenavn til politiet. Rutiner for tilbakemelding til kundesentre og informasjon til kundene om pågående svindelkampanjer bidrar til å begrense skadeomfang, samt å engasjere de som utsettes for svindelforsøk til å fortsette å melde inn nye forsøk på svindel.

Coop jobber for å etablere mer samarbeid med andre virksomheter som utsettes for det samme, slik at man mer effektivt kan samhandle mot svindelaktørene. Inntrykket er at svindelaktørene i lang tid har kunnet operere uten større risiko for å bli tatt. Samarbeid og kompetanseutveksling mellom politi og samarbeidende virksomheter vil kunne endre dette. Datakriminalitet er ikke begrenset av landegrenser, og den enkelte virksomhet har ofte begrenset mulighet til å identifisere og forfølge svindelaktører med base i utlandet. Politiets respons på anmeldelser og deres evne til å agere mot svindelaktørene vil være svært viktig for engasjementet i virksomhetene.

Erfaringer fra Telenor

I Etterretningstjenestens trusselvurdering FOKUS 2018 fremheves fremmede staters bruk av digitale kanaler som den største etterretningstrusselen mot Norge. Statlige aktører, kontraktører, organiserte kriminelle og politisk motiverte hacktivister driver operasjoner mot, eller i, vår infrastruktur og våre tjenester. Telenor Norge opplever at trusselaktørene blir stadig mer avanserte og utholdende. Dette gjelder både de kriminelle miljøene og de statlige aktørene. Avanserte aktører med økonomisk vinning som intensjon har blitt mer målrettet og fått tilgang på mer avanserte verktøy. Telenor Norge opplever også at trusselaktører ønsker å utnytte aktører på innsiden for å oppnå sine mål.

Telenor Norge er et attraktivt mål for avanserte aktører på grunn av vår samfunnskritiske infrastruktur, vår nasjonale symbolverdi og våre kunder fra alle bransjer og sektorer.

9. Forebyggende aktiviteter/tiltak

Gode forebyggende aktiviteter og tiltak bidrar til redusert sårbarhet og reduserte konsekvenser. Vi har derfor innhentet gode råd og veiledninger fra ulike aktører.

9. Forebyggende aktiviteter/tiltak

9.1 Digital sikkerhetskultur

Samfunnets evne til egenbeskyttelse er avhengig av at både offentlige og private virksomheter har tilstrekkelig digital sikkerhetskompetanse. Samfunnet forventer at den enkelte virksomhet skal klare å beskytte seg selv, og bidra til å beskytte andre. Det betyr at alle må vite hva man skal gjøre, og hva man ikke skal gjøre. Dette er enklere sagt enn gjort, for kompleksiteten øker og stadig nye områder digitaliseres. Regjeringen legger til rette for en langsiktig oppbygging av digital sikkerhetskompetanse gjennom en nasjonal kompetansestrategi for IKT-sikkerhet. Slik skal det legges et grunnlag for at den oppvoksende generasjonen har med seg IKT-sikkerhetskompetanse inn i det videre utdanningsløpet og senere i arbeidslivet.

I denne undersøkelsen er phishing og sosial manipulering de vanligste informasjonssikkerhetshendelsene, og det er mer enn en dobling av antallet siden 2016. Nå en spør om årsakene til at hendelser skjer, er de fire mest vanlige årsakene tilfeldigheter og uflaks, menneskelige feil, mangel på sikkerhetsbevissthet hos de ansatte og at eksisterende prosesser ikke blir fulgt. NorSIS anbefaler at grundig opplæring og trening i digital sikkerhet vil både forebygge slike hendelser og sørge for at konsekvensene blir mindre når hendelsen er et faktum.

- Sørg for at medarbeiderne får opplæring i virksomhetens sikkerhetsrutiner med et spesielt fokus på å motstå sosial manipulering og svindel.
- Styrk medarbeideres sikkerhetskunnskap, eksempelvis ved hjelp av opplæringspakker fra NorSIS og intern trening. Nasjonal sikkerhetsmåned arrangeres hver oktober og kan brukes til å gi medarbeidere innsikt i trusselbildet og hvordan de ved å følge virksomhetens sikkerhetsprosesser kan minske faren for uønskede hendelser.
- Kartlegg virksomhetens digitale sikkerhetskultur for å avdekke om det er behov for å igangsette tiltak.
- Økonomimedarbeidere bør få opplæring om direktørsvindel, og virksomheten bør innføre rutiner rundt overføringer av større beløp som gjør det vanskeligere for direktørsvindlere å lykkes.

9.2 Benytt NSMs Grunnprinsipper

Ivareta en sikker IKT-infrastruktur

For at virksomhetens ansatte skal jobbe effektivt og ha tillit til arbeidsverktøyene må informasjonssystemene kunne stoles på. Dette gjøres ved å etablere robuste systemer og tjenester, konfigurere og tilpasse maskin- og programvare og verifisere at konfigurasjonen er riktig.

Virksomheter med et fåtall ansatte kan ha nytte av å se på anbefalinger hos nettvett.no for sikring av datamaskin, mobiltelefon og nettbrett.

Ha kontroll på IKT-infrastruktur

Virksomhetens IKT-infrastruktur vil være utsatt for ytre og indre påvirkninger. Dette kan være skadelig programvare som kan skade maskiner og nettverk, eller planlagte endringer som følge av et nytt regnskapssystem som skal innføres. Det vil uansett være en del hensyn virksomheten må ta slik at informasjonssystemene opprettholder den ønskede robustheten. I tillegg til rådene i grunnprinsipp 2.4 – «Ha kontroll på IKT-infrastruktur», bør virksomheten innføre tiltak for beskyttelse mot skadevare, overvåkning og analyse av IKT-systemet og håndtering av endringer. For å undersøke om de korrekte sikkerhetsmekanismene er på plass vil det i mange tilfeller lønne seg å gjennomføre tester og øvelser hvor man forsøker å oppnå tilgang til ressurser og data som man ikke skal ha tilgang til.

Ha kontroll på virksomhetens data og tjenester
Virksomheter må ha kontroll på egne data og tjenester slik at behovet for konfidensialitet, integritet og tilgjengelighet ivaretas. Dette gjøres ved å ha kontroll på informasjonsflyten inn til og ut av virksomhetens nettverk, samt innad i eget nettverk. Data og tjenester må beskyttes både når det ligger lagret hos virksomheten, eller hos en tjenesteleverandør (se tiltak 3), og når data formidles over ulike informasjonskanaler. E-post og nettleser bør ha et særskilt fokus da mange av truslene (skadevare som kryptovirus, phishing-forsøk, direktørsvindel osv.) fra Internett kommer inn via disse kanalene. Se også NSM veileder «Grunnleggende tiltak for sikring av e-post».

Kontroller tilgang til data og tjenester
Tilgangen til virksomhetens data og tjenester må kontrolleres slik at det ikke blir misbrukt av uvedkommende. Dette gjøres ved å ha kontroll på kontoer, kontrollere bruk av administrative privilegier, sørge for sikker pålogging, f.eks. med «To-faktor autentisering» og etablere hensiktsmessig logging.

9.3 Sikkerhetsfaglige anbefalinger for tjenesteutsetting

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester. Tilgang til ekspertkompetanse og verktøy man ikke selv besitter kan bedres, kostnader kan bli lavere og mer forutsigbare og det kan i større grad bidra til bedre fokus på virksomhetens kjerneaktivitet. Samtidig må virksomheter være bevisst hvilken risiko en tjenesteutsetting medfører. Tilsvarende eller høyere nivå på både tjenestekvalitet og IKT-sikkerhet bør være en målsetning ved tjenesteutsetting.

En tjenesteutsetting stiller store krav til egen virksomhet og krever annen kompetanse enn om tjenesten leveres av egen organisasjon. Før det foretas en strategisk beslutning om bruk av tjenesteutsetting bør virksomheten vurdere om den er «rigget» for å håndtere alle faser i en tjenesteutsettingsprosess. Virksomheten må også kartlegge hvilke lover, krav og regler som gjelder både nasjonalt og internasjonalt. Eksempelvis gir både Sikkerhetsloven og Personopplysningsloven med forskrifter føringer ved tjenesteutsetting. Noen sektorer har også regulert hvilke muligheter virksomheten har til å tjenesteutsette.

For å ivareta IKT-sikkerheten ved tjenesteutsetting, anbefaler NSM at virksomheten er bevisst behovet for:

- Oversikt og kontroll på hele livsløpet
- God bestillerkompetanse
- Gode risikovurderinger for å kunne ta riktig beslutning
- Riktige og gode krav til ikt-tjenesten og til leverandør
- Riktig beslutning på riktig nivå

I dagens digitaliserte samfunn vil bortfall av IKT-tjenester som oftest påvirke hele eller store deler av virksomheten. Settes virksomhetskritiske tjenester ut til en tredjepart, kan det øke risikoen for både tilsiktede og utilsiktede hendelser som for eksempel bortfall av tjeneste eller tap/endring av data.

Beslutningen om tjenesteutsetting bør ikke utelukkende tas av virksomhetens IKT-miljø alene. Valg av leverandørmodell og tjenesteutsetting av IKT-tjenester er en viktig strategisk del av virksomhetsstyringen. Virksomhetens leder bør sørge for en godt forankret prosess for alle berørte parter i virksomheten. Når en beslutning om tjenesteutsetting tas, bør den baseres på risikovurderinger som beskriver tjenesteutsettingens påvirkning på hele virksomheten, herunder leveranseevne, IKT-portefølje, økonomi og behov for kompetanse.

9. Forebyggende aktiviteter/tiltak

9.4 Personvernforordningen (GDPR)

Datatilsynets råd til virksomheter:

- Kartlegg hvilke personopplysninger dere behandler, og sørg for at behandlingen dere gjør er lovlig, gjennom bl.a. å dokumentere formål og etterleve slettekrav.

- Etabler internkontroll eller styringssystem for å ivareta deres plikter og de registrertes rettigheter (som f.eks. å gi informasjon, innsyn, rette og slette opplysninger).

- Gjennomfør risikovurdering av personopplysningene dere behandler og sørg for å sikre opplysningene tilstrekkelig både med tekniske og organisatoriske tiltak. Her må man sikre konfidensialitet, integritet, tilgjengelighet og robusthet. Man må for eksempel både sikre seg mot at uvedkommende får tilgang til å se, endre og ødelegge data, samt mot hendelser som er forårsaket av uhell, menneskelig svikt og manglende rutiner. Noen basistiltak er å etablere tilgangsstyring, slå på tofaktor-
- autentisering der det er mulig, kryptere kommunikasjonskanaler og enkeltfiler, holde systemer og programvare oppdatert, og innarbeide kultur for personvern og informasjonssikkerhet.

- Dersom man outsourcer systemer eller tar i bruk tjenester der en leverandør er databehandler, er virksomheten fortsatt ansvarlig for personopplysningene man behandler. Dette innebærer blant annet at man vet hvor data fysisk er lagret, gjør risikovurdering av leverandør, etablerer databehandleravtale, og gjennomfører sikkerhetsrevisjon av leverandøren.

- Etabler rutiner for blant annet å evne å gjenopprette normaltilstand ved hendelser, samt prosess for å teste, analysere og vurdere sikkerhetstiltakene.

- Etabler rutiner for hendelseshåndtering, det vil si rutiner for å oppdage og håndtere hendelser, avgjøre om personopplysninger er omfattet av hendelsen og om Datatilsynet skal varsles, samt om man må informere personene som er omfattet av hendelsen.

Les mer om de nye personvernreglene, internkontroll og avvikshåndtering på datatilsynet.no.

9.5 Sikring av nettsider og e-post

I takt med at internett blir en stadig mer kritisk del av samfunnets infrastruktur blir det viktigere og viktigere å sikre at informasjon ikke forfalskes eller havner hos feil mottaker. Bak kryptiske forkortelser som DNSSEC, SPF, DKIM og DMARC skjuler det seg muligheter til å sørge for sikrere kommunikasjon på nettet. DNSSEC (DNS Security Extensions) er en sikkerhetsmekanisme som legges inn i domenenavnsystemet. Med DNSSEC signeres svarene på et domeneoppslag på en slik måte at det er mulig å kontrollere at de kommer fra riktig kilde og ikke er endret underveis.[3)]

Hvorfor er DNSSEC viktig?

I dagens samfunn er internett en viktig plattform for verdiskaping. I 2017 ble det omsatt for over tjue milliarder kroner via nettbutikker i Norge (kilde: SSB). Fem prosent av alle norske domenenavn som har en nettside har en handlekurvfunksjon knyttet til siden, og for mange bedrifter er nettet den primære salgskanalen. Internett er også primær kanal for kommunikasjon mellom det offentlige og innbyggere og bedrifter, for eksempel for å rapportere inn selvangivelse og arbeidsgiveravgift, og for tilgang til offentlige tjenester. I alle disse tilfellene er det svært viktig at brukerne faktisk kommer til den nettsiden de mente å nå.

Du kan hente opp en nettside på ulike måter: Gjennom å klikke på en lenke, fra en app, via treff fra en søkemotor, eller ved å taste inn adressen

3) Les mer på: https://www.norid.no/no/dns/dette-er-dnssec/

i en nettleser. I alle disse tilfellene slår du opp et domenenavn. Oppslaget setter i gang et søk etter en IP-adresse som brukes til å kontakte den maskinen som driver den tjenesten brukeren ønsker tilgang til. Opprinnelig var ikke domenenavnsystemet laget slik at det sikret at svaret på et oppslag faktisk kom fra riktig kilde. Det betyr at det er mulig for en angriper å forfalske svar og sende en bruker til en annen IP-adresse enn den som egentlig er knyttet til domenet. For eksempel kan en bruker bli sendt til en nettside som ser ut som den nettbutikken hun eller han mente å gå til, men som er et nettsted som ligger på en maskin som kontrolleres av en svindler.

DNSSEC (DNS Security Extensions) er en sikkerhetsmekanisme som tilbyr en løsning på dette problemet. Når et domene er sikret med DNSSEC vil alle svar på domeneoppslag være signert kryptografisk. Dette gjør det mulig å kontrollere både at svaret kommer fra riktig kilde og at det ikke er endret underveis.[4)]

Teknologier for sikring av e-post

SPF (Sender Policy Framework) lar deg fortelle omverdenen hvilke maskiner/systemer som har lov til å sende e-post fra ditt domene. Det du oppnår er at omverdenen kan beskytte seg mot falsk epost som ser ut som om den kommer fra ditt domene. Slik er du med på å sikre at ditt domenenavn ikke assosieres med spam. I tillegg bidrar du til et "renere" internett, siden andre kan bruke informasjonen du publiserer til å beskytte seg selv.

Tilsvarende kan din virksomhet bruke SPF-informasjon andre publiserer til å sjekke at en e-post kommer fra den avsenderen som er oppgitt. Kontroll av SPF settes opp på det mottakende e-postkontoret for ditt domene, og man kan bruke informasjonen til enten å avvise e-post eller til å merke den slik at den f.eks. kan sendes til sterkere viruskontroll.

DKIM (DomainKeys Identifiserte Mail) lar en avsender signere en e-post kryptografisk med offentlig nøkkelteknologi, der den offentlige nøkkelen publiseres i domenenavnsystemet som DKIM-informasjon. Signeringen gjøres vanligvis av e-postkontoret til virksomheten og er dermed «usynlig» for brukerne.

Mottaker sitt e-postkontor kan bruke den offentlige nøkkelen til sender for å verifisere at e-posten kommer fra noen som har kontroll over domenenavnet som er brukt, og at innholdet i e-posten er uendret. Du bør vurdere å ta dette i bruk for utgående e-post fra ditt domene. Tilsvarende som for SPF hjelper du omverdenen til å unngå falske e-poster tilsynelatende sendt fra ditt domene. Ditt e-postkontor kan også settes opp til å sjekke DKIM-informasjon på innkommende e-post, noe som kan hjelpe dine brukere til å oppdage forfalskede e-poster.

DMARC (Domain basert Message Authentication) bygger på både SPF og DKIM og gir en anbefaling om hva mottakers e-postkontor bør gjøre dersom en e-post som har kommet inn feiler en av disse to sjekkene. I likhet med SPF og DKIM publiseres DMARC-informasjonen i DNS knyttet til det domenenavnet som brukes til å sende e-post. Dersom du ønsker å ta i bruk SPF, DKIM eller DMARC for ditt domene må du ta kontakt med de som driver e-postkontoret ditt slik at de kan sette det i drift.

STARTTLS er en utvidelse av protokollen for overføring av e-post mellom e-posttjenere. Den gir kryptert overføring av epost mellom e-posttjenere dersom begge e-posttjenere som snakker sammen har aktivert dette. Dette krever ingen innsats fra brukeren som sender e-post, eller krav til e-post klienten som brukes. TLS sertifikater brukes for konfidensialitetsbeskyttelse. Autentisering får man bare dersom man bruker sertifikater utstedt av en tiltrodd tredjepart.

4) Les mer og se animasjon: Slik virker DNS SEC: https://www.norid.no/no/dns/

DNSSEC bidrar også her

Både SPF, DKIM og DMARC baserer seg på at mottaker slår opp informasjon tilknyttet et domenenavn i DNS. Det er imidlertid mulig for svindlere å forfalske disse svarene og dermed lure en mottaker til å akseptere falsk e-post.

Når et domene er sikret med DNSSEC, vil imidlertid alle svar på domeneoppslag være signert kryptografisk. Dette gjør det mulig å kontrollere både at svaret kommer fra riktig kilde og at det ikke er endret underveis. Å signere domenenavnet vil dermed være nyttig, selv om man bare bruker domenet til e-post.

Å signere domenenavnet er gratis, men informasjonen må registreres av Norid i tillegg. Selve signeringen og kontakten med Norid er det virksomhetens domeneforhandler som tar seg av.

Forebyggende aktiviteter og tiltak bidrar til å redusere konsekvensene av hendelser.

10. Etterord

I årets undersøkelse er et av de mest positive og viktige funnene at det å ha styringssystemer og drive systematisk forebyggende sikkerhetsarbeid er det som gir virksomhetene bedre oppdagelsesevne. I tillegg gir det rom for å iverksette riktige og konsekvensreduserende tiltak. Dette er verdifull kunnskap for et digitalt samfunn som sammen må jobbe kontinuerlig mot et trusselbilde som blir stadig mer avansert, omfattende og som berører oss alle uavhengig av bransje.

Samtidig viser årets undersøkelse at kunnskap er viktig for å kunne forebygge. Kunnskap som alle virksomheter uansett størrelse bør få tilgang på uavhengig av geografisk plassering. Mange trenger hjelp til å omsette kunnskap til tiltak i egne virksomheter. Vi trenger derfor fremdeles arenaer for nettopp det å dele oppdatert kunnskap og erfaringer som samlet vil kunne bidra til et mer robust digitalt samfunn. Vi trenger oppdaterte og relevante veiledninger, råd og mulighet for støtte fra de respektive myndigheter ved cyberhendelser.

Erfaringer og kunnskap er også viktig for økt risikoforståelse. Jo mer bevisste landets virksomheter og ansatte er om dagens risikobilde og hvordan de i henhold til det skal forvalte egne verdier, desto bedre rustet er vi til sammen å håndtere det digitale trusselbildet vi står overfor i dag og fremover. Dette er viktige byggesteiner for økt sikkerhetsforståelse og en felles digital sikkerhetskultur vi alle bør være en del av.

Vi håper derfor at årets undersøkelse kan bli brukt som et aktivt verktøy i det pågående sikkerhetsarbeidet som opptar både virksomheter og myndigheter, samt bidra til å fremme mer samarbeid innen digital sikkerhet.

Bidragsytere til undersøkelse og rapport, utover utvalget

Næringslivets sikkerhetsråd har flere samarbeidsprosjekter som pågår til enhver tid, men som alle omhandler sikkerhet på ulikt vis. Det gir oss bedre breddeforståelse, samt tilgang til ressurser og kunnskap som bidrar til høy kvalitet på våre produkter. I forbindelse med analyser knyttet til Mørketallsundersøkelsen 2018 ønsker vi derfor å takke følgende bidragsytere:

Birgitte Førsund – Senior Manager, KPMG
Ingunn Kolberg Vedeld– Associate, KPMG
Magdalena Agata Szwiec – Associate, KPMG
Espen Johansen – Operations & Security Manager, Visma Software International
Isabel Quiroga Arkvik – Fraud management, Nordea.
Hege Ossletten – Nestleder UNINETT Norid AS

Informasjonssikkerhetsutvalget

Tønnes Ingebrigtsen, Daglig leder og gründer av mnemonic. (Utvalgsleder)
Tønnes har ledet IT- og informasjonssikkerhetsselskapet mnemonic siden selskapet ble grunnlagt våren 2000. Han sitter i styret i NTNUs Center for Cyber and Information Security (CCIS), og er utvalgsleder i NSRs ekspertutvalg Informasjonssikkerhetsutvalget. Han har en master i informatikk fra NTNU.

Johnny Mathisen, seniorrådgiver Telenor Group
Johnny har en mastergrad i telematikk fra NTH i Trondheim og en i informasjonssikkerhet fra Høgskolen i Gjøvik. Han har jobbet i Telenor i over 30 år, hvorav de siste 25 med informasjonssikkerhet, og han har vært medlem av NSRs Informasjonssikkerhetsutvalg siden 2010.

Christophe Birkeland, administrerende direktør i Symantec (Norway) AS
Før han gikk over til det private næringsliv i 2011 hadde han ulike lederstillinger i det offentlige (E-Tjenesten og Nasjonal sikkerhetsmyndighet). Birkeland har en doktorgrad fra NTNU i 1997, og har også gått Forsvarets Høyskole i 2005..

Vidar Østmo, Sikkerhetsarkitekt/CISO, Verdipapirsentralen ASA
Vidar er CISSP og GCIH sertifisert og har mange års erfaring innen arbeid med informasjonssikkerhet både innen Telecom og Finans. Han har erfaring fra både tekniske og ikke tekniske sider ved sikkerhetsarbeidet.

Martha Eike, fagdirektør i Datatilsynet
Martha er utdannet dataingeniør med bakgrunn fra programvareutvikling i privat sektor Hun har jobbet i Datatilsynet siden 2012 og har erfaring med innebygd personvern, DPIA, skytjenester, digitalisering av offentlig sektor, opplæringssektoren og Big Data. Martha koordinerer det utadrettede arbeidet med informasjonssikkerhet.

Peggy Heie, administrerende direktør i NorSIS
Peggy er utdannet siviløkonom med spesialisering innen informasjonsledelse. Hun er også CISA og CRISC sertifisert fra ISACA. Peggy har siden 1998 jobbet med ulike oppgaver innen risikostyring, bedriftsutvikling, IT-revisjon, finansiell revisjon og informasjonssikkerhet.

Bente Hoff, fungerende avdelingsdirektør Nasjonalt cybersikkerhetssenter, Nasjonal sikkerhetsmyndighet
Bente har mer enn tjue års erfaring med digitalisering og cybersikkerhet i både privat og offentlig sektor. Hun er sivilingeniør fra NTH og har en mastergrad i teknologiledelse.

John Arild A. Johansen, Informasjonssikkerhetsansvarlig (CISO) og Personvernombud (DPO), Gjensidige Bank
John Arild har mer enn 25 års erfaring innen området fra både offentlig og privat sektor, har vært mangeårig Styreleder og styremedlem i Norsk Informasjonssikkerhetsforum (www.isf.no), Norm for informasjonssikkerhet helse og omsorgstjenesten (Normen.no) og jobber for tiden som sikkerhetsleder og personvernombud i Gjensidige Bank.

Ole Tom Seierstad, National Security Offiser, Microsoft Norge
Ole Tom har jobbet i Microsoft siden 1990 og har hatt flere ulike roller. De siste årene har han fokusert på sikkerhet og problemstillinger rundt dette. Ansvarsområdet inkluderer de fleste Microsoft-produkter og kontakt mot de ulike segmentene som bruker Microsoft-programvare, det være seg forbrukere eller større organisasjoner.

Anders R Hovdum, fagdirektør for samfunnssikkerhet i Statens vegvesen Vegdirektoratet
Anders er ansvarlig for å følge opp samfunnssikkerhet i Statens vegvesen, herunder informasjonssikkerhet og beredskap. Anders har lang fartstid innen sikkerhetsområdet blant annet fra Samferdselsdepartementet og Direktoratet for samfunnssikkerhet og beredskap.

Soner Sevin, CISO, COOP
Soner Sevin har lang fartstid fra Informasjonssikkerhetsområdet og har jobbet som CISO i ulike offentlige og private virksomheter. Han har opp gjennom årene jobbet på operativt, taktisk og strategisk nivå. Hans engasjement og bidrag på sikkerhetsområdet har inspirert mange i bransjen. Soner har de siste fem årene jobbet som sikkerhetssjef i Coop konsernet, hvor han blant annet har bidratt til avsløring av ulike type nettsvindelkampanjer i tillegg til å etablere en operativ CSIRT enhet i Coop.

Bjørn R. Watne, CISO, Storebrand ASA
Watne har jobbet med informasjonssikkerhet siden tusenårsskiftet, og siden 2014 som sikkerhetssjef i Storebrandkonsernet. Han sitter i styret for ISACA Norge – en interesseforening for profesjonelle innen IT-revisjon og -sikkerhet, og er i tillegg også engasjert i faggrupper hos Den Norske Dataforening, Norsk Informasjonssikkerhetsforum og Cloud Security Alliance. Av utdannelse er han ingeniør innen Datateknikk, og har en MBA fra ESCP i Paris.

Rune Rudi, Politioverbetjent, Seksjon for datakriminalitet, Kripos
Rune jobber med datakriminalitet på Kripos og har bred erfaring som etterforsker, men han har de siste årene jobbet med etterretning innen cyber. Han har tidligere bakgrunn fra Forsvaret og privat sikkerhetsbransje.

Arne Røed Simonsen, seniorrådgiver i Næringslivets Sikkerhetsråd (utvalgssekretær)
Arne har vært ansatt i NSR siden 2004, han har bakgrunn fra både Forsvaret og politiet. Han var ansatt ved Etterforskningsseksjonen i Kripos før han ble ansatt i NSR.

www.nsr-org.no

Mot kriminalitet - for næringsliv og samfunn