



ÅRSRAPPORT 2019

Norsk senter for
informasjonssikring

Innhold

1

Innledning | 4-6

2

Fakta om NorSIS | 7

3

Mål strategi og verdigrunnlag | 8-9

4

Strategisatsinger | 10

5

Aktiviteter og resultater | 11-19

6

Rapporter | 21-21

7

Formidling | 22-23

8

Målsetninger og konkrete resultater | 24



Regnskap | 25

1 Økt frykt for digitalisering løses med mer kunnskap og opplæring



Administrerende direktør i NorSIS,
Peggy Sandbekken Heie

Samtidig som stadig flere tjenester blir digitale, tyder NorSIS' undersøkelser på at frykten for å ta dem i bruk øker. Det har aldri vært viktigere med uavhengig kunnskap og opplæring enn det er akkurat nå.

Økt medieoppmerksomhet, stadig flere besøk på våre nettsteder og rekordmange foredrag viser med all tydelighet at det er behov for en uavhengig aktør som NorSIS.

For fjerde år på rad ga vi med støtte fra Justis- og beredskapsdepartementet i september ut rapporten «Nordmenn og digital sikkerhetskultur». Rapporten viser at vi fremdeles ikke er godt nok rustet til å beskytte oss mot de risikoene som et stadig mer digitalt samfunn representerer. Uavhengig av om det er passordbruk, ukritisk åpning av e-poster eller

ID-tyveri har vi fremdeles en vei å gå før vi kan si oss fornøyde. Samtidig viser undersøkelsen at vi opplever mer frykt når vi bruker nettbanken eller deler personopplysninger med det offentlige.

Kunnskap og opplæring reduserer frykten

NorSIS tror at dette handler om noe så enkelt som manglende kunnskap. Når vi vet mer om det vi frykter, er sjansen større for at vi sikrer oss bedre. Det høres vanskeligere ut enn det er. Vårt

inntrykk er at det har spredd seg en holdning om at det er vanskelig og nærmest en heldagsjobb å sikre seg tilstrekkelig mot stadig nye trusler. Slik er det heldigvis ikke. Totrinnsbekreftelse, oppdatert programvare, antivirusbeskyttelse og et mer bevisst forhold til hva vi legger igjen av opplysninger om oss selv eller vår egen bedrift digitalt er viktige tiltak som bedrer sikkerheten.

Det er helt avgjørende å øke den enkelte innbyggers kunnskap om informasjonssikkerhet. De kriminelle

«Nordmenn opplever mer frykt når vi bruker nettbanken eller deler personopplysninger med det offentlige»

som opererer i den digitale verden blir hele tiden mer profesjonelle og utspekulerte. Vi ser også en tendens til at de i økende grad angriper mennesket, ikke de stadig sikrere maskinene. For ikke å la seg lede av såkalt sosial manipulasjon er det helt avgjørende at den enkelte kan se faretegnene og gjennomskue svindelen.

Nettkurs og forståelige tips om de vanligste digitale truslene

Derfor satser NorSIS på tilrettelagte kurs rettet spesielt mot definerte grupper. Bare det siste året har vi lansert eget seniorkurs og et kurs rettet mot små og mellomstore bedrifter. Selvstudiekursene i digital sikkerhet ved bruk av internett er lagt til kursportalen på Nettvett. Her finnes det også en rekke andre veiledere med tips og råd. Bare siden 2017 har antall brukere av Nettvett.no mer enn doblet seg.

Rapporten «Trusler og trender 2019–2020» er et helt unikt verktøy for små og mellomstore bedrifter, kommuner og enkeltpersoner. Her får du oversikt over destørste digitale truslene i Norge og en enkel og forståelig oppskrift på hvordan du kan sikre deg. Rapporten fikk bred medieoppmerksomhet da den ble overrakt justisminister Monica Mæland i starten av februar i år.

Økende interesse for nasjonal dagnad

Interessen for Nasjonal sikkerhetsmåned er også et eksempel på at det er behov for enkel, tilgjengelig og uavhengig informasjon for en tryggere digital hverdag. Sammenlignet med 2018 var det langt flere virksomheter som bestilte opplæringspakken vår i 2019. Vi gjennomførte også langt flere foredrag enn i 2018. Temaene for fjorårets sikkerhetsmåned var blant annet hva en stadig mer tilkoblet verden med ny teknologi krever av oss samt hvordan du skal unngå å bli svindlet på nett. Hele 238 011 ansatte ved i alt 691 virksomheter mottok i fjor opplæringspakken.

NorSIS har hele befolkningen som målgruppe for sine råd for en tryggere digital hverdag. Samtidig har vi sterkt fokus på SMB-markedet, kommunene og den enkelte innbygger. Det sier seg selv at det må forskjellige virkemidler til for å nå så lite ensartede målgrupper. Vi har blant annet hjulpet NRK med råd og innspill til den nye ungdomsserien «Nudes», som fra de unges synsvinkel problematiserer den stadig vanligere spredningen av nakenbilder.

«Bare siden 2017 har antall brukere av Nettvett.no mer enn doblet seg»

Konferanser og kurs for både eksperter og folk flest

Samtidig som en bølge av pornosvindler og løsepengevirus skylte inn over landet på starten av året, avholdt vi sammen med Skatteetaten årets ID-konferanse. ID-tyveri er fremdeles blant de digitale truslene både virksomheter og nordmenn flest frykter mest. Ifølge vår siste undersøkelse har dette rammet så mange som 105 000 nordmenn over 18 år i løpet av de to siste årene. Selv om det er en nedgang fra tidligere år, er det fremdeles altfor mange som blir utsatt for dette.

Å være ute hos næringslivet og befolkningen for øvrig har alltid vært en sentral del av NorSIS' strategi for å gi alle en tryggere digital hverdag. I løpet av 2019 har vi gjennomført i alt 46 foredrag. Vi har også arrangert hele 12 konferanser.

143 deltakere møtte opp da vi gjennomførte årets Security Divas på Gjøvik. Dette er en viktig arena og en unik møteplass for kvinner. Målet med konferansen er å bidra til å bevare og øke andelen kvinner som jobber med informasjonssikkerhet.

«Det er helt avgjørende å øke den enkelte innbyggers kunnskap om informasjonssikkerhet. De kriminelle som opererer i den digitale verden, blir hele tiden mer profesjonelle og utspekulerte»

I tillegg har vi gjennomført Sikkerhetstoppmøte, Stopp nettsvindler-forum og Seniorkurs i 2019. NorSIS er også medarrangør av Sikkerhetsfestivalen, som ble avholdt på Lillehammer i slutten av august i fjor. Ambisjonen er at dette skal bli Norges største og viktigste sikkerhetsarrangement. Festivalen arrangeres i tett samarbeid med blant annet Nasjonal sikkerhetsmyndighet (NSM), NTNU, IKT-Norge, Difi og tidligere Oppland fylkeskommune.

Medieomtale med mer enn 100 millioner kroner i annonseverdi

Vår unike uavhengige rolle gjør NorSIS til en troverdig og uavhengig kilde i det pågående ordskiftet i mediene. I 2019 ble vi nevnt i 6 prosent flere saker enn året før. De 1489 medieoppslagene hadde ifølge Retriever en annonseverdi på hele 107 millioner kroner. Det er helt avgjørende for å nå gjennom med gode råd og tips som både befolkningen og små og mellomstore bedrifter kan vite er nettopp det, og ikke et forsøk på salg.

Fortsatt fokus på barn og unge

Barn og unge har alltid vært en viktig målgruppe for NorSIS. Vi er ofte rundt på skoler og konferanser for å prate med unge om digital sikkerhet. Gjennom Slettmeg.no hjelper vi fremdeles flest i den yngre målgruppen. I 2019 løste våre mange dyktige medarbeidere 5497 saker sendt til Slettmeg.no.

NorSIS har også i 2019 jobbet aktivt med å øke den digitale sikkerheten og dømmekraften i grunnutdanningen. For at skolen skal lykkes med å ruste elevene til å mestre livene sine og møte fremtiden, er digital kompetanse grunnleggende. Prosjektet retter seg mot lærere, elever og foreldre, og har som mål å øke de respektive målgruppens kompetanse innenfor områdene informasjonssikkerhet, digital sikkerhet, nettvett og digital dømmekraft.

«Den røde tråden i NorSIS' arbeid er å være en uavhengig ikke-kommersiell aktør som i tett samarbeid med det private og det offentlige gir alle en tryggere digital hverdag»

Egen løsning for cybervarsel

NorSIS har det siste året jobbet med en rekke forskjellige løsninger for å bli enda bedre på å gjøre befolkningen til tryggere digitale borgere. Med løsningen Cybervarsel er målet å få et «realtime»-oversiktsbilde på hendelser og statistikk i NorSIS. Løsningen, som er under utvikling, vil på sikt kunne tilbys nærmere definerte målgrupper for å informere om trusler og trender.

Mindre egeninteresse – mer samarbeid for det felles beste

I 2020 vil NorSIS prioritere arbeid knyttet til opplæring og kompetanseheving blant SMB og

innbyggerne. Vi planlegger konkrete veiledninger og andre tiltak som kan gi de minste virksomhetene og enkeltpersoner bedre evne til å beskytte egne verdier og ta del i digitale gevinster.

Den røde tråden i NorSIS' arbeid er å være en uavhengig ikke-kommersiell aktør som i tett samarbeid med det private og det offentlige gir alle en tryggere digital hverdag.

2 Fakta om NorSIS

Norsk senter for informasjonssikring (NorSIS) er en ideell og uavhengig organisasjon og medlemsforening som ble stiftet i 2010.

Virksomheten er en videreføring av Senter for informasjonssikring (SIS), som ble opprettet av Handels- og næringsdepartementet som et prøveprosjekt i 2000. I 2006 flyttet SIS til Gjøvik og ble etter hvert videreført som NorSIS, med Gjøvik kunnskapspark som operatør.

Styringsinstruks

- NorSIS mottar årlig tilsagnsbrev fra Justis- og beredskapsdepartementet med tilskudd til drift av virksomheten. Tilskuddet skal styrke informasjonssikkerheten og gjøre informasjons- og kommunikasjonsteknologien i samfunnet mindre sårbar. Tilskuddet er en del av regjeringens satsing på informasjonssikkerhet.
- NorSIS er en uavhengig og nøytral informasjonssikkerhetsinstans og skal opptre i samsvar med det. Informasjonen fra NorSIS skal være åpen og tilgjengelig for alle.
- NorSIS skal, gjennom sin uavhengige rolle, etablere og videreutvikle møteplasser og arenaer for å bygge kompetanse og erfaringer samt sette søkelys på viktige tiltak for bedre informasjonssikkerhet for målgruppen.
- NorSIS skal, som uavhengig aktør, aktivt søke samarbeid med media for å nå sine målgrupper. Senterets aktivitet skal bidra til å fremme god sikkerhetskultur hos brukere av informasjonssystemer og nettverk, blant annet gjennom bevisstgjøring av trusler og tiltak.

Drift og organisering

NorSIS har per 31. desember 2019 ni fast ansatte og en på engasjement. I tillegg er åtte studenter engasjert på deltid. Medarbeiderne har bred relevant høyere utdanning og lang erfaring innen informasjonssikkerhet, både fra privat og offentlig sektor.

NorSIS styres etter egne vedtekter og har etablert et eget styre. Fra juni 2019 består styret av:

Morten Andreas Meyer (leder),
Huseiernes Landsforbund

Bjørn Erik Thon,
Datatilsynet

Kristine Beitland,
Microsoft

Nils Kalstad,
NTNU

Heidi Austlid,
IKT-Norge

Ivar Kjærem,
NorSIS

Robin Bakke/Martin Kjellsen
(observatører), Justis- og beredskapsdepartementet

3 Mål og strategi

Målgruppe

Justis- og beredskapsdepartementet definerer NorSIS' primære målgruppe til å være norske virksomheter i privat og offentlig sektor, inklusiv kommunene. De små og mellomstore virksomhetene skal prioriteres.

NorSIS skal også vektlegge råd og veiledning til befolkningen. Erfaring viser at denne informasjonen også videreføres til de små og mellomstore virksomhetene gjennom deres ansatte. Informasjon til befolkningen er også viktig for å skape en sikkerhetskompetanse som det er behov for i den videre digitaliseringen av Norge.

Visjon

NorSIS mener at god informasjonssikkerhet bidrar til økt verdiskaping og styrker velferden.

Vår visjon er å gjøre informasjonssikkerhet til en naturlig del av hverdagen i norske styrerom, i norske virksomheter og blant befolkningen.

Strategi og virksomhetsidé

Cybertrusselen utvikler seg raskt og blir stadig mer kompleks. Digitalisering gir store økonomiske og samfunnsmessige fordeler, men åpner også for ny kriminalitet.

Stadig flere nordmenn rammes av datakriminalitet, og de økonomiske tapene er økende.

NorSIS spiller en viktig rolle i å fylle befolkningens behov for informasjon om trusler og risiko samt tiltak den enkelte selv kan iverksette.

Verdigrunnlag

Uavhengige

- Vi skal gi synspunkter, råd og veiledninger som er basert på flere kilder, og som ikke er påvirket av kommersielle interesser eller andre aktørers synspunkter eller behov.

Fremtidsrettede

- Vi skal være faglig oppdaterte, dynamiske og omstillingsvillige og ha en optimistisk holdning til ny teknologi.
- Vi skal være oppdaterte på målgruppens behov.
- Vi skal være tidlig ute med å informere om utvikling innen informasjonssikkerhetsområdet.

Troverdige

- Vi skal være imøtekommende, respektfulle, interesserte og lydhøre i vår kommunikasjon med målgruppene.
- Vi skal sette målgruppene i fokus og gi råd som er praktiske og anvendelige.
- Våre prosesser skal være transparente og tillitsskapende.
- Vi skal være åpne med hensyn til hvilke virksomheter vi samarbeider med.

Kunnskapsbaserte

- Våre avgjørelser, vurderinger, uttalelser og råd skal være forankret i faglig kunnskap, dokumentert praksis, erfaring og informasjon – fra egne og andres tjenester.

Strategiske hovedmål

NorSIS er gjennom sine vedtekter og tildelingsbrev fra Justis- og beredskapsdepartementet pålagt kjerneoppgaver som innebærer kunnskapsformidling og gjennomføring av informasjonssikkerhetstiltak i målgruppen.

NorSIS' tre strategiske hovedmål for 2018–2020

1. Posisjon

NorSIS skal være kjent som et nasjonalt og uavhengig ekspertorgan, kunnskapsforvalter og kulturutvikler innen informasjonssikkerhet.

2. Samarbeid

NorSIS skal oppleves og være anerkjent som en attraktiv og verdifull samarbeidspartner.

3. Effekt

NorSIS skal informere og dele kunnskap som skaper forståelse og påvirker adferd som gir en tryggere digital hverdag.



4 NorSIS' fem strategiske satsingsområder for 2018–2020

1. Bruke samarbeid som et strategisk virkemiddel

NorSIS skaper verdi gjennom å samarbeide med virksomheter og aktører i både offentlig og privat sektor. Samarbeid bidrar til å øke kvaliteten til og omfanget av vår formidling til målgruppene og til å sikre en stabil og forutsigbar drift av NorSIS.

2. Modernisere og videreutvikle våre tjenester

NorSIS har siden etableringen utviklet et sett med tjenester som tilbys til målgruppene. Vi skal utvikle våre tjenester slik at de er i takt med målgruppens behov og slik at vi kan levere tjenestene på en ressurseffektiv måte.

3. Øke effektiviteten i vår formidling til målgruppene

NorSIS bruker i dag svært mange forskjellige kommunikasjonskanaler og -plattformer til å formidle sine budskap til flere ulike målgrupper. Det skal i strategiperioden utvikles en helhetlig kommunikasjonsplan som omfatter alle tjenester og produkter.

4. Styrke datafangst og analyse av data fra våre tjenester og aktiviteter

NorSIS har en unik posisjon til å samle inn og nyttiggjøre seg data som samles inn fra organisasjonens tjenester og aktiviteter. Vi skal i strategiperioden systematisere dette arbeidet for å sikre at vi samler inn de riktige dataene og utnytter disse på en måte som gir høy kvalitet og effekt for de råd vi gir til våre målgrupper.

5. Effektivisere interne prosesser

NorSIS er en liten organisasjon med et stort samfunnsoppdrag. Størrelsen på organisasjonen tillater i liten grad at interne funksjoner har god nok redundans. En gjennomgang av våre interne prosesser vil kunne frigjøre kapasitet slik at våre leveranser blir styrt og fulgt opp på en mer effektiv måte.



5 Aktiviteter og resultater i 2019

En av NorSIS' strategiske oppgaver er å bidra til godt nettnett samt å gi råd til de som føler seg krenket på nett, opplever uønskede hendelser eller utsettes for datakriminalitet.

På de følgende sidene oppsummerer vi noen av våre viktigste satsinger for å oppnå dette målet og hva som er resultatet av denne innsatsen.

Nettnett.no

NorSIS har i fem år hatt både redaktøransvar og det daglige driftsansvaret for Nettnett.no. Målet med tjenesten er å bidra til sikrere bruk av internett. I løpet av to år har antall brukere av siden blitt mer enn doblet.

Nasjonal kommunikasjonsmyndighet (Nkom) og Nasjonal sikkerhetsmyndighet (NSM) er med på eiersiden, og bidrar også med innhold og utvikling. Tjenesten ble opprettet i 2005 av daværende Post- og teletilsynet (PT) på oppdrag fra regjeringen.

De siste årene har antall brukere av Nettnett.no blitt mer enn doblet – fra 147 000 i 2017 til hele 338 479 i 2019.

Målet med Nettnett.no er å bidra til sikrere bruk av internett, særlig blant innbyggerne og små og mellomstore bedrifter. NorSIS jobber med å videreutvikle og revitalisere tjenesten for å sikre at portalen fortsatt bidrar til koordinert og forbedret informasjon om sikkerhet og sikkerhetskultur. Det legges vekt på at både råd og veiledninger skal være enkle og forståelige.

Det er også et betydelig fokus på å etablere online opplæringspakker, spesielt tilrettelagt for ulike grupper og med forskjellige temaer. Bare i løpet av 2019 er det publisert tre nye kurs: «Digital sikkerhet for seniorer», «Digital sikkerhet for bedrifter» samt temakurset «Hvordan sikre din egen identitet?». Det første onlinekurset, «Sikkerhet i hverdagen», ble gjort tilgjengelig i 2018. I 2020 håper vi å kunne lansere enda flere nettbaserte opplæringsstilbud.

Nettnett.no i 2019



Antall brukere: **338 479**
 Antall sidevisninger: **635 253**
 Antall veiledninger: **>140**
 Følgere på Facebook: **2484**



130 %
 Økningen i antall brukere av
 Nettnett.no fra 2017 til 2019

Slettmeg.no

NorSIS er i sitt niende driftsår av Slettmeg.no. Tjenesten har vært under kontinuerlig utvikling, og håndterte i 2019 i underkant av 6000 henvendelser. Slettmeg.no hadde nesten 350 000 brukere i 2019.

Tjenesten har også åpningstider på telefon mandag og torsdag fra 12.00 til 17.00, kan kontaktes via kontaktskjema på hjemmesidene, per e-post eller ved bruk av Messenger i Facebook.

Behovet for bistand til å håndtere nettytringer og krenkelses samt sletting av digitalt innhold er stort. Tjenesten ivaretar alle aldersgrupper og håndterer et bredt spekter med utfordringer. Vi ser at flere løser problemene sine ved å bruke veiledningene man finner på Slettmeg.no sine nettsider.

Utviklingen med stadig mer krevende saker å håndtere fortsetter også. Dette har sammenheng med den økte bruken av mobilbaserte apper og tjenester. Spredningsmønsteret av krenkende innhold har også endret seg de siste årene. Dette krever mer av tjenesten, både når det gjelder tidsbruken per sak og behovet for videreutvikling.

Datagrunnlaget som Slettmeg.no frembringer gjennom å samle data om de ulike henvendelsene tjenesten mottar er helt unikt, og gir god innsikt i årsaken til de problemene folk møter på nett. Slettmeg.no har derfor vært brukt som kompetansekilde både hos Ung.no, Barneombudet, Facebook og i forbindelse med høringer, konferanser og foredrag.

De fleste som kontakter Slettmeg.no oppgir at de føler seg maktesløse og ofte blir en kasteball i systemet. Selv om flertallet kommer fra privatpersoner, er det også mange fra både private og offentlige virksomheter som henvender seg til Slettmeg.no for å få hjelp.

Det er kommet flere aktører som hevder at de kan hjelpe til i forbindelse med denne typen problematikk. Slettmeg.no sin erfaring er at flere av disse nærmest lover å kunne hjelpe, men at mange opplever at problemet ofte ikke er så lett å løse.

Slettmeg.no i 2019



350 000 unike brukere
Håndterte nesten **6000**
henvendelser

ID-tyveri og IDentitetskonferansen

NorSIS bidrar til å forebygge ID-tyveri og støtter enkeltpersoner og organisasjoner som har blitt utsatt for dette. I tillegg både arrangerer og deltar NorSIS i flere konferanser, forum og nettverk som jobber aktivt for å forhindre ID-tyveri. I fjor ble mer enn 100 000 nordmenn utsatt for ID-tyveri.

I 2019 ble det også lansert et eget kurs som skal gjøre befolkningen flinkere til å ha kontroll over egen identitet, både fysisk og digitalt.

Sammen med Skatteetaten arrangerte NorSIS den årlige konferansen IDentitet i februar 2019. Hele 152 påmeldte deltakere og stor medieinteresse tyder på at det er både behov og stor interesse for det som er den eneste nasjonale samlingsarenaen for å diskutere problemstillinger innen identitetsområdet. Deltakerne kom fra store deler av offentlig og privat sektor. Politidirektoratet, som tidligere har deltatt i programkomiteen, valgte å trekke seg fra samarbeidet for å konsentrere seg om egne leveranser knyttet til pass og ID.

I samarbeid med Skatteetaten gjennomfører NorSIS en årlig undersøkelse for å kartlegge omfanget av identitetstyveri i Norge. Denne ble tatt opp i desember 2019, og viser at det har vært en nedgang i antall ID-tyverier det siste året. Mens rundt 150 000 personer (tilsvarende 3,9 prosent av de spurte) tidligere har oppgitt at deres identitet har blitt misbrukt til å begå straffbare handlinger, er det nå rundt 105 000 personer som har opplevd det samme. Det er en signifikant endring.

På ID-feltet bidrar NorSIS også i nasjonalt ID-nettverk og i referansegruppen til Koordineringsgruppe for ID-forvaltning (KoID), underlagt SKATE. Dette er arenaer hvor de fleste forvaltningsenheter innen ID-området i offentlig og privat sektor deltar. Forumet ledes av Nasjonalt ID-senter og Skatteetaten. Tidligere har NorSIS poengtert behovet for en overordnet styringsenhet og strategi på feltet, på tvers av sektorer. KoID er en kjærkommen tilvekst som skal stå for en koordinering av ID-feltet. NorSIS støtter dette arbeidet og vil bidra med forbrukerperspektivet i det videre arbeidet med helhetlige rutiner for og tilnærminger til håndtering av dokument- og identitetsverifisering.

NorSIS håper også at initiativet fra Finansdepartementet om en gjennomgang av ID-området i sin helhet vil føre til gode tiltak for en bedre forvaltning.

NorSIS' engasjement for å forhindre ID-tyveri:



- Arrangerer IDentitetskonferansen årlig
- Forebygger ID-tyveri med regelmessig informasjon og et nytt nettbasert temakurs – «Hvordan sikre din egen identitet?»
- Gir råd til enkeltpersoner og virksomheter som har blitt utsatt for ID-tyveri
- Arrangerer Stopp nettsvindler-forum 2–3 ganger i året
- Deltar som aktør i Nasjonalt ID-nettverk og i referansegruppen for KoID



105 000

nordmenn har i løpet av de to siste årene opplevd at deres identitet har blitt misbrukt til å begå straffbare handlinger.

Stopp nettsvindel-forum

Stopp nettsvindel-forum drives av NorSIS med støtte fra deltakerne selv. I forumet, som ble avholdt to ganger i 2019, møtes 25–30 små og store aktører fra offentlig og privat sektor for en åpen erfaringsutveksling om svindelmetoder og tiltak for å redusere omfanget av nettsvindel.

Med en av deltakerne i forumet som vertskap, diskuteres nettsvindel i en uformell tone. Naturlige temaer er alt fra konkrete tiltak og virkemidler samt hvilke gode råd som kan gis mot en spesifikk svindelmetode, til hvilket ansvar som bør legges på den enkelte forbruker, bransjen eller myndighetene.

Nøkkelen for suksessen til forumet er en erfaringsutveksling hvor åpenhet og trygghet er gjeldende. Dette skaper grobunn for samarbeid internt i bransjer og på tvers av eksisterende skillelinjer.

Telenor, Telia, Nordea, SpareBank 1, DNB, Coop, Tryg Forsikring, Buypass, Vipps, politiet, PayEx, Finn.no, Datatilsynet, Finanstilsynet og Forbrukertilsynet er bare noen av aktørene som regelmessig deltar i forumet.

NorSIS' erfaring er at aktører i økende grad setter seg ned sammen for å se på problemstillingene som blir tatt opp i forumet. Ved bred deltakelse her får også NorSIS god innsikt i svindelhverdagen til norske virksomheter. Dette bidrar til å gi oss et riktigere situasjonsbilde som vi igjen kan bruke i tilpasningen av vårt arbeid.

Nasjonal sikkerhetsmåned

Nasjonal sikkerhetsmåned er en nasjonal dugnad for en sikrere digital hverdag for alle. I oktober ble den arrangert for niende gang. Kampanjens største volum er opplæringspakken som NorSIS har laget. I 2019 var det rekordmange norske virksomheter hvor de ansatte gjennomførte e-læringskurset i informasjonssikkerhet.

«Nasjonal sikkerhetsmåned er en nasjonal dugnad for en sikrere digital hverdag for

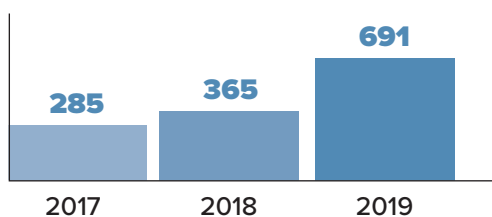
Hele 238 011 ansatte ved i alt 691 norske virksomheter mottok opplæringspakken i 2019. Det er en kraftig økning fra året før, da det tilsvarende antallet virksomheter var 365.

Opplæringspakken er gratis for alle virksomheter med under 20 ansatte. De små og mellomstore virksomhetene er også NorSIS' hovedmålgruppe.

Vi er derfor svært glade for at antallet små virksomheter som bestilte opplæringspakken hadde en såpass stor økning i 2019. 75 prosent av alle virksomhetene som deltok har 0–20 ansatte.

Nasjonal sikkerhetsmåned er en felles dugnad hvor både private og offentlige virksomheter deltar. I tillegg til opplæringspakken inneholder Nasjonal sikkerhetsmåned tilbud om en rekke foredrag og flere andre aktiviteter. Målet er at alle – både privatpersoner, bedrifter og offentlig sektor – sammen skal få den nødvendige digitale kompetansen for å møte den pågående digitaliseringen som skjer i samfunnet.

Antall virksomheter som mottok opplæringspakken 2017–2019



Mange av virksomhetene som deltar i dugnaden utarbeider også eget materiell og egne opplæringsopplegg. Det bidrar til å løfte kunnskapsnivået om informasjonssikkerhet i samfunnet. I samarbeid med nasjonale samarbeidspartnere og det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA) ble det fokusert på to temaer i 2019:

- Ny teknologi – hva betyr det for den enkelte arbeidstaker i hverdagen?
- Nettvett – lett å bli lurt. Hvordan unngå å bli det «svakeste leddet»?

Nasjonal sikkerhetsmåned bidrar til samfunnet ved å bevisstgjøre og tilrettelegge for opplæring slik at den enkelte kan forebygge og håndtere sikkerhetshendelser. Mye tyder på at oktober allerede er etablert som en måned hvor stadig flere setter av tid til opplæring av egne ansatte. Dette bidrar til et tryggere digitalt samfunn. Kunnskapen de får er ferskvare og sikkerhetsutfordringene endrer seg kontinuerlig. Derfor bør Nasjonal sikkerhetsmåned fortsette å være den viktige nasjonale dugnaden den er i dag.

Nasjonal sikkerhets-måned i 2019:



- 238 011 ansatte i 691 virksomheter mottok opplæringspakken
- Antall virksomheter som mottok opplæringspakken økte med 89 prosent fra 2018
- 75 prosent av alle virksomhetene som deltok har mindre enn 20 ansatte



50 %

Økningen i antall foredrag under foredragsdugnaden i Nasjonal sikkerhetsmåned fra 2018

Andre aktiviteter fra årets sikkerhetsmåned

- Det ble gjennomført i alt 70 foredrag i forbindelse med foredragsdugnaden som NorSIS koordinerte i løpet av Nasjonal sikkerhetsmåned i 2019. Det er en økning på nesten 50 prosent sammenlignet med 2018. Denne typen foredrag gir særlig små virksomheter muligheten til å få faglig påfyll fra informasjonssikkerhetseksperter.
- NorSIS markedsførte egne kurs i sosiale medier, også rettet mot privatpersoner.
- Det ble gjennomført en egen kampanje i sosiale medier knyttet til de ti rådene for virksomheter fra regjeringens strategi for digital sikkerhet.

Samarbeidspartnere fra offentlig og privat næringsliv

Også i år har vi hatt en økning i antall samarbeidspartnere fra 23 til 34. Flere av samarbeidspartnerne våre har vært med i flere år. Av disse ønsker vi særlig å trekke frem Næringslivets sikkerhetsråd (NSR), Difi, Kripos, Datatilsynet og Nasjonal sikkerhetsmyndighet (NSM).

Det at store private næringslivsaktører også deltar aktivt i den nasjonale sikkerhetsdugnaden, sender et viktig signal til egen bransje, media og øvrig næringsliv. Samarbeidet bidrar også til en økning i

spredningen av informasjon om forebyggende sikkerhet både til virksomheter og til befolkningen. Det er svært viktig for å gjøre samfunnet vårt mer motstandsdyktig mot trusler og kriminalitet som rammer både forbruker, det offentlige og næringslivet for øvrig.

Internasjonalt samarbeid

ENISA er NorSIS' viktigste internasjonale samarbeidspartner. Vi har samarbeidet med dem om Nasjonal sikkerhetsmåned i ni år. Som nasjonal koordinator for sikkerhetsmåned i Norge, har NorSIS en sterk posisjon i ENISA. Vi er et av de landene som er mest aktive med tanke på å engasjere partnere og næringsliv, arrangere foredrag, bruke media til å spre budskapet om informasjonssikkerhet og skape positiv oppmerksomhet via opplæringspakken.

Sikkerhetstoppmøtet

Sikkerhetstoppmøtet er en rundebordskonferanse med avgrenset deltakelse, i hovedsak myntet på ledere og sikkerhetsledere i norske virksomheter. Det ble arrangerte tre sikkerhetstoppmøter i 2019 – ett på våren i Oslo og to på høsten i henholdsvis Bergen og Oslo.

I 2019 er det niende året NorSIS arrangerer Sikkerhetstoppmøtet. Møtet i Bergen i oktober ble arrangert i samarbeid med Dataforeningen i Hordaland og lagt i tilknytning til Sikkerhetssymposiet. Tema for vårmøtet var «GDPR – erfaringer fra innføring av nytt regelverk». På høstmøtene var temaet «Hva virker av sikkerhetsopplæring?».

Totalt deltok om lag 90 personer på de tre sikkerhetstoppmøtene som ble arrangert i 2019.

Norwegian Cyber Range

NorSIS deltar i prosjektet Norwegian Cyber Range (NCR), som gjennomføres av NTNU. NCR er en arena for testing, trening og øving innen cybersikkerhet, der brukere og systemer eksponeres for realistiske hendelser i trygge omgivelser.

Målet med deltakelsen i prosjektet er todelt:

- NorSIS har mye data som kan benyttes som grunnlagsdata for NCR. Disse dataene må kartlegges, struktureres og anonymiseres før de kan benyttes.
- NCR kan bli en god kilde til kunnskapsutvikling og kunnskapsbygging for NorSIS' målgruppe. Gjennom bidrag til å utvikle gode tjenester i NCR, ønsker NorSIS å legge til rette for gode sikkerhetstjenester som kan benyttes av befolkningen generelt og små og mellomstore bedrifter spesielt.

NorSIS har i varierende grad vært involvert i de innledende prosjektaktivitetene, og organisasjonens del av prosjektet er planlagt gjennomført i perioden 2019–2021. Rammen, inklusive egeninnsats, for NorSIS' prosjektdeltakelse, er 4,75 millioner kroner over tre år.

Prosjekt for utvikling og utprøving av kompetansetiltak i grunnutdanningen knyttet til digital sikkerhetskultur

Prosjektet retter seg mot lærere, elever og foreldre, og har som mål å øke de respektive målgruppens kompetanse innenfor områdene informasjonssikkerhet, digital sikkerhet, nettvett og digital dømmekraft.

Fra skolestart høsten 2020 begynner innføringen av nye læreplaner for grunnopplæringen. NorSIS ønsker at ressursene som utarbeides i prosjektet skal støtte skolene i arbeidet med forberedelser, kompetanseheving og implementering av nye læreplaner. Det er et mål at deltakelse i prosjektet skal oppleves som et ekstra bidrag til skoleeiere, skoler og lærere i arbeidet med nye læreplaner knyttet til temaet digital sikkerhet slik at elevene får best mulig opplæring.

Prosjekt mål

Prosjektets mål er å øke forståelse for og kunnskap om digital sikkerhet, nettvett og digital dømmekraft hos lærere, elever og foreldre i grunnopplæringen.

Prosjektet adresserer problemstillinger av stor betydning for barn og unges læring, helse og trivsel. Digital sikkerhet og digital dømmekraft er viktige ferdighetsområder under den grunnleggende ferdigheten digitale ferdigheter, det er knyttet til læring i fagene og digitale hendelser har betydning for elevers opplevelse av et godt og trygt skolemiljø. For at skolen skal lykkes i å ruste elevene til å mestre livene sine og møte fremtiden, er digital kompetanse grunnleggende.

En viktig forutsetning for å lykkes med dette er tett samarbeid med fylkeskommunen og kommuner som skoleeiere samt andre ressurspersoner. NorSIS samarbeider med Innlandet fylke og Nordre Land kommune, og har etablert en arbeidsgruppe med lærere fra hele grunnopplæringen.

Delmål

- Etablere prosjektorganisasjon, utarbeide prosjektplaner og inngå samarbeid med skoler i Oppland
- Utvikle digitale ressurser i digital sikkerhetskultur for lærere og skoleledelse
- Utvikle læreplantulpassede undervisningsressurser i digital sikkerhetskultur for elever
- Utvikle digitale ressurser i digital sikkerhetskultur for foreldre
- Gjennomføre forprosjekt om bruk av digitalt informasjons-/kulturutviklingskonsept for skolesektoren blant annet ved anvendelse av spillelementer og teknologi
- Planlegge og gjennomføre lansering og erfaringsoppsummering
- Evaluere og rapportere prosjekterfaringer
- Initiere samarbeid med aktuelle forskningsaktører

Prosjektet ble igangsatt høsten 2018 og vil bli ferdigstilt våren 2020.

Arendalsuka

Sammen med Medietilsynet arrangerte NorSIS «Hacket mot alle odds» under Arendalsuka. Arrangementet var en del av hovedprogrammet i Arendalsuka Ung.

Bakgrunnen for arrangementet var at mange unge oppgir å ha fått opplæring i nettvett og digital sikkerhet. Samtidig viser undersøkelser og erfaring fra Slettmeg.no at mange unge velger å ikke følge datasikkerhetsrådene de har fått. Vi ønsket å belyse hvorfor det er slik, hvor lett det egentlig er å hacke noen, hva som kan skje, hvilke konsekvenser det gir og hvordan ungdommen tenker at vi kan løse dette.

Arrangementet var tredelt. Seansen begynte med en samtale om hacking med en ungdom fra Gjøvik. Videre presenterte vi tall fra en kort undersøkelse om unges holdninger til passord og beskyttelse av egne opplysninger, og rundet av med en panelsamtale mellom ulike ungdomsrepresentanter.

Arrangementet ble avholdt på utescenen på Torget, og var godt besøkt.

Sikkerhetsfestivalen

NorSIS var medarrangør av Sikkerhetsfestivalen på Lillehammer 26.–28. august 2019. Festivalen er en arena for erfaringsutveksling, og ambisjonen er at dette skal bli Norges største og viktigste sikkerhetsarrangement og en samlende arena for alle med interesse eller ansvar for cyber, IKT og informasjonssikkerhet.

Sikkerhetsfestivalen ble arrangert i tett samarbeid med Nasjonal sikkerhetsmyndighet (NSM),

tidligere Oppland fylkeskommune, Lillehammer kommune, NTNU, UiO, ISACA, Cloud Security Alliance, Den norske dataforening, Foreningen kommunal informasjonssikkerhet (KiNS), Difi, NorSIS og IKT-Norge.

NorSIS gjennomførte to arrangementer under Sikkerhetsfestivalen. Det ene hadde ungdom som målgruppe, og der deltok rundt 450 studenter fra Innlandet. Her ble det også vist en førpremiere av NRK-serien «Nudes», som NorSIS har vært fagkonsulenter for. Det andre var et arrangement rettet mot pensjonister.

Security Divas – en arena for kvinner som jobber i eller med sikkerhet

Security Divas er en viktig møteplass for kvinner. Målet er å bidra til å skape en arena for nettverksbygging og samarbeid for kvinner som jobber i eller med sikkerhet. Security Divas konferansen ble arrangert på Gjøvik i januar med 143 deltagere.

Det er viktig å understreke at vi vektlegger fagkunnskap og bredden i denne, ikke ulikheter mellom kjønn. Gjennom 2019 har vi samarbeidet med Accenture. Både i forkant av konferansen på Gjøvik i januar og ved at Accenture arrangerte et frokostmøte i Oslo i mars. Vi arrangerte også et nettverkstreff i september i regi av BuyPass i september. Det var fulltegnet flere uker før det ble gjennomført og fikk gode tilbakemeldinger på evalueringen.

Det internasjonale SC Magazine kåret i 2019 NorSIS' administrerende direktør, Peggy Sandbekken Heie, til en av de viktigste kvinnene innen cybersikkerhet i Europa, blant annet for arbeidet med Security Divas og Nasjonal sikkerhetsmåned.

Difi samarbeidsprosjekt

Digitaliseringsdirektoratet (tidligere Difi) har fått ansvaret for gjennomføring av et prosjekt for oppfølging av anbefalingene som er gitt i Difi-rapport 2018:4, «Arbeid med informasjonssikkerhet i statsforvaltningen, kunnskapsgrunnlag». NorSIS er gitt ansvar for gjennomføring av delprosjektet som fokuserer på sikkerhetskultur.

Delprosjektet skal utarbeide en metode som skal sette statlige og kommunale virksomheter i stand til å kartlegge sin sikkerhetskultur, og på bakgrunn av kartleggingen lage en plan for videre arbeid med tiltak og forbedringer.

Delprosjektet har følgende leveranser:

- Tilpasse eksisterende metode for kartlegging av digital sikkerhetskultur til bruk i statsforvaltningen
- Utarbeide en veiledning for kartlegging av digital sikkerhetskultur i statsforvaltningen
- Utarbeide en veiledning for arbeid med digital sikkerhetskultur og kompetanse i statsforvaltningen
- Foreslå føringer for bruk av metoden og veiledningene i statsforvaltningen

Første leveranse ble levert i desember 2019, mens de øvrige skal leveres i løpet av første halvår 2020. Delprosjektet skal være ferdig innen sommeren 2020.

Varslingstjeneste

I 2019 har NorSIS gjennomført et forprosjekt med tanke på å fremskaffe et beslutningsgrunnlag for etablering av en varslingstjeneste som skal bidra til økt robusthet mot datakriminalitet som rammer befolkningen og norske virksomheter. Dette er ønskelig å få til gjennom utarbeidelse og spredning av tidstriktede og relevante varsler om kjente trusler og sårbarheter. Forprosjektet ble finansiert av en tildeling på 400 000 kroner fra Oppland fylkeskommune. Forprosjektrapporten ble oversendt fylkeskommunen i desember 2019.

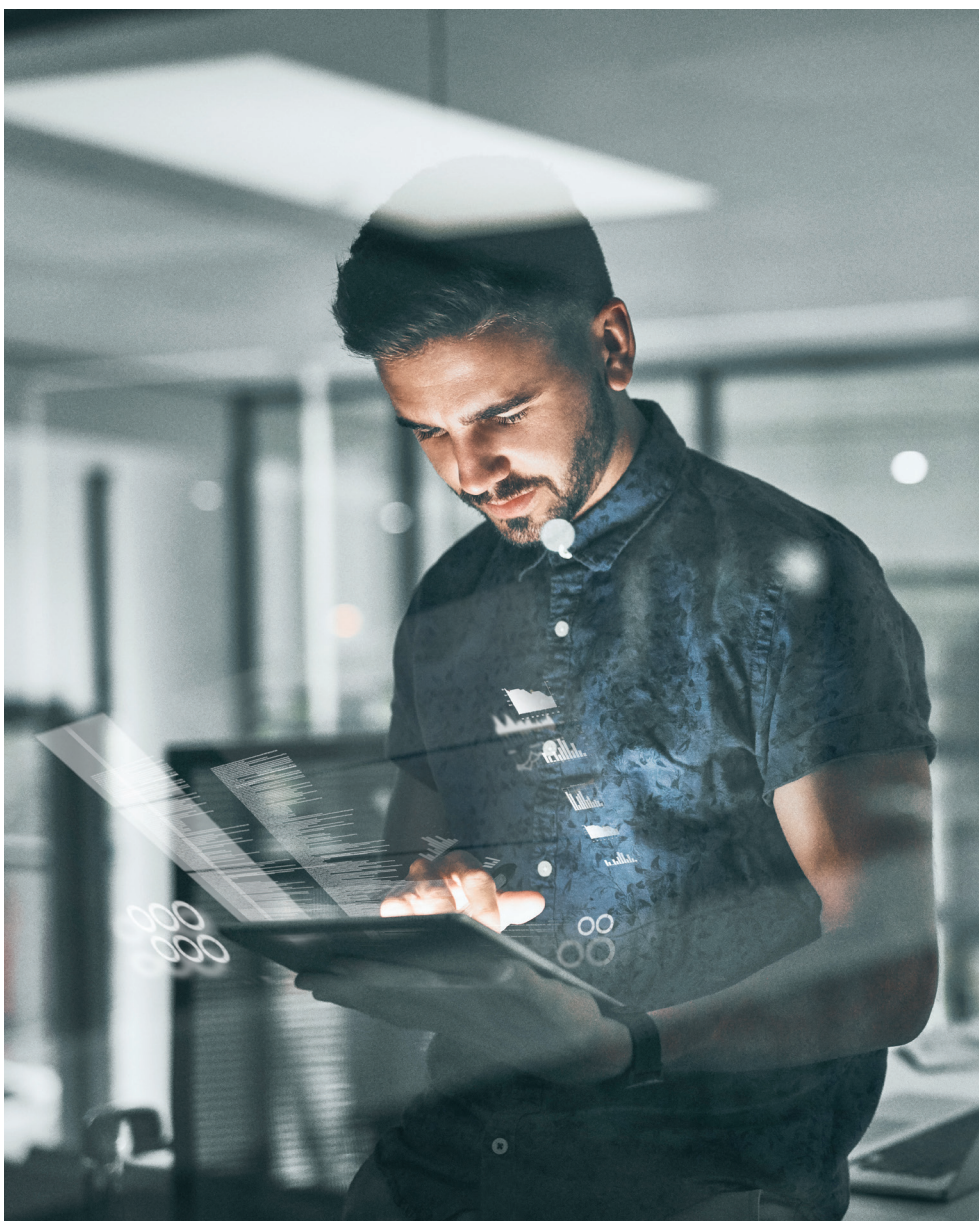
Cybervarsel

NorSIS har utviklet en løsning som gir oss et «realtime»-oversiktsbilde på hendelser og statistikk. Løsningen viser antall saker til behandling, hvilke trender vi ser samt hvilke sider og veiledninger som blir brukt. Løsningen er under utvikling, og vil på sikt kunne tilby vår målgruppe informasjon om trusler og trender.

LiveAgent

NorSIS har tatt i bruk en felles helpdesk-løsning (LiveAgent) for alle våre tjenester. Det gjør at vi kan håndtere alle henvendelser på en enhetlig og effektiv måte.

LiveAgent gir oss også viktige metadata som benyttes til statistikk og analyse av trender og hendelser.



6 Rapporter og undersøkelser i 2019

Rapporten «Trusler og trender 2019–2020»

Behov

Kunnskap om det digitale trusselbildet, de kommende trendene og dine egne verdier er sammen med en oversikt over hvordan du konkret forholder deg til truslene et svært viktig redskap for å bli trygg på nett. Det er nettopp det «Trusler og trender 2019–2020» er.

NorSIS' årlige rapport er en oppsummering av de truslene som har preget Norge i året som gikk, og som høyst sannsynlig også kommer til å gjøre det i året som ligger foran oss.

Rapporten ser nærmere på trendene i det digitale trusselbildet for å gi både enkeltpersoner og de nærmere en million små og mellomstore bedriftene i Norge en mulighet til å sikre sine verdier bedre.



«Rapporten ser nærmere på trendene i det digitale trusselbildet for å gi både enkeltpersoner og de nærmere en million små og mellomstore bedriftene i Norge en mulighet til å sikre sine verdier bedre»

Tidlig i november startet vi arbeidet med denne rapporten. Den ble overrakt justisminister Monica Mæland i februar 2020.

Innsikt

NorSIS har i rapporten fått innspill fra Dataforeningen, Kripos, DNB, Nasjonal sikkerhetsmyndighet (NSM) og Microsoft. Vi har, basert på disse innspillene og egen erfaring, pekt på de ti største digitale truslene slik situasjonen var ved årsskiftet 2019/2020. Rapporten inneholder også konkrete råd og tips den enkelte kan ta i bruk for å beskytte seg mot truslene.

De 10 største digitale truslene:

1. Løsepengevirus
2. ID-tyveri
3. Falske trusler og utpressingskrav (som pornosvindel)
4. Phishing
5. Utpressing og svindel
6. Kontohacking
7. Datainnbrudd
8. Menneskelige feil
9. Krenkelser
10. Verdikjedeangrep

De digitale trendene det advares mot i rapporten er at stadig sikrere maskiner gjør at de kriminelle vil angripe mennesker ved bruk av sosial manipulasjon. Det advares blant annet mot økt sosial manipulasjon for å fralure enkeltpersoner deres BankID. Også økt sårbarhet for angrep mot skytjenester og det økende antallet nettilkoblede enheter og sårbarheten disse utgjør blir tatt opp i rapporten. Her blir det også gitt gode råd for hvordan den enkelte kan beskytte seg mot disse trusseltrendene.

Rapporten «Nordmenn og digital sikkerhetskultur 2019»

Behov

Rapporten er den fjerde i rekken som beskriver den norske digitale sikkerhetskulturen. Å følge utviklingen av digital sikkerhetskultur over tid kan gi både myndigheter og andre god innsikt i effekten av ulike sikkerhetstiltak i befolkningen. Det benyttes store ressurser for å tilføre informasjon og kompetanse til ansatte og befolkningen generelt om sårbarhet, trusler og risiko knyttet til bruk av digitale verktøy og tjenester. Gir ressursbruken god effekt? Det er et spørsmål som kartlegging av digital sikkerhetskultur i samfunnet eller virksomheten kan være med på å besvare.



Innsikt

Fjorårets rapport tyder på at det fortsatt er behov for fokus på digital sikkerhet. Vi ser en positiv trend på noen områder. Bruk av gode passord og totrinnsbekreftelse øker, og vi ser at flere får opplæring. Dessverre ser vi også at frykten for bruk av digitale tjenester øker i befolkningen. Det tyder på at vi når frem med informasjon om de trusler som eksisterer knyttet til bruk av internett og internettbaserte tjenester, men at informasjon om hvordan man kan bruke disse tjenestene på en trygg måte ikke er kommunisert like godt.

«Å følge utviklingen av digital sikkerhetskultur over tid kan gi både myndigheter og andre god innsikt i effekten av ulike sikkerhetstiltak i befolkningen»

Rapporten «Sikkerhetskultur i vann- og kraftsektoren 2019»

Behov

Dette er to sektorer som de aller fleste av oss er i befatning med til daglig, uten at vi tenker så mye over det. Vi forventer at tjenestene fra disse sektorene er tilgjengelige. Sektorene er også i stor grad digitaliserte, og opprettholdelse av tjenestene baserer seg på at de som arbeider med dette har tilgang til digitale verktøy daglig.

Innsikt

Denne rapporten ble laget i samarbeid med Norsk Vann, Energi Norge og forskningsinstitusjonen NORCE. Kartleggingen viser blant annet at 8 prosent i kraftsektoren og 15 prosent i vannsektoren ikke vet om arbeidsplassen har regler for digital sikkerhet. Klare regler for hvordan en organisasjon skal forholde seg til sikkerhet i den digitale hverdagen er et viktig element i det å trygge verdiskapingen i organisasjonen. At så mange angir at de ikke vet om det finnes slike regler på arbeidsplassen, tyder på at den enkelte virksomhet i langt større grad enn i dag må informere om slike regler og hvordan de skal forstås.



7 Formidling i 2019

NorSIS er en formidler. I tillegg til å være synlig i mediene som en ekspert med gode råd og tips til både virksomheter og befolkningen for øvrig, bruker senteret ressurser på å formidle gjennom egne kanaler – både nyhetsbrev, egne nettsaker og aktiviteter i sosiale medier. NorSIS jobber også aktivt med samarbeidspartnere for å få ut informasjon i deres kanaler.

Økt medieomtale

NorSIS har i mange år hatt en sterk posisjon som eksperter på informasjonssikkerhet i mediene. I 2019 økte vi igjen antall medieoppslag fra et allerede høyt nivå året før.

NorSIS hadde i alt 1489 medieoppslag i 2019. Det er en økning på mer enn 6 prosent sammenlignet med 2018. Omtalen fordeler seg mellom alt fra nettaviser til papiraviser, radio og tv. Det er et snitt på 26,9 oppslag hver eneste uke, eller nesten fire saker hver dag.

Gjennom en målrettet satsing på denne typen informasjonsformidling, blir våre vurderinger og råd hyppig gjengitt av mediene.

- Det skjer ved at NorSIS selv aktivt oppsøker mediene med temaer for å sikre at befolkningen forholder seg til det til enhver tid gjeldende trusselbildet og iverksetter de tiltak som også bekreftes gjennom trusselrapportene fra NSM, PST, E-tjenesten og Kripos.
- Det skjer også ved at NorSIS blir kontaktet for ekspertuttalelser i forbindelse med pågående saker som dreier seg om digital sikkerhet.

Mens merkevaren NorSIS står for hoveddelen av oppslagene (61 prosent), er også Slettmeg.no (19 prosent) og Nettvett.no (13 prosent) ofte gjengitt.

NorSIS' mediestrategi innebærer å ha en sterkt forankret faglig posisjon og god kontakt med media for å nå ut til de relevante målgruppene med de riktige rådene.

6 %

Økningen i medie-
omtalen i 2019



4

Antall medie-
oppslag i
gjennomsnitt
hver dag i 2019



107 millioner kroner

Retrievers anslåtte annonseverdi på
mediedekningen NorSIS hadde i 2019

Bruk av våre nettsider i 2019*

- norsis.no: **83 867** brukere
- nettvett.no: **338 479** brukere
- slettmeg.no: **342 975** brukere

*Kilde: Google Analytics



1489

medieoppslag i 2019

6717

mottar vårt ukentlige
nyhetsbrev



2,5

Antall nyhetssaker
publisert i gjennomsnitt
hver uke på norsis.no

15 998

Følger våre
Facebook-sider



70

Antall foredrag avholdt
i foredragsdugnaden



21

Antall veiledninger
publisert i 2019
på Nettvett.no og
slettmeg.no

857

Antall håndterte saker
av NorSIS i 2019



1001
000
1001

5497

Antall saker håndtert i
2019 av slettmeg.no

8

Oppsummering: Målsettinger og resultater

Justis- og beredskapsdepartementet (JD) har fastsatt flere målsettinger for tilskuddet til NorSIS i 2019. I dette kapitlet vil vi presentere fakta og vurderinger som gjelder de enkelte resultatindikatorerne. Tabellen gir en oversikt over aktiviteten i 2019 og en indikasjon på utviklingen fra tidligere år.

Resultatindikator	Kriterier	2017	2018	2019	Vurdering
Økt kunnskap og bevissthet om informasjonssikkerhet	Relevant informasjon til rett målgruppe – formidlet som grunnlag for økt bevissthet og effektive tiltak.				NorSIS har styrket målgruppens bevissthet ved å kommentere og gi råd ved vesentlige sårbarheter og hendelser. NorSIS har nådd bredt ut med veiledning, formidling og opplæring.
Tilskudd fra JD som andel av samlet driftsbudsjett	Balansert offentlig tilskudd og egen finansiering. God inndeckning av ideelle formål. Bidra til økt offentlig/privat samarbeid.	51,76 %	61,18 %	58,23 %	NorSIS sin andel av offentlig finansiering har økt siden 2017. Dette skyldes finansiering av slettmeg.no fra 2018 med to millioner kroner i årlig tilskudd.
Samarbeidspartnere: omfang og type	Bredde i sammensetning og effekt av samarbeidet				NorSIS arbeider systematisk med å få de rette samarbeidspartnerne i relevante sektorer. God faglig forankring og felles målsettinger er viktige kriterier.
Fora og nettverk for utveksling av informasjon	Skape og opprettholde arenaer for å dele informasjon.				NorSIS arbeider aktivt med å ha relevante samarbeidspartnere. Det søkes samarbeidspartnere som støtter opp under det målrettede arbeidet mot NorSIS sine målgrupper og som har bred kontakflate mot befolkningen og SMB-virksomheter.
Antall leverte nyheter på norsis.no per uke	Relevant og regelmessig informasjon.	3,3	2,4	2,5	Antall nyhetssaker på norsis.no har vært stabilt de siste to år. Det er planlagt en gjennomgang av nyheter, omfang og innhold i 2020. Antall besøkende på norsis.no er forholdsvis stabilt. Veiledninger finnes på nettvett.no
Antall besøkende på norsis.no		75 610	88 277	83 687	
Antall sidevisninger på norsis.no		213 755	224 533	197 708	
Antall besøkende og sidevisninger på nettvett.no	Bredde og aktualitet som dekker målgruppens behov for praktisk veiledning.	147 832 319 618	229 061 463 374	338 479 635 263	Veiledninger på nettvett oppdateres i takt med hendelser og inntrufne sårbarheter. Siden er blitt betraktelig mer besøkt i 2019.
Antall personer som har fått hjelp fra slettmeg.no	Kapasitet til å håndtere faktiske henvendelser med akseptabel responstid.	5350	5935	5497	Antall personer som får «en-til-en-hjelp» hos Slettmeg har vært forholdsvis stabil siste årene, med noe nedgang i 2019. Dette kan skyldes flere aktører i markedet som hjelper sine kunder med lignende oppgaver.
Antall besøkende og sidevisninger på slettmeg.no	Etablert og kjent tjeneste som dekker målgruppens behov for faktisk hjelp.	356 353 1 022 840	351 306 960 305	342 975 876 817	Nettstedet er flittig og stabilt besøkt.
Medieeksponering med antall omtaler	Evne til å håndtere henvendelser og utnytte muligheter til formidling av informasjon og råd.	1733	1402	1489	God medieeksponering, særlig i forhold til et marked hvor det de senere årene har kommet til mange aktører som «kjempere» om medieeksponering i forhold til digital sikkerhet.
Nasjonal sikkerhetsmåned (antall partnere og personer i e-opplæring)	Relevante tema og opplevd verdi: antall partnere og rekkevidde på e-opplæring.	19 144 000	23 256 144	1489	Økning i antall partnere som bidrar aktivt i Nasjonal Sikkerhetsmåned. Antall ansatte som har mottatt opplæring har gått noe ned i 2019, men det skyldes en markant satsning og økning med å få med bedrifter med 1-20 ansatte.
Antall virksomheter		.*	365	691	
Antall konferanser og seminarer arrangert	Ivareta behov særlig på områder som ikke dekkes av andre aktører.	12	9	12	Stabilt med antall arrangement hvert år.
Antall foredrag holdt	Imøtekomme målgruppens etterspørsel etter direkte formidling.	47	47	45	Det holdes et stabilt antall foredrag hvert år.

* NorSIS skiftet e-læringsleverandør i forkant av sikkerhetsmåned 2018 med bedre statistikk over antall virksomheter.

Årsregnskap 2019

Norsk Senter For Informasjonssikring

Resultatregnskap
Balanse
Noter til regnskapet

Org.nr.: 995 195 003

Norsk Senter For Informasjonssikring
RESULTATREGNSKAP FOR 2019

	Note	2019	2018
DRIFTSINTEKTER OG KOSTNADER			
Salgsinntekt	3	17 498 182	16 208 456
Annen driftsinntekt		910	911
Sum driftsinntekter		17 499 092	16 209 366
Varekostnad		1 331 356	1 655 117
Lønnskostnad	2	10 868 907	9 149 795
Avskrivning varige driftsmidler	4	13 144	2 191
Annen driftskostnad	2	4 729 210	3 275 899
Sum driftskostnader		16 942 617	14 083 001
DRIFTSRESULTAT		556 474	2 126 365
Finansinntekt og finanskostnad			
Annen renteinntekt		47 993	35 017
Annen finansinntekt		5 675	5 795
Annen rentekostnad		-3 453	-1 486
Annen finanskostnad		-432	0
Resultat av finansposter		49 782	39 326
ÅRSRESULTAT		606 257	2 165 692
OVERFØRINGER			
Avsatt til annen egenkapital	6	606 257	2 165 692
SUM OVERFØRINGER		606 257	2 165 692

Org.nr: 995 195 003

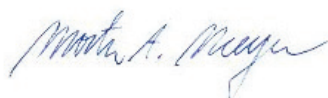
Norsk Senter For Informasjonssikring
BALANSE PR. 31. DESEMBER 2019

	Note	2019	2018
EIENDELER			
Inventar og utstyr	4	49 290	62 434
Sum varige driftsmidler		49 290	62 434
SUM ANLEGGSMIDLER		49 290	62 434
OMLØPSMIDLER			
Fordringer			
Kundefordringer		68 596	498 446
Andre fordringer		732 241	42 110
Sum fordringer		800 836	540 556
Betalingsmidler			
Bankinnskudd og kontanter	5	8 732 161	7 997 722
Sum betalingsmidler		8 732 161	7 997 722
SUM OMLØPSMIDLER		9 532 997	8 538 279
SUM EIENDELER		9 582 287	8 600 712

Norsk Senter For Informasjonssikring
BALANSE PR. 31. DESEMBER 2019

	Note	2019	2018
EGENKAPITAL OG GJELD			
EGENKAPITAL			
Opptjent egenkapital			
Annen egenkapital	6	6 450 322	5 844 066
Sum opptjent egenkapital		6 450 322	5 844 066
SUM EGENKAPITAL		6 450 322	5 844 066
GJELD			
Kortsiktig gjeld			
Leverandørgjeld		951 523	340 536
Skyldige offentlige avgifter		1 018 846	1 085 436
Annen kortsiktig gjeld		1 161 596	1 330 675
Sum kortsiktig gjeld		3 131 965	2 756 647
SUM GJELD		3 131 965	2 756 647
SUM EGENKAPITAL OG GJELD		9 582 287	8 600 712

Gjøvik, 19.03.2020



Morten Andreas Meyer
styreleder



Nils Kalstad
styremedlem



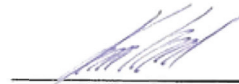
Bjørn Erik Thon
styremedlem



Heidi Arnesen Austlid
styremedlem



Ivar Kjærem
styremedlem



Kristine Beitland
styremedlem



Peggy Lill Sandbekken
daglig leder

Regnskapsprinsipper

Årsregnskapet er satt opp i samsvar med regnskapsloven og NRS 8 - God regnskapsskikk for små foretak. Virksomheten er organisert som en forening og den ble stiftet 2. februar 2010.

Driftsinntekter

Inntektsføring ved salg av varer skjer på leveringstidspunktet. Tjenester inntektsføres etter hvert som de leveres.

Skatt

Foreningen er unntatt beskatning.

Klassifisering og vurdering av anleggsmidler

Anleggsmidler omfatter eiendeler bestemt til varig eie og bruk. Anleggsmidler er vurdert til anskaffelseskost. Varige driftsmidler balanseføres og avskrives over driftsmidlets økonomiske levetid. Avskrivningsperioden for fast eiendom anskaffet etter 2009 er dekomponert i en del som gjelder råbygget og en del som gjelder faste tekniske installasjoner. Varige driftsmidler nedskrives til gjenvinnbart beløp ved verdifall som forventes ikke å være forbigående. Gjenvinnbart beløp er det høyeste av netto salgsverdi og verdi i bruk. Verdi i bruk er nåverdi av fremtidige kontantstrømmer knyttet til eiendelen. Nedskrivningen reverseres når grunnlaget for nedskrivningen ikke lenger er til stede.

Klassifisering og vurdering av omløpsmidler

Omløpsmidler og kortsiktig gjeld omfatter normalt poster som forfaller til betaling innen ett år etter balansedagen, samt poster som knytter seg til varekretsløpet. Omløpsmidler vurderes til laveste verdi av anskaffelseskost og virkelig verdi.

Fordringer

Kundefordringer og andre fordringer oppføres til pålydende etter fradrag for avsetning til forventet tap. Avsetning til tap gjøres på grunnlag av en individuell vurdering av de enkelte fordringene.

Note 2 Lønnskostnader og ytelser, godtgjørelser til daglig leder, styret og revisor

Lønnskostnader	2019	2018
Lønninger	8 963 708	7 209 042
Arbeidsgiveravgift	1 349 818	1 075 814
Pensjonskostnader	451 885	454 101
Andre ytelser	129 184	399 359
Sum	10 894 595	9 138 315

Selskapet har i 2019 sysselsatt 9,8 årsverk.

Pensjonsforpliktelser

Selskapet er pliktig til å ha tjenestepensjonsordning etter lov om obligatorisk tjenestepensjon. Selskapets pensjonsordninger tilfredsstiller kravene i denne lov.

Ytelser til ledende personer	Daglig leder	Styret
Lønn	1 132 147	175 000
Annen godtgjørelse	19 990	0
Sum	1 152 137	175 000

Honorar til revisor eks. mva utgjør:	2019	2018
Lovpålagt revisjon, inkl. regnskapsteknisk bistand	36 645	35 785
Regnskapsteknisk bistand	0	0
Andre attestasjonstjenester	7 120	0
Andre tjenester utenfor revisjon	29 735	2 100
Sum	73 500	37 885

Note 3 Offentlig tilskudd

Selskapet har mottatt kr 10 416 000 i grunnfinansiering. For øvrig er det mottatt prosjektstøtte på kr 1 997 128.

Note 4 Anleggsmidler

	Driftsløsøre, inventar ol.	Sum
Anskaffelseskost pr. 01.01.19	284 974	284 974
= Anskaffelseskost 31.12.19	284 974	284 974
Akkumulerte avskrivninger 31.12.19	235 685	235 685
= Bokført verdi 31.12.19	49 290	49 290
Årets ordinære avskrivninger	13 144	13 144
Økonomisk levetid	5 år	

Selskapet leier kontoriokaler. Årets kostnad inkl felleskostnader utgjør kr 586 142.

Note 5 Bankinnskudd

Innestående midler på skattetrekkkonto (bundne midler) er på kr. 377 873.

Note 6 Egenkapital

	Annen egenkapital	Sum egenkapital
Pr. 31.12.2018	5 844 066	5 844 066
Endringer ført mot EK	0	0
Pr 01.01.2019	5 844 066	5 844 066
Årets resultat	606 257	606 257
Pr 31.12.2019	6 450 322	6 450 322

Uttalelse fra ledelsen

Deloitte AS
Att.: Thomas Hagen Alm
Trondhjemsvegen 3
2821 Gjøvik

19.03.2020

Dette brevet sendes i forbindelse med Deres revisjon av regnskapet for Norsk Senter for Informasjonssikring for året som ble avsluttet den 31. desember 2019, med det formål å kunne konkludere om hvorvidt regnskapet i det alt vesentlige gir et rettviseende bilde i samsvar med Regnskapslovens regler og god regnskapsskikk i Norge.

Vi bekrefter etter beste evne og overbevisning, og etter å ha foretatt de forespørsler vi har ansett som nødvendige for å innhente de nødvendige opplysninger at:

Regnskap

- Vi har oppfylt vårt ansvar som fastsatt i vilkårene for revisjonsoppdraget datert 25.09.2017, vedrørende utarbeidelsen av regnskapet i samsvar med lov og forskrifter, og bekrefter at regnskapet gir et rettviseende bilde i samsvar med Regnskapslovens regler og god regnskapsskikk i Norge.
- Viktige forutsetninger som er brukt av oss ved utarbeidelsen av regnskapsestimater, herunder regnskapsestimater målt til virkelig verdi, er rimelige, og at all relevant informasjon tilgjengelig på 19.03.2020 knyttet til virkelig verdi vurdering og vesentlig estimater er tatt hensyn til.
- Det er tatt tilstrekkelig hensyn til og opplyst om forhold til nærstående parter og transaksjoner med disse i overensstemmelse med kravene i Regnskapslovens regler og god regnskapsskikk i Norge.
- Hendelser og transaksjoner som ledelsen er blitt oppmerksom på og som har funnet sted frem til 19.03.2020 og som etter Regnskapslovens regler og god regnskapsskikk i Norge medfører korrigerende eller omtale, er korrigert eller omtalt.
- Regnskapet ikke inneholder vesentlig feilinformasjon eller mangler. Virkningen av ikke-korrigert feilinformasjon er uvesentlig, både enkeltvis og samlet for regnskapet sett som helhet.
- Vi har påsett at selskapets regnskap og formuesforvaltning av betydning for regnskapet er gjenstand for betryggende kontroll, herunder slik intern kontroll som vi finner nødvendig for å muliggjøre utarbeidelsen av et regnskap som ikke inneholder vesentlig feilinformasjon, verken som følge av misligheter eller feil.
- Vi erkjenner vårt ansvar for og bekrefter at vi har oppfylt vår plikt til å sørge for ordentlig og oversiktlig registrering og dokumentasjon av enhetens regnskapsopplysninger i samsvar med lov og forskrifter.
- Alle kjente faktiske eller mulige rettsvister og krav som kan ha slik betydning at de må tas hensyn til ved utarbeidelsen av regnskapet, er gjort kjent for revisor og er redegjort for og gitt tilleggsopplysninger om i samsvar med Regnskapslovens regler og god regnskapsskikk i Norge.
- At ledelsen erkjenner sitt ansvar for utformingen, iverksettelsen og vedlikeholdet av intern kontroll for å forhindre og avdekke misligheter.
- At alle transaksjoner er registrert i regnskapsposter og reflektert i regnskapet.
- At regnskapet og eventuell «øvrige informasjon» gitt revisor før datoen på revisjonsberetningen er i overensstemmelse med hverandre, og at øvrige informasjon ikke inneholder vesentlig feilinformasjon.

Informasjon som er gitt

- Vi har gitt revisor:
 - tilgang til all informasjon som vi er kjent med, og som er relevant for utarbeidelsen av regnskapet, som for eksempel regnskapsregistreringer, dokumentasjon og øvrige forhold,
 - ytterligere informasjon som revisor har bedt om fra oss for revisjonsformål, og
 - ubegrenset tilgang til personer i Norsk Senter for Informasjonssikring som det etter revisors vurdering er nødvendig å innhente revisjonsbevis fra.
- Vi har gitt revisor informasjon om resultatene av vår vurdering av risikoen for at regnskapet kan inneholde vesentlig feilinformasjon som følge av misligheter.
- Vi har gitt revisor all informasjon om eventuelle misligheter eller mistanker om misligheter som vi er kjent med og som kan ha påvirket Norsk Senter for Informasjonssikring, og som involverer:
 - Ledelsen,
 - ansatte som har en betydningsfull rolle i forhold til intern kontroll, eller
 - andre hvor misligheten kunne hatt en vesentlig virkning på regnskapet.
- Vi har gitt revisor informasjon om alle eventuelle påstander eller mistanker om misligheter som kan ha påvirket Norsk Senter for Informasjonssikrings regnskap og som er kommunisert av ansatte, tidligere ansatte, analytikere, tilsynsmyndigheter eller andre.
- Vi har gitt revisor informasjon om alle kjente tilfeller av manglende overholdelse eller mistanke om manglende overholdelse av lover og forskrifter, og som kan ha vesentlig virkning på regnskapet.
- Vi har gitt revisor informasjon om identiteten til Norsk Senter for Informasjonssikrings nærstående parter og alle forhold til nærstående parter og transaksjoner med disse som vi er kjent med.
- Vi har gitt revisor informasjon om alle dokumenter som ledelsen forventer å utstede som kan inneholde «øvrig informasjon», og har gitt revisor alle dokumenter som inneholder «øvrig informasjon» og som foreligger før dato for revisjonsberetningen.
- Med hensyn til «øvrig informasjon» som ikke er gitt til revisor før datoen for revisjonsberetningen, har vi gitt revisor informasjon om vi har til hensikt å utarbeide og utstede slik «øvrig informasjon» og det forventede tidspunktet for denne utstedelsen. Vi bekrefter at dokumenter som inneholder «øvrig informasjon» og som ikke er tilgjengelige for revisor før dato for revisjonsberetningen vil bli gjort tilgjengelig for revisor før utstedelse av informasjonen.
- Vi har gitt revisor informasjon om eventuelle brudd på datasikkerheten (cyber-security) som ledelsen er blitt oppmerksom på, og som har potensiale for å legge til, endre eller slette data eller transaksjoner knyttet til årsregnskapet.

Bandsblær

Daglig leder



Deloitte AS
Trondhjemsvegen 3
NO-2821 Gjøvik
Norway

Tel: +47 400 34 100
www.deloitte.no

Til årsmøtet i Norsk Senter for Informasjonssikring

UAVHENGIG REVISORS BERETNING

Uttalelse om revisjonen av årsregnskapet

Konklusjon

Vi har revidert Norsk Senter for Informasjonssikrings årsregnskap som viser et overskudd på kr 606 257. Årsregnskapet består av balanse per 31. desember 2019, resultatregnskap for regnskapsåret avsluttet per denne datoen og noter til årsregnskapet, herunder et sammendrag av viktige regnskapsprinsipper.

Etter vår mening er det medfølgende årsregnskapet avgitt i samsvar med lov og forskrifter og gir et rettviseende bilde av organisasjonens finansielle stilling per 31. desember 2019, og av dens resultater for regnskapsåret avsluttet per denne datoen i samsvar med regnskapslovens regler og god regnskapsskikk i Norge.

Grunnlaget for konklusjonen

Vi har gjennomført revisjonen i samsvar med lov, forskrift og god revisjonsskikk i Norge, herunder de internasjonale revisjonsstandardene International Standards on Auditing (ISA-ene). Våre oppgaver og plikter i henhold til disse standardene er beskrevet i Revisors oppgaver og plikter ved revisjon av årsregnskapet. Vi er uavhengige av organisasjonen slik det kreves i lov og forskrift, og har overholdt våre øvrige etiske plikter i samsvar med disse kravene. Etter vår oppfatning er innhentet revisjonsbevis tilstrekkelig og hensiktsmessig som grunnlag for vår konklusjon.

Styrets og daglig leders ansvar for årsregnskapet

Styret og daglig leder (ledelsen) er ansvarlig for å utarbeide årsregnskapet i samsvar med lov og forskrifter, herunder for at det gir et rettviseende bilde i samsvar med regnskapslovens regler og god regnskapsskikk i Norge. Ledelsen er også ansvarlig for slik intern kontroll den finner nødvendig for å kunne utarbeide et årsregnskap som ikke inneholder vesentlig feilinformasjon, verken som følge av misligheter eller utilsiktede feil.

Ved utarbeidelsen av årsregnskapet må ledelsen ta standpunkt til organisasjonens evne til fortsatt drift og opplyse om forhold av betydning for fortsatt drift. Forutsetningen om fortsatt drift skal legges til grunn for årsregnskapet så lenge det ikke er sannsynlig at virksomheten vil bli avvirket.

Revisors oppgaver og plikter ved revisjonen av årsregnskapet

Vårt mål er å oppnå betryggende sikkerhet for at årsregnskapet som helhet ikke inneholder vesentlig feilinformasjon, verken som følge av misligheter eller utilsiktede feil, og å avgi en revisjonsberetning som inneholder vår konklusjon. Betryggende sikkerhet er en høy grad av sikkerhet, men ingen garanti for at en revisjon utført i samsvar med lov, forskrift og god revisjonsskikk i Norge, herunder ISA-ene, alltid vil avdekke vesentlig feilinformasjon som eksisterer. Feilinformasjon kan oppstå som følge av misligheter eller utilsiktede feil. Feilinformasjon blir vurdert som vesentlig dersom den enkeltvis eller samlet med rimelighet kan forventes å påvirke økonomiske beslutninger som brukerne foretar basert på årsregnskapet.

Som del av en revisjon i samsvar med lov, forskrift og god revisjonsskikk i Norge, herunder ISA-ene, utøver vi profesjonelt skjønn og utviser profesjonell skepsis gjennom hele revisjonen. I tillegg:

- identifiserer og anslår vi risikoen for vesentlig feilinformasjon i årsregnskapet, enten det skyldes misligheter eller utilsiktede feil. Vi utformer og gjennomfører revisjonshandlinger for å håndtere slike risikoer, og innhenter revisjonsbevis som er tilstrekkelig og hensiktsmessig som grunnlag for vår konklusjon. Risikoen for at vesentlig feilinformasjon som følge av misligheter ikke blir avdekket, er høyere enn for feilinformasjon som skyldes utilsiktede feil, siden misligheter kan innebære samarbeid, forfalskning, bevisste utelatelser, uriktige fremstillinger eller overstyring av intern kontroll.
- opparbeider vi oss en forståelse av den interne kontroll som er relevant for revisjonen, for å utforme revisjonshandlinger som er hensiktsmessige etter omstendighetene, men ikke for å gi uttrykk for en mening om effektiviteten av organisasjonens interne kontroll.
- evaluerer vi om de anvendte regnskapsprinsippene er hensiktsmessige og om regnskapsestimater og tilhørende noteopplysninger utarbeidet av ledelsen er rimelige.
- konkluderer vi på hensiktsmessigheten av ledelsens bruk av fortsatt drift-forutsetningen ved avleggelsen av årsregnskapet, basert på innhentede revisjonsbevis, og hvorvidt det foreligger vesentlig usikkerhet knyttet til hendelser eller forhold som kan skape tvil av betydning om organisasjonens evne til fortsatt drift. Dersom vi konkluderer med at det eksisterer vesentlig usikkerhet, kreves det at vi i revisjonsberetningen henleder oppmerksomheten på tilleggsopplysningene i årsregnskapet, eller, dersom slike tilleggsopplysninger ikke er tilstrekkelige, at vi modifiserer vår konklusjon om årsregnskapet. Våre konklusjoner er basert på revisjonsbevis innhentet inntil datoen for revisjonsberetningen. Etterfølgende hendelser eller forhold kan imidlertid medføre at organisasjonen ikke fortsetter driften.
- evaluerer vi den samlede presentasjonen, strukturen og innholdet i årsregnskapet, inkludert tilleggsopplysningene, og hvorvidt årsregnskapet gir uttrykk for de underliggende transaksjonene og hendelsene på en måte som gir et rettviseende bilde.

Vi kommuniserer med dem som har overordnet ansvar for styring og kontroll blant annet om det planlagte omfanget av revisjonen og til hvilken tid revisjonsarbeidet skal utføres. Vi utveksler også informasjon om forhold av betydning som vi har avdekket i løpet av revisjonen, herunder om eventuelle svakheter av betydning i den interne kontrollen.

Uttalelse om andre lovmessige krav

Konklusjon om registrering og dokumentasjon

Basert på vår revisjon av årsregnskapet som beskrevet ovenfor, og kontrollhandlinger vi har funnet nødvendig i henhold til internasjonal standard for attestasjonsoppdrag ISAE 3000 *Attestasjonsoppdrag som ikke er revisjon eller forenklet revisorkontroll av historisk finansiell informasjon*, mener vi at ledelsen har oppfylt sin plikt til å sørge for ordentlig og oversiktlig registrering og dokumentasjon av organisasjonens regnskapsopplysninger i samsvar med lov og god bokføringskikk i Norge.

Gjøvik, 19. mars 2020
Deloitte AS

Thomas Hagen Alm
statsautorisert revisor

PENNEO

Signaturene i dette dokumentet er juridisk bindende. Dokument signert med "Penneo™ - sikker digital signatur".
De signerende parter sin identitet er registrert, og er listet nedenfor.

"Med min signatur bekrefter jeg alle datoer og innholdet i dette dokument."

Thomas Hagen Alm

Statsautorisert revisor

På vegne av: Deloitte AS

Serienummer: 9578-5999-4-1419315

IP: 217.173.xxx.xxx

2020-03-24 07:28:53Z



Penneo Dokumentnøkkel: UXXAN-T07YV-CTKXP-AUMTZ-NE1EH-6QLDU

Dokumentet er signert digitalt, med **Penneo.com**. Alle digitale signatur-data i dokumentet er sikret og validert av den datamaskin-utregnede hash-verdien av det opprinnelige dokument. Dokumentet er låst og tids-stemplet med et sertifikat fra en betrodd tredjepart. All kryptografisk bevis er integrert i denne PDF, for fremtidig validering (hvis nødvendig).

Hvordan bekrefter at dette dokumentet er originalen?

Dokumentet er beskyttet av ett Adobe CDS sertifikat. Når du åpner dokumentet i

Adobe Reader, skal du kunne se at dokumentet er sertifisert av **Penneo e-signature service <penneo@penneo.com>**. Dette garanterer at innholdet i dokumentet ikke har blitt endret.

Det er lett å kontrollere de kryptografiske beviser som er lokalisert inne i dokumentet, med Penneo validator - <https://penneo.com/validate>



Teknologiveien 22

2815 Gjøvik

Org.nr. 995195003

Telefon: 40 00 58 99

www.norsis.no

post@norsis.no