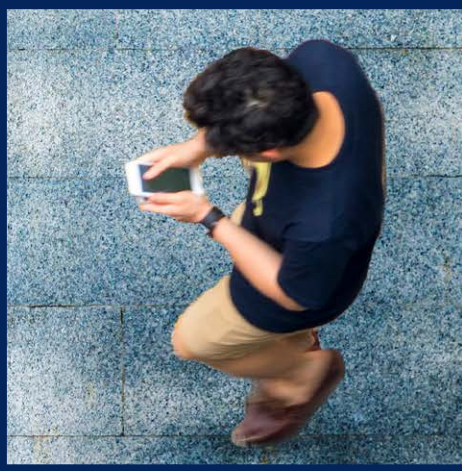
NorSIS



ÅRSRAPPORT 2021

INNHOLD

RAPPORT

ÅRSREGNSKAP

VI MÅ BYGGE EN SIKKERHETSKULTUR

De digitale truslene og angrepene øker i omfang – det gjør også vår sårbarhet. Nå trenger vi et partnerskapssamarbeid for å bygge en god digital sikkerhetskultur.

Året som gikk, har vært begivenhetsrikt – på flere måter. Det har knapt gått en uke uten at vi har lest om dataangrep på norske virksomheter, avanserte bedrageriforsøk, utpressing og sikkerhetsbrudd. Og til tross for at dette var det andre året med pandemi og hjemmekontor, skulle det vise seg at vi ikke sto så mye bedre rustet mot nettkriminelle og digitale angrep enn året før.

2021 var også året da Kripos, i samarbeid med blant annet Europol og et knippe andre lands politistyrker, aksjonerte mot hackere i Ukrainia som var mistenkt for blant annet å stå bak angrepet mot Hydro i 2019. Det representerer på mange måter et veiskille – en anerkjennelse av at digital kriminalitet er et felles problem og en kollektiv vilje til å gjøre noe med det.

De siste par årene har vist oss at vi trenger en oppgradering av holdninger og adferd. Vi må bygge en nasjonal, digital sikkerhetskultur, og det er enkeltmennesket som sitter med nøkkelen. Samtidig er det arbeidsgiver som må lære oss å bruke den.

Pekefingermoral har ingen hensikt når det vi trenger er en kultur der folk tør å si fra hvis de har kommet i skade for å klikke på noe, åpne noe eller surfe på noe de ikke burde – uten å måtte føle seg dumme eller skyldige. For ansatte og borgerne handler det om å lære å skille sant fra usant, gjenkjenne de farene som lurer og be om hjelp hvis uhellet først er ute.

To typer trusler har økt spesielt i 2021. Den ene er sosial manipulering, hvor kriminelle spiller på elementer som frykt, tillit og fristelser. Det kan være i form av falske virusvarsler eller pornosvindler, at de utgir seg for å være aktører man stoler på – eller lokker med gevinster eller penger tilbake på skatten.

Den andre er digital utpressing og løsepengevirus, som den siste tiden har økt med flere hundre prosent i omfang. For de kriminelle er risikoen fortsatt liten og gevinsten potensielt stor, men for virksomhetene som rammes, kan konsekvensene være massive. I verste fall rammer det samfunnskritisk infrastruktur.

Etter hvert som grensene stengte, søkte kriminelle grupperinger til nye forretningsområder, og på internett finnes ingen landegrenser. De kriminelle blir stadig mer kreative, raffinerte og profesjonelle – rene innovatører som ligger et hestehode foran næringsliv og ordensmakt i å tenke nye løsninger. Den gebrokne telefonsamtalen på engelsk fra noen som påstår at de ringer fra Microsoft, eller e-posten fra finansministeren i Nigeria, er historie. Dagens svindelforsøk er personalisert og skreddersydd. De refererer til navn på personer man kjenner og bruker ekte e-postadresser, og de både prater og skriver norsk.

Å bygge den digitale sikkerhetskulturen som gjør at vi sammen står godt rustet for

To typer trusler har økt spesielt i 2021: sosial manipulering samt digital utpressing og løsepengevirus.

å møte denne typen trusler, er ikke noe bedrifter eller enkeltpersoner løfter på egen hånd. Vi som samfunn har et kollektivt ansvar for å skape morgendagens sikkerhetskultur, fordi de samfunnsøkonomiske konsekvensene av dårlig sikkerhet – også på individnivå – er et felles problem.

Digital kriminalitet har ingen grenser. Enkeltpersoner jobber i privat eller offentlig sektor. Store virksomheter med gode sikkerhetssystemer bruker mindre underleverandører uten den samme kompetansen. Den andres problem blir fort ditt eget. Derfor må vi jobbe sammen for å skape en partnerskapsmodell for digital sikkerhet – hvor politikere, kommuner, organisasjoner, næringsliv og fagmiljøer trekker i flokk.

Inn i 2022 – og videre – vil vi i NorSIS være spydspissen for det arbeidet. Derfor vil vi intensivere innsatsen med opplæring og holdningsarbeid mot enkeltpersoner og små og mellomstore virksomheter, samarbeide tett med myndighetene og gjøre det vi kan for å samle bransje og næringsliv for å bygge en solid norsk sikkerhetskultur. Vi håper at vi får flere med på dugnaden.

Lars-Henrik Gundersen
administrerende direktør

«God nasjonal sikkerhetskultur styrker velferdssamfunnet, skaper verdier og verner om demokratiet.»

DETTE ER NORSIS

Norsk senter for informasjonssikring (NorSIS) er en uavhengig organisasjon og medlemsforening. Vi arbeider for at alle skal ha en trygg digital hverdag.

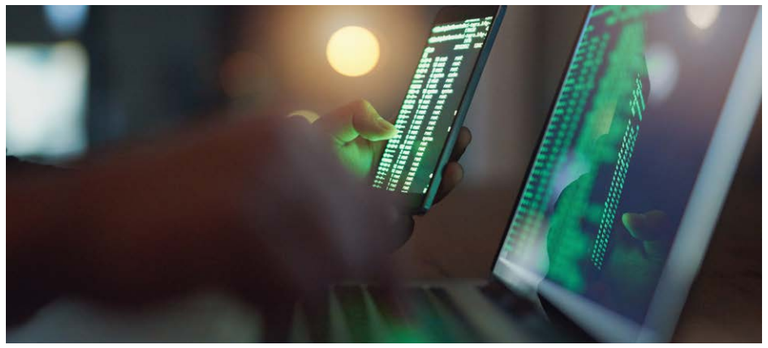
Livet blir mer digitalisert for de aller fleste av oss – alt fra arbeidshverdagen, privatøkonomien og digitale løsninger i hjemmet til offentlig tjenestetilbud og detaljhandel. I dag er så godt som alle deler av samfunnet i større eller mindre grad digitalisert.

I takt med denne utviklingen, øker også vår digitale sårbarhet. Det gjelder oss som enkeltmennesker, virksomheter – og samfunnet som helhet. Vi mener god nasjonal sikkerhetskultur styrker velferdssamfunnet, skaper verdier og bidrar til å verne om demokratiet. Derfor er god sikkerhetskultur og en trygg digital hverdag et viktig samfunnsprosjekt.

Vi jobber hver dag for å fylle vårt samfunnsoppdrag – med særlig fokus på allmennheten og små og mellomstore bedrifter. Det gjør vi gjennom veiledning og opplæring, nettverksbygging, kunnskapsdeling og kommunikasjon for å styrke befolkningens holdninger og adferd knyttet til informasjonssikkerhet.

I tråd med egne vedtekter og tildelingsbrev fra Justisdepartementet skal NorSIS:

- være et nasjonalt og uavhengig ekspertorgan, en kunnskapsforvalter og kulturutvikler innen informasjonssikkerhet
- være en attraktiv og verdifull samarbeidspartner
- informere og dele kunnskap som skaper forståelse, og påvirke adferd som gir en tryggere digital hverdag



Våre verdier

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 oppdatert, dynamiske og omstillingsvillige og ha en optimistisk holdning til ny teknologi.
- Vi skal være oppdatert på målgruppenes 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.

NorSIS:

- er en ideell og uavhengig organisasjon og medlemsforening som ble stiftet i 2009
- er en videreføring av Senter for informasjonssikring (SIS), som ble opprettet av Handels- og næringsdepartementet som et prøveprosjekt i 2000
- er lokalisert på Gjøvik med kontor i Oslo
- har per 31. desember 2021 åtte fast ansatte og én på engasjement. Fem studenter er engasjert på deltid. NorSIS' medarbeidere har solid kompetanse innen informasjonssikkerhet

ÅRET SOM BLOTTSTILTE VÅR SÅRBARHET

2021 var preget av stortingsvalg, polariserte debatter og pandemi. Det var også et år som viste oss vår digitale sårbarhet som samfunn.

Hjemmekontortilværelsen i 2021 påvirket hvordan vi opplever sikkerhet og risiko. Både befolkningen og virksomhetene ble mer digitalt modne. Men selv om befolkningen har blitt mer sikkerhetsbevisste, har ikke den faktiske sikkerheten nødvendigvis blitt bedre av den grunn.

Løsepengevirus, kryptovirus og svindelforsøk mot både privatpersoner og virksomheter preget både folks bekymringer og mediebildet.

– Vi ser at bevisstheten omkring digital sikkerhet øker – og hele 20 prosent er mer bekymret for egen datasikkerhet sammenlignet med året før, ifølge en befolkningsundersøkelse som NorSIS bestilte fra YouGov i 2021. Samtidig ser vi også at trusselen fra organiserte kriminelle øker. Det innebærer at risikoen er større enn noen gang, sier seniorrådgiver i NorSIS, Vidar Sandland.

2021 viste hvor sårbare vi er

Eksemplene fra fjoråret er mange og til dels oppsiktsvekkende. Angrepet på Østre Toten kommune fikk stor oppmerksomhet på begynnelsen av året. Ett eneste massivt løspengevirusangrep lammet alt fra e-post til utbetaling av sosialhjelp, alarmer og medisinutlevering til eldre. Angrepet viste tydelig hvor digitalt sårbare vi er som samfunn. Resten av året så vi en rekke andre store angrep på norske virksomheter, blant annet Stortinget og Amedia. Flere av disse angrepene har det til felles at de har potensial til å sette samfunnskritisk infrastruktur ut av spill.

– En tydelig trend de siste årene er at kriminelle blir stadig proffere og mer utspekulerte – de gjør grundigere research på virksomheten de ønsker å angripe, og iverksetter ikke et angrep når det ikke er penger å hente. Dette kan forklare hvorfor vi i fjor opplevde så mange angrep på store virksomheter med stor betalingsevne. Angrep rammer også små og mellomstore virksomheter, gjerne som ledd i målrettede angrep mot større virksomheter. Det er trolig mørketall i antall angrep, fordi ikke alle angrep lenger ute i verdikjeden er kjent, og fordi mange virksomheter ikke ønsker offentlighet rundt hendelser de er utsatt for, sier Sandland.

Digital utpressing er trolig den største digitale trusselen mot virksomheter i europeisk sammenheng, og ENISA anslo i 2019 at 10,1 milliarder euro ble utbetalt i løsepenger. Alt tyder på at trusselen bare vil øke.

Individet er veien inn

Kriminelle angripere velger ofte den letteste veien inn i en virksomhet. Det betyr ofte de ansatte. Ifølge Mørketallsundersøkelsen 2020 fra Næringslivets sikkerhetsråd skyldes hele 50 prosent av sikkerhetsbruddene i norske virksomheter menneskelige feil.

– Alt som skal til er én uheldig ansatt som åpner feil vedlegg eller tillater å installere noe etter å ha klikket på en lenke, dette kan lamme en hel virksomhet, sier Sandland.

– Vi må ta ansvaret bort fra brukeren

Et viktig tiltak, som NorSIS har fokusert på i 2021, er å få flere til å aktivere totrinnsbekreftelse.

En YouGov-undersøkelse NorSIS gjennomførte i 2021 viser at 65 prosent vet hva totrinnsbekreftelse er – men at bare 38 prosent av disse bruker det. Det er også tydelige tegn på at bruken av totrinnsbekreftelse flater ut.

– Tiden er derfor inne for å tenke nytt om hvordan vi oppfordrer folk til å ta dette og andre viktige sikkerhetstiltak i bruk. At bevisstheten øker er bra, så lenge vanene følger etter. Da må både arbeidsgivere og storsamfunnet komme enda tydeligere på banen. Dette vil prege arbeidet vårt i 2022, slår Sandland fast.

8%
av alle nordmenn ble utsatt for løsepengevirus*

8 av 10
datainnbrudd i sky- og lagringstjenester er knyttet til kompromitterte passord**

10%
av alle nordmenn har mistet full kontroll over egne e-post- eller sosiale medier-kontoer*

6 av 10
ledere tillater bruk av privat datautstyr***

32%
av ledere tillater nedlastning av programvare på jobb-PC eller mobil uten godkjenning***

18%
har lagt igjen sensitiv informasjon som personnummer og kontonummer uten å vite hvem som eier den****

* YouGov-undersøkelse for NorSIS, juli 2020
** Securelink/ Verizon Data Breach Report
*** YouGov, lederundersøkelse for NorSIS, 2019
**** YouGov-undersøkelse for Buypass, november 2020

MER RELEVANT ENN NOEN GANG

– Etter to år med pandemi, varierende grad av nedstengning og digitalisering i høyt tempo, er NorSIS som uavhengig aktør innen IT-sikkerhet, mer relevant enn noen gang.

Det mener styreleder i NorSIS, Hans-Henrik Merckoll. Han er til daglig administrerende direktør i IBM Norge og har bakgrunn fra Hewlett Packard, Evry og Telenor. Fra sitt ståsted, sentralt plassert i IT-Norge og med kunder som daglig møter utfordringene det nye, digitale trusselbildet representerer, blir han ofte minnet på betydningen av en organisasjon som NorSIS.

– Jeg hører stadig kunder og forretningsforbindelser refere til NorSIS som den nøytrale stemmen når det gjelder IT-sikkerhet. Og selv om det på ingen måte blir galt å drive business på dette området – det gjør jeg jo selv i IBM – trenger vi aktører med høy grad av troverdighet som både næringslivet og innbyggerne lytter til. At vi også forvalter et samfunnsoppdrag på vegne av myndighetene, både gjennom det generelle informasjonsarbeidet og i form av tjenestene nettvett.no og slettmeg.no, mener jeg styrker den posisjonen.

Å skalere gjennom partnere

På samme måte som de digitale arenaene og trusselbildet endrer seg, er også NorSIS i utvikling for å møte dagens og morgendagens utfordringer.

– Våre primære målgrupper er befolkningen generelt, og SMB-segmentet i næringslivet spesielt, sier Merckoll.
– Oppgavene til NorSIS handler mye om å øke bevisstheten om digitale trusler og sårbarheter og deretter informere om konkrete tiltak gjennom nyheter, råd og veiledning. Vi er en «påvirkningsaktør» med et mål om å bidra til å skape gode holdninger innen informasjonssikkerhet.

Gitt størrelsen til organisasjonen som har hovedkontor på Gjøvik, blir det også et poeng å jobbe gjennom et nettverk av partnere som skalerer NorSIS' rekkevidde.
– Vi har tradisjon for å jobbe partnerbasert, og dette vil også være strategien fremover. Det handler om samarbeid med organisasjoner som SMB Norge og Digital Norway, men også om prosjekter sammen med næringslivsaktører, som for eksempel Security Divas, der Accenture har en sentral rolle.

Tre forhold som påvirker sikkerheten

På spørsmål om hvordan styrelederen og IT-toppen oppsummerer dagens trusselbilde, trekker han frem særlig tre forhold.

– Vi blir stadig mer eksponert, i takt med at produkter, tjenester og prosesser blir digitale. Dermed blir vi også mer sårbare dersom viktige digitale arbeidsverktøy faller bort. Kostnadene ved å bli kompromittert kan fort bli enorme for dem som ikke har forberedt seg godt, både med et forsvar og planer for gjenoppbygging.

– De store verdiene ligger i data. Det handler om informasjon om privatpersoner, forbrukere, industrielle prosesser, helse- og treningsdata – det finnes knapt grenser for hva som legger igjen spor og datapunkter når samfunnet blir digitalt.

«Vi er en påvirkningsaktør med et mål om å bidra til å skape gode holdninger innen informasjonssikkerhet.»

Hans-Henrik Merckoll, styreleder i NorSIS

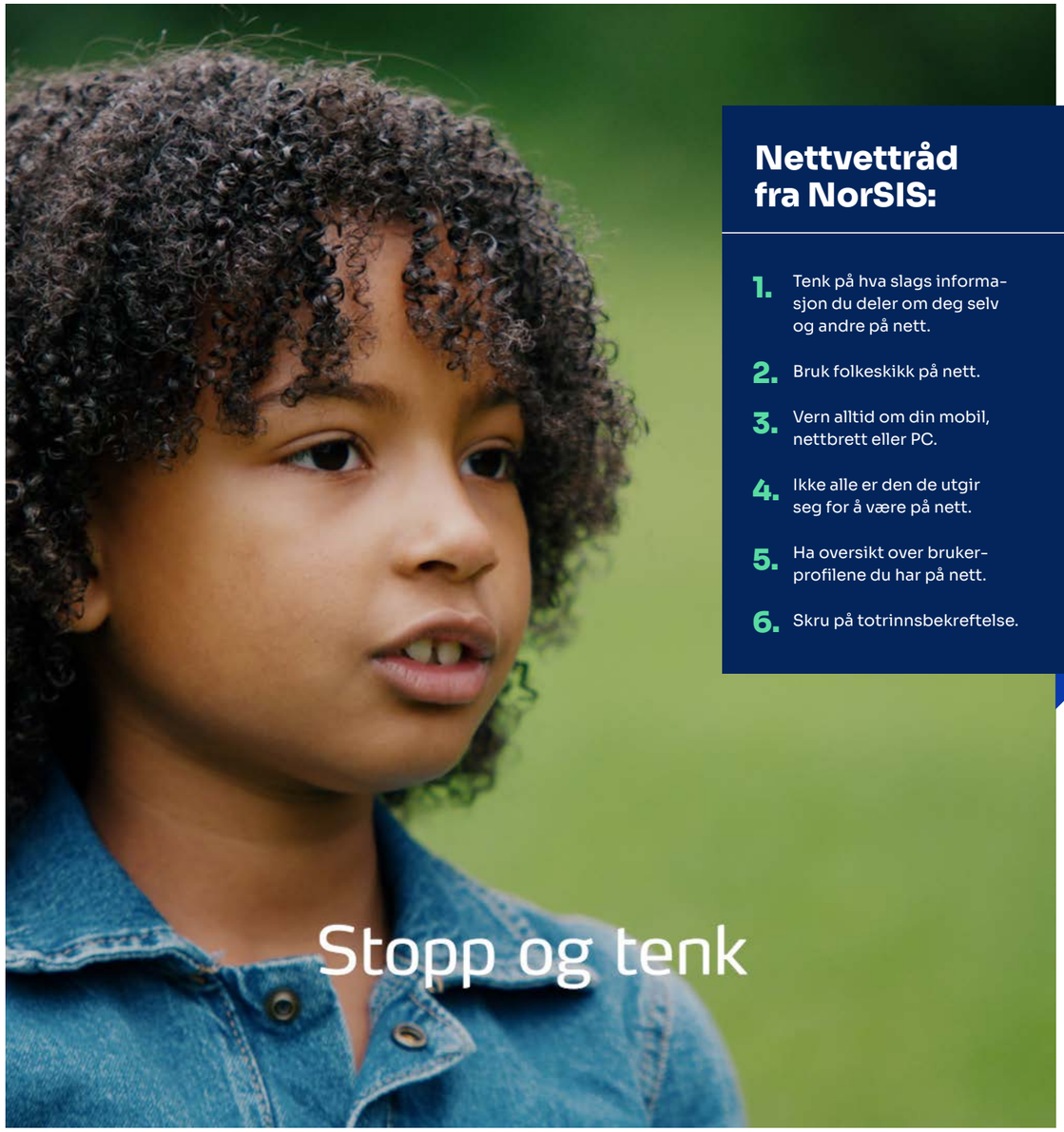
Å få tilgang til disse, representerer store muligheter – også for kriminelle.

– De kriminelle ligger foran, de tilpasser seg, er tidlig ute med ny teknologi – og spiller på den grunnleggende tilliten som får Norge og andre demokratiske samfunn til å fungere effektivt. Det er verdt å minne oss selv på at det ikke bare er økonomiske verdier som står på spill, men samfunnsverdier og kvaliteter knyttet til vårt demokratiske system.

En digital sikkerhetskultur

– I møte med denne utviklingen er NorSIS opptatt av det vi kaller en digital sikkerhetskultur – både i næringslivet og på hjemmebane. Og god sikkerhet innebærer en balanse: Vi trenger nok kunnskap, sunn skepsis og grunnleggende holdninger. Så må vi også bruke teknologien for det den er verdt, slå på de sikkerhetsmekanismene som finnes og lage passord som er sterke nok. Hvis sikkerheten er effektiv, uten å gjøre brukerne ineffektive, da har vi funnet den balansen som gjør det mulig å overbevise folk – gjennom informasjon og opplæring – om at for eksempel tofaktorautentisering er verdt den ekstra lille omveien.

– Denne sikkerhetskulturen skapes av myndigheter, virksomheter, organisasjoner og enkeltpersoner i samarbeid – og NorSIS har en sentral rolle, avslutter styreleder Hans-Henrik Merckoll.



Nettvettråd fra NorSIS:

1. Tenk på hva slags informasjon du deler om deg selv og andre på nett.
2. Bruk folkeskikk på nett.
3. Vern alltid om din mobil, nettbrett eller PC.
4. Ikke alle er den de utgir seg for å være på nett.
5. Ha oversikt over brukerprofilene du har på nett.
6. Skru på totrinnsbekreftelse.

Kampanjen «Stopp – tenk deg om»

252
medieoppslag

Over
3,5 mill.
filmvisninger

2966
visninger av kampanjesiden

VÅRE NETTVETTRÅD TIL BEFOLKNINGEN

Vi jobber kontinuerlig for å bygge god digital dømmekraft blant Norges befolkning – både unge og gamle. Folkeopplysningskampanjen «Stopp – tenk deg om», som vi gjennomførte i 2021, var en viktig del av dette arbeidet.

Kampanjens mål var å øke privatpersoners kunnskap slik at de bedre kunne beskytte personvernet og sine digitale verdier.

– Dette er et mål vi jobber mot hver dag. Vi bevisstgjør befolkningen på konsekvenser og oppfordrer til refleksjon, forteller Karoline Hultman Tømte, leder for partnerskap og myndighetskontakt i NorSIS.

Det finnes dessverre ingen enkel løsning på å bekjempe netthets og svindel. Det er mange gråsoner, og mye som juridisk sett er lovlig, men som likevel ikke er akseptabel oppførsel.

Vi jobber forebyggende:
Stopp – tenk deg om
Kampanjen, som gikk fra juli til og med Nasjonal sikkerhetsmåned i oktober, var et samarbeid mellom NorSIS, politiet, Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap (DSB) og Justis- og beredskapsdepartementet.

– Folkeopplysningskampanjer er et viktig bidrag for å øke motstandsdyktigheten mot uønsket påvirkning og digital svindel. Evnen til å forstå at ikke alt vi hører og ser på nett er det som det utgir seg for å være, er en viktig egenskap for å beskytte sine egne og samfunnets verdier, sier Roar Thon, fagdirektør i NSM.

For at kampanjen skulle nå den overordnede målsetningen om bevisstgjøring og godt nettvett best mulig, utarbeidet vi følgende budskap som grunnmur:

Stopp – tenk deg om. Du kan faktisk avsløre både svindler, falske nyheter og unngå å si noe du senere angrer på ved å tenke deg om en ekstra gang før du foretar deg noe på nett.

Det ble skrevet seks pressemeldinger som totalt genererte hele 252 medieoppslag. I tillegg ble det produsert åtte filmer som sirkulerte i sosiale medier gjennom kampanjeperioden.

Filmene fikk over 3,5 millioner visninger.

– Det er vi svært fornøyde med, sier Tømte.

For å gi befolkningen konkrete råd, verktøy og hjelpemidler for å ta bedre digitale valg for seg selv og sine nærmeste, ble det opprettet en kampanjeside der besøkende kunne finne mer informasjon og konkrete råd. Disse rådene ble også delt som del av det totale kampanjeløpet. Kampanjesiden, norsis.no/tenk, fikk 2966 sidevisninger i kampanjeperioden.

Bekjemper hat og falske nyheter med kunnskap
Kampanjen var en viktig del av informasjonsarbeidet til NorSIS og samarbeidspartnere i forkant av fjorårets stortingsvalg.

– Ved å oppfordre befolkningen til å være kildekritiske og tenke over hva slags informasjon de finner på internett, og hvem som står bak, gjør vi dem bedre rustet til å stå imot svindelforsøk, falske nyheter og desinformasjon. Derfor er digital dømmekraft og kildekritikk helt avgjørende for demokratiet, slår hun fast.

Karoline Tømte understreker at dette er et langsiktig arbeid.

– Det er en viktig del av vårt pågående og kontinuerlige arbeid å minne folk på nettvettrådene. En kampanje endrer ikke holdningene og handlingene til folk på nett, men hvis budskapet gjentas ofte nok, vil vi på sikt se at det norske folks nettvaner bedrer seg, avslutter hun.

«Vi bevisstgjør befolkningen på konsekvenser og oppfordrer til refleksjon.»

Karoline Hultman Tømte, leder for partnerskap og myndighetskontakt i NorSIS

Nordmenn og digital sikkerhetskultur

– VI BEKYMRER OSS MER FOR DIGITAL RISIKO

Vi bekymrer oss mer for digital risiko. Det viser NorSIS' årlige undersøkelse om nordmenn og sikkerhetskultur. Men betyr det at vi blir bedre på sikkerhet?

Det er et av spørsmålene den årlige rapporten «Nordmenn og digital sikkerhetskultur» ønsker å besvare. Rapporten baserer seg på en representativ spørreundersøkelse gjennomført av analyseinstituttet YouGov blant mer enn 1000 respondenter.

Den kartlegger hovedstrømningene og beskriver hvordan det norske folk opplever digital risiko – og hvor god sikkerhetskulturen er blant oss.

Økt risikoopplevelse
Hva bekymrer vi oss over? I hvilken grad etterlever vi sikkerhetsråd? Hvordan påvirker den kunnskapen vi har, nettadferden vår? Og hvordan tilegner vi oss kunnskap om sikkerhetskultur?

Et hovedfunn er at stadig flere – 33 prosent – føler at den digitale risikoen har økt. Vi opplever høyere risiko knyttet til våre egne handlinger, som å bruke samme passord på flere tjenester. Samtidig frykter flere å bli utsatt for datakriminalitet, som at bankkortene våre blir misbrukt.

Det er en økning fra 24 prosent ved inngangen på pandemien. Og det er ikke uten grunn at vi bekymrer oss. De kriminelle blir stadig smartere, og vi ser oftere vellykkede digitale angrep mot norske virksomheter. Kombinert med utstrakt bruk av hjemmekontor og digitale løsninger, privat og i jobbsammenheng, har dette trolig bidratt til at bekymringsnivået har økt i løpet av pandemien.

Svak bedring av norske vaner
I takt med at flere av oss uttrykker bekymring for den digitale risikoen, ser vi tegn til at bevisstheten om digital sikkerhet øker på flere områder.

Flere sjekker – 76 prosent mot 71 prosent året før – lenker eller vedlegg før de åpner dem, og 58 prosent undersøker om en nettside er trygg. 35 prosent oppgir at de sikkerhetskopierer viktige private data månedlig eller oftere. Det mistenker vi er et kunstig lavt tall ettersom mange har skylagring som sikkerhetskopierer automatisk.

På andre områder har det skjedd mindre. Bare halvparten – 49 prosent – bruker fremdeles totrinnsbekreftelse. Også nordmenns passordvaner er i stor grad uendret. 42 prosent benytter ulike passord for de fleste tjenestene på nett, mens 35 prosent er opptatt av å lage sikre passord.

Mange opplever digital mestring – men 1 av 10 faller utenfor
Nytt i 2021-undersøkelsen var spørsmålet om hvilken grad av mestring folk flest opplever innen digital sikkerhet. Hensikten var å avdekke i hvilken grad nordmenn mener at de vil klare å utføre noen av de mest grunnleggende tiltakene som beskytter dem mot digitale trusler.

Funnene viser at mange håndterer viktige sikkerhetsrutiner. 55 prosent vet hvordan de aktiverer totrinnsbekreftelse, og 60 prosent er i stand til å vurdere om lenker og vedlegg er trygge.

Samtidig innrømmer så mange som 7 til 11 prosent at de i liten grad mestrer sentrale sikkerhetsaktiviteter. En annen trend er at andelen som bevisst bryter det de opplever som regler for informasjonssikkerhet, stiger – fra 11 prosent i 2017 til 17 prosent i 2021.

Dette opplever vi som mest risikofylt – topp fem

79%	å dele passord med andre
68%	å bruke samme passord på flere nettjenester
60%	å ikke ta sikkerhetskopi
49%	å ikke bruke totrinnsbekreftelse
41%	å delta i pengespill på nett

32%
mener den digitale risikoen har økt for dem selv som følge av koronapandemien

24%
har fått opplæring de siste to årene

1 av 10
mestrer ikke sentrale sikkerhetstiltak

49%
bruker totrinnsbekreftelse

42%
bruker ulike passord for de fleste tjenestene på nett

35%
er bevisst sikre passord

– VI TRENGER BEDRE OG MER OPPLÆRING!

– Holdninger til sikkerhet endres ikke over natten, og de positive endringene vi ser, har nok skjedd over en lengre periode.

Det sier seniorrådgiver i NorSIS, Eivind Reiner-Holm. Han var sentral i utviklingen og gjennomføringen av «Nordmenn og digital sikkerhetskultur» i 2021. Da gjennomgikk også rapporten en revisjon.

Fra å være en publikasjon på rundt 70 sider, ble den kokt ned til en konkret og lettfattelig rapport som enkelt viser frem hovedfunnene fra undersøkelsen. Hensikten var å gjøre den mer tilgjengelig for leseren – det være seg media, bedrifter, privatpersoner eller politikere og myndigheter.

– Det er mye som er positivt. Mange har fått bedre vaner, og det faktum at folk er bekymret tyder på en økt bevissthet omkring de truslene som finnes. Samtidig ser vi at altfor mange fremdeles har en lang vei å gå.

Han mener god opplæring er nøkkelen. Til tross for et komplekst trusselbilde, viser nemlig tall fra undersøkelsen at andelen nordmenn som har fått organisert opplæring i datasikkerhet, nærmest har stått stille de siste årene. Kun 1 av 4 respondenter oppgir at de har fått organisert opplæring i løpet av de to siste årene. Reiner-Holm advarer norske arbeidsgivere.

– Den enkelte kan ikke være overlatt til seg selv. Vi ser tydelig at gode vaner styrkes når folk får opplæring i datasikkerhet. Da må arbeidsgivere ta ansvar og jobbe aktivt for å skape en god digital sikkerhetskultur blant sine ansatte. Det er rett og slett lønnsomt. Kunnskap er grunnmuren til god sikkerhetskultur, og virksomheten er aldri sterkere enn det svakeste leddet, avslutter han.

NASJONAL SIKKERHETSMÅNED

NorSIS koordinerer Nasjonal sikkerhetsmåned i Norge på vegne av Justis- og beredskapsdepartementet. Sikkerhetsmåneden er en del av EUs informasjonssikkerhetsorgan ENISAs årlige europeiske sikkerhetsmåned.

Formålet med Nasjonal sikkerhetsmåned er å øke engasjementet, bevisstheten og kunnskapen om digital sikkerhet, både i befolkningen og i små og store virksomheter. I 2021 var temaet for sikkerhetsmåneden «en trygg digital hverdag for alle», med undertemaene «forebygging og digital førstehjelp». Tematikken tok utgangspunkt i hovedbudskapene i den europeiske sikkerhetsmåneden.

Slik løste vi oppdraget
Nasjonal sikkerhetsmåned skal blant annet bidra til å videreutvikle møteplasser og arenaer for å bygge kompetanse og erfaring, samt synliggjøre viktige tiltak for bedret digital sikkerhet for målgruppen. Dette var bakgrunnen for at NorSIS planla og koordinerte følgende arrangementer i løpet av sikkerhetsmåneden:

- åpningsmarkering av Nasjonal sikkerhetsmåned, i samarbeid med Kripos
- nettverksseminar for Security Divas, i samarbeid med Accenture
- cybersecurity-seminar på Stortinget, i samarbeid med SMB Norge

Åpningsmarkeringen ble holdt hos Kripos og innledet av justis- og beredskapsminister Monica Mæland. Flere bidro med faglige innlegg i etterkant, blant annet den skandinaviske entreprenørkjeden GK som ble rammet av et løsepengevirus sommeren 2021.

Nettverksseminaret for Security Divas ble arrangert av NorSIS og vår samarbeidspartner Accenture. Samlingen inneholdt ulike foredrag om sikkerhet og teknologi. Til tross for pandemien var det godt fremmøte med rundt 40 deltakere.

I slutten av sikkerhetsmåneden arrangerte NorSIS i samarbeid med SMB et seminar om cybersecurity på Stortinget. Her ble det rettet fokus mot hvilke utfordringer SMB-sektoren har når det gjelder cybersecurity generelt. Det var også et tema hvilket ansvar styret i bedriften har for datasikkerhet. Bedriftsledere, stortingsrepresentanter og politiske rådgivere deltok, til sammen rundt 50 stykker.

For å koordinere aktiviteter og synliggjøre alle de spennende aktivitetene som ble gjennomført i sikkerhetsmåneden, opprettet vi en aktivitetsoversikt for våre egne og andres arrangementer og aktiviteter.

«Foredragsdugnaden er et etterspurt og populært tilbud under sikkerhetsmåneden. Responsen blant både foredragsholdere og publikum vitner om at foredragsdugnaden er en spennende og god måte å formidle kunnskap på.»

Karoline Hultman Tømte,
prosjektleder for Nasjonal sikkerhetsmåned

POPULÆR FOREDRAGSDUGNAD OG GRATIS KURS

NorSIS er opptatt av at den nasjonale sikkerhetsmåneden skal være et fellesprosjekt, og at vi sammen løfter den digitale kompetansen i Norge. Dette er bakgrunnen for at vi også i 2021 arrangerte en foredragsdugnad under sikkerhetsmåneden.

Konseptet går ut på at virksomheter kan bestille gratis foredrag om ulike temaer innenfor informasjonssikkerhet. I 2021 var ekspertene som stilte opp som foredragsholdere, blant annet fra Nasjonal sikkerhetsmyndighet (NSM), politiets IKT-tjenester og en rekke store og små private virksomheter med spisskompetanse innenfor fagfeltet.

Digitale opplæringspakker og gratis kurs
NorSIS har over tid opparbeidet kunnskap og innsikt innenfor digital sikkerhet. Dette har dannet grunnlaget for våre egne opplæringspakker som er utviklet i samarbeid med den digitale læringsplattformen Motimate. Opplæringspakkene består av åtte interaktive og engasjerende opplæringsmoduler tilrettelagt for pc, nettbrett og mobil, med tips og råd for å redusere sjansen for uønskede hendelser og dataangrep på arbeidsplassen og hjemme.
Det var 137 virksomheter og totalt 113 322 ansatte som gjennomførte dette i oktober.

NorSIS har også kurs som er gratis og åpne for alle. Kursene tar opp ulike temaer innen informasjonssikkerhet og er utarbeidet av NorSIS og våre samarbeidspartnere. Alle kursene er samlet på kampanjesiden til sikkerhetsmåneden: sikkert.no.

Kampanje i sosiale medier
Våre kanaler i sosiale medier ble benyttet til eksternkommunikasjon under sikkerhetsmåneden. Vi publiserte kampanjemateriale i form av tekst og videoer utarbeidet av ENISA, og disse ble likt og delt av våre følgere på Facebook, Instragram og LinkedIn.

Folkeopplysningskampanjen «Stopp – tenk deg om» utgjorde også en del av sikkerhetsmåneden, men var mer vinklet mot datasikkerhet/svindel. Kampanjen, som ble gjennomført i juli–oktober, forsterket budskapene i sikkerhetsmåneden.

Erfaringer og veien videre
NorSIS er godt fornøyd med gjennomføringen av sikkerhetsmåneden i 2021. Vi erfarte at samarbeid mellom ulike aktører innen informasjonssikkerhet er en suksessfaktor. Arrangementene ble godt mottatt, og vi mener vi traff med årets tema. Samtidig er det viktig å gjøre fortløpende vurderinger av hvilke behov målgruppen har, og av hvilken plattform de nås best på. Sikkerhetsmåneden blir aldri bedre enn summen av alle som bidrar og deltar. Vi vil jobbe for å få med enda flere samarbeidspartnere i årene fremover, for å nå ut med budskapene til alle målgruppene.

113 322

ansatte i 137 virksomheter benyttet opplæringspakkene våre i løpet av oktober 2021

Fakta om foredragsdugnaden

- **24** ulike foredrag
- **over 100 foredrag** bestilt og gjennomført
- **bidragsytere:** blant annet NSM, KPM og politiet
- **tematikk:** personvern, DarkWeb, digital sikkerhet i skolen, ID-tyveri, teknisk sikkerhetsdialog med leverandør

«I den digitale virkeligheten er det mer krevende å skille mellom det som er falskt og det som er ekte.»

SLETTMEG.NO – EN STØTTESPILLER OG EN RÅDGIVER I MER ENN TI ÅR

Ti år etter etableringen er Slettmeg.no mer nødvendig enn noen gang. Tjenesten blir benyttet av personer i alle aldre, og i en rekke forskjellige situasjoner som spenner fra nakenbilder på avveier, stjålne Facebook-kontoer, ID-tyverier og sjikane.

Slettmeg.no er en gratis rådgivnings- og veiledningstjeneste for å hjelpe personer som blant annet opplever å få personvernet sitt krenket på internett. Tjenesten blir benyttet av personer i alle aldre. De vanligste henvendelsene handler om hjelp til å slette kontoer, utfordringer knyttet til hackede profiler i sosiale medier og bilder eller videoer som er delt uten samtykke.

NorSIS overtok driftsansvaret for Slettmeg.no fra Datatilsynet i 2012. Tjenesten ble i sin tid opprettet som et resultat av Personvernkommisjonen (NOU 2009: 1), som i sin utredning foreslo opprettelse av «en tjeneste som kan bistå de som får sitt personvern krenket på Internett».

Hundretusener sliter digitalt

Digitaliseringen preger stadig større deler av livet vårt, og vi lever tidvis i en digital virkelighet. Vi bygger relasjoner og kommuniserer med andre gjennom sosiale medier, deler bilder og historier. En rapport fra siste kvartal i 2021 viser at 65 prosent av den norske befolkning over 18 år oppgir at de bruker Facebook hver dag (IPSOS Norge, 2021).

Tall fra Medietilsynet viser at 11 prosent av befolkningen har opplevd en eller annen form for sjikane på internett de siste 12 månedene. 20 prosent i alderen 16-25 år har opplevd minst én av sjikaneformene hatefulle ytringer, mobbing, trakassering, trusler om vold eller hetsing eller latterliggjøring i debatter i 2021 (Medietilsynet, 2021). Den årlige undersøkelsen som Response Analyse utfører på vegne av NorSIS og Skatteetaten, viste i 2021 at over 100 000 nordmenn hadde opplevd ID-tyveri de siste to årene. Samtidig viste NorSIS-rapporten «Nordmenn og digital sikkerhetskultur 2021» at hundretusener sliter med å mestre de viktigste sikkerhetsrådene.

Verdifull innsikt

Mulighetene den digitale hverdagen gir oss, er mange, men krever samtidig bevissthet og kunnskap om fallgruvene. I den fysiske verden vet vi hvem vi snakker med. I den digitale virkeligheten er det mer krevende å skille mellom det som er falskt og det som er ekte. Denne sårbarheten utnyttes av kriminelle og kan true vår integritet.

I dette landskapet er slettmeg-tjenesten en støttespiller og rådgiver for innbyggerne. Henvendelsene som kommer inn til oss, blir registrert og analysert, og gir et bilde på hvilke problemstillinger folk står overfor. Dette gir oss verdifull innsikt som vi benytter for å gi nyttige råd, i tillegg til at NorSIS kan bringe informasjonen videre til myndigheter, næringsliv og andre relevante samarbeidspartnere og aktører. Slettmeg-tjenesten bidrar med andre ord til en tryggere digital hverdag for alle.

«Mer enn 100 000 nordmenn har opplevd ID-tyveri de siste to årene.»

ANTALL HACKEDE FACEBOOK-PROFILER SOM ER BEHANDLET AV NORSIS I 2021:

740

ANTALL HACKEDE INSTAGRAM-PROFILER SOM ER BEHANDLET AV NORSIS I 2021:

185

ANTALL SAKER MED HETS* I 2021:

149

*Hets er her definert som saker som er tagget med «mobbing/trakassering» eller «ærekrenkelse»

EN TJENESTE SOM STADIG FLERE TRENGER

– Å være rådgiver i Slettmeg.no gir mening – både når vi lykkes med å hjelpe dem som tar kontakt, men også de gangene vi ikke får gjort så mye mer enn å være en sympatisk lytter som kan forklare en vanskelig situasjon for en frustrert innringer.

Det forteller rådgiverne Vladimir Haug og Iver Hurum, to av personene som svarer når nordmenn i alle aldre tar kontakt med tjenesten Slettmeg.no som NorSIS drifter på vegne av norske myndigheter.

– Det er en klar overvekt av saker fra de yngre aldersgruppene, særlig 12-18 og 19-25, men jeg har hjulpet personer helt opp i 80-årene som har tatt kontakt med oss. Vi vet at begravelsesbyråer anbefaler sine klienter å be oss om hjelp hvis de sliter med å stenge ned kontorer i sosiale medier, og at politiet også henviser til Slettmeg.no i møte med mennesker som prøver å ta tilbake kontrollen over brukere på forskjellige tjenester på nettet – eller som rett og slett ikke forstår brukerveiledningen og hva de skal gjøre for å avslutte en brukerkonto på for eksempel Facebook, Instagram eller Spotify, forklarer Iver Hurum.

Nakenbilder på avveier

De to rådgiverne, som også tar en mastergrad i informasjonssikkerhet på NTNU på Gjøvik, har begge nesten tre års erfaring fra Slettmeg.no-rommet på NorSIS-hovedkontoret. De inngår i et team på fem som jobber i to skift for å bemanne e-post og telefon, og som står klare til å hjelpe – både i akutte situasjoner og når spørsmålene er av enklere karakter.

– Det er mange som er fortvilet når de tar kontakt, og som har gruet seg til å ringe. Nakenbilder på avveier i kombinasjon med utpressing er en type saker vi ser mange av, sier Vladimir Haug. – Og ofte følger disse sakene et relativt likt mønster, der alt starter med at en gutt eller en jente treffer noen på nett som de finner tonen med – og som de tror er jevnaldrende og gjensidig interessert i dem.

– Samtalepartneren foreslår etter hvert at de skal chatte videre på Hangout eller i en annen kanal der de enten kan streame lyd og bilde – eller utveksle bilder med privat innhold. Når de har sikret seg film eller foto, blir det raskt klart at de verken er jevnaldrende eller interessert i noe annet enn penger. De har ofte kartlagt det sosiale nettverket ditt ved hjelp av vennelisten og tidslinjen din på Facebook, og truer raskt med å distribuere bildene til familie og kjente hvis du ikke betaler. Ofte handler det om høye summer, noen ganger i hundretusenkronersklassen. Og det hjelper sjelden å betale – da starter bare utpressingen på nytt, sier Haug.

En god dag på jobben

Iver Hurum fortsetter: – I en sånn situasjon, med mye følelser og fortvilelse, kan vi både være den som lytter – ofte føles det godt å fortelle noen om hva som har skjedd – og prøve å hjelpe dem som ringer, med å få lukket profiler der utpresserne finner informasjon, ta kontakt med politiet for å anmelde og håndtere situasjonen på en måte som kanskje kan hindre at bildene blir publisert.

– I andre situasjoner, der bildene er lagt ut på en pornoside på nett, vet vi hvordan vi skal henvende oss til domeneeierne, hva vi skal be om og hvilke regler og lover vi kan vise til. At vi skriver fra en slettmeg.no-adresse gir ekstra tyngde, og det er liten tvil om at personvernforordningen har gjort det enklere for oss å hjelpe nettbrukere med å få tilbake kontrollen over personlig informasjon som har kommet på avveier.

Iver Hurum og Vladimir Haug hjelper dem som tar kontakt med Slettmeg.no.

– Det skjer selvfølgelig ofte at henvendelsene våre blir ignorert av useriøse tjenesteleverandører, men det er heller ikke uvanlig at vi klarer å ta ned bildene det er snakk om. I 2021 lyktes vi faktisk med å ta ned et helt domene, 24 GB med nakenbilder av norske jenter som var publisert uten at de hadde gitt samtykke eller, for mange av dem, visste om. Det var en god dag på jobben, smiler både Haug og Hurum.

Liv og død – og digitalt hverdagsliv

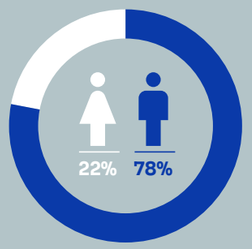
Slettmeg.no mottar flere hundre henvendelser i uken. Spørsmålene og problemstillingene som rådgiverne forsøker å hjelpe med, spenner fra nakenbilder på avveier, ID-tyverier, til avdøde som fortsetter å «leve» på nettet, folk som blir sjikanert og mobbet, trenger hjelp til å få fjernet en feilaktig informasjon – og andre som har mistet tilgang til en blogg som de ikke har brukt på 15 år.

– Av og til står det om liv og død, forteller Vladimir Haug. – Dypt fortvilte mennesker som blir utpresset eller mobbet, og som er drevet helt til grensen av hva de kan tåle. Men ofte bistår vi også personer som har søkt på «slett meg» på Google, og som bare trenger hjelp til å avslutte en brukerkonto på en digital tjeneste. Eller det kan dreie seg om ungdommer som sender inn anonyme spørsmål via ung.no, som vi svarer på.

– Tallene for 2021 viser at bilder og videoer på avveier, hackede kontoer og falske profiler topper listen over saker vi har hjulpet folk med. Men minst like viktig som tallene, er innsikten i trender og mønstre, både over tid og her og nå. Vi er i en unik posisjon til å plukke opp nye utfordringer tidlig, formidle dem videre til kollegaer i NorSIS som deretter kan informere om dem på konferanser, foreslå tiltak og forebygging i møte med myndighetene og bygge kunnskapen inn i den generelle informasjonsvirksomheten, avslutter Vladimir Haug og Iver Hurum.

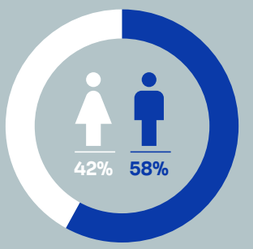
«Det er mange som er fortvilet når de tar kontakt, og som har gruet seg til å ringe.»

ANTALL UTPRESSINGSSAKER FORDELT PÅ KJØNN 2021:



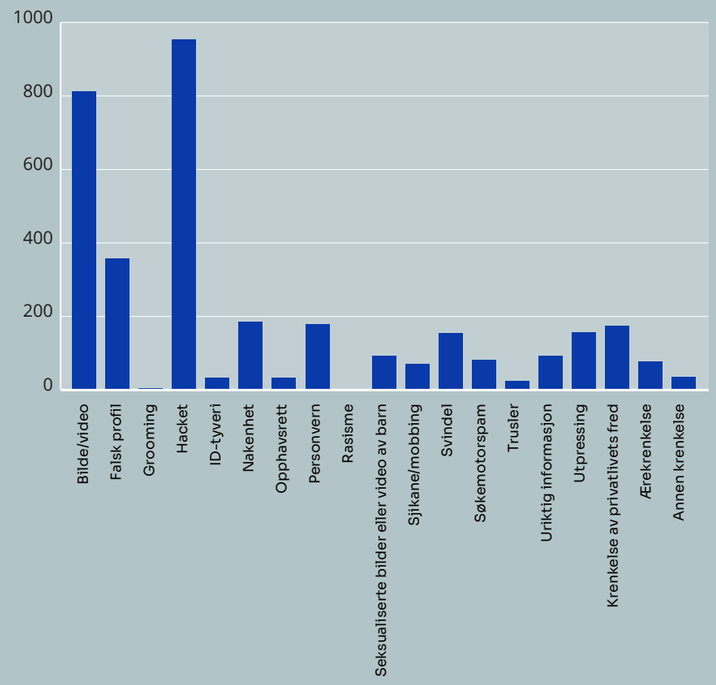
totalt **156** saker

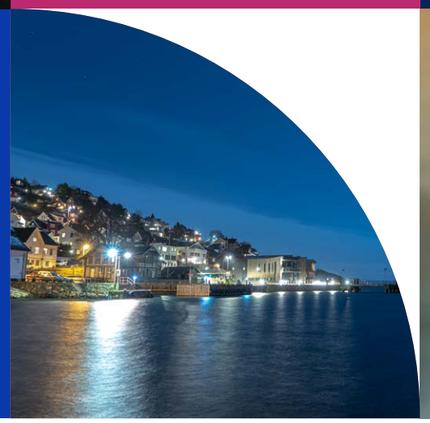
ANTALL SVINDELSAKER FORDELT PÅ KJØNN I 2021:

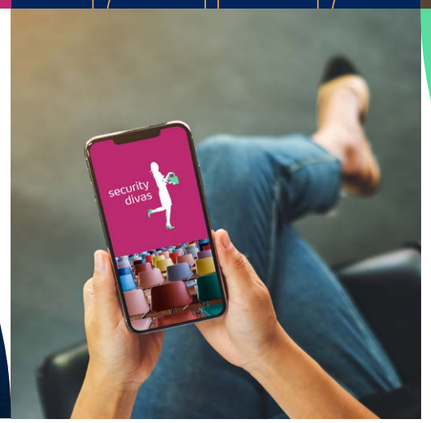


totalt **154** saker

ANTALL SAKER FORDELT PÅ TYPE KRENKELSE I 2021:







«Målet med Security Divas er å skape et fellesskap der kvinner kan utveksle erfaringer, tilegne seg ny fagkunnskap og diskutere bransjerelaterte problemstillinger.»

Karoline Hultman Tømte, leder for partnerskap og myndighetskontakt i NorSIS

Informasjonssikkerhet er fortsatt en manns-dominert bransje i Norge. Det ønsker NorSIS å endre. Security Divas handler om å støtte kvinner i bransjen – fra lesesalen til de går av med pensjon.

SECURITY DIVAS: JOBBER FOR LIKESTILLING INNEN INFORMASJONS-SIKKERHET

Da Security Divas-konferansen gikk av stabelen for første gang i 2010, var det bare ti deltakere. Antallet deltakere har økt år for år, og på konferansen i 2020 deltok så mange som 175 engasjerte kvinner.

I løpet av disse 12 årene har konferansen utviklet seg til å bli et viktig nettverk for alle kvinner som jobber med informasjons-sikkerhet. Fokuset er fag, men nettverks-bygging og erfaringsutveksling er minst like viktig.

– Målet med Security Divas er å skape et fellesskap der kvinner kan utveksle erfaringer, tilegne seg ny fagkunnskap og diskutere bransjerelaterte problem-stillinger, forklarer Karoline Hultman Tømte, leder for partnerskap og myndig-hetskontakt i NorSIS.

Accenture – viktig partner for Security Divas

I 2021 ble det på grunn av pandemien dessverre ikke mulig å gjennomføre Security Divas-konferansen. Det ble derimot gjennomført et frokostseminar med Accenture.

– Accenture er stolt hovedpartner for Security Divas. Security Divas jobber fokusert for å være et viktig nettverk for kvinner som jobber innen fagfeltet, og for å motivere kvinner som studerer, til å velge en retning innen informasjonssikkerhet, sier Torbjørn Eik-Nes, administrerende direktør i Accenture Norge.

Accenture og Security Divas har siden 2016 samarbeidet for å fremme interesse, mangfold og likestilling i informasjons-sikkerhetsbransjen.

– Det målrettede arbeidet Security Divas gjør – ved å både være et samlingspunkt og en arena for faglig diskusjon – baner vei for fremtidens kvinnelige informasjons-sikkerhetskollegaer, legger han til.

Likestilling er fortsatt viktig å kjempe for

Nettverket skaper møteplasser på tvers av sektorer, og viser bredden innen informa-sjonssikkerhet. På Security Divas deltar alt fra toppledere til HR-medarbeidere og utviklere – fra kommersielle bedrifter så vel som fra offentlige og ideelle organisasjoner.

NorSIS' arbeid er knyttet til FNs bære-kraftsmål nummer fem: «Likestilling mellom kjønnene». Derfor er Security Divas et viktig tiltak for å øke mangfoldet i en mannsdominert bransje.

– Hele bransjen har et ansvar for å bidra til likestilling og mangfold. Informasjons-sikkerhet er et viktig samfunnsanliggende, og for å løse fremtidens utfordringer trenger vi kloke hoder som representerer hele befolkningen, forklarer Tømte.

Konferansen evalueres fortløpende opp mot samfunnsoppdraget og behovet for fornyelse, på lik linje med andre prosjekter og aktiviteter i NorSIS.

KOMMUNIKASJON OG KUNNSKAPSFORMIDLING – EN KJERNEOPPGAVE

En av kjerneoppgavene til NorSIS er å sørge for kunnskapsformidling til målgruppene. NorSIS skal informere og dele kunnskap som skaper forståelse for og påvirker adferd som gir en tryggere digital hverdag.

I NorSIS benytter vi oss av ulike kanaler for å nå frem med våre budskap og vårt innhold. I 2021 har NorSIS bygget videre på praksisen med bruk av pressemeldinger, nyhetsartikler på norsis.no, nyhetsbrev, poster på sosiale medier samt råd og veiledninger på nettvett.no. Vi har også deltatt i flere podcaster som omhandler informasjonssikkerhet.

Vi bruker Facebook og LinkedIn aktivt for å være synlige og invitere brukere til dialog. Vi har også gjennomført noen sponsede kampanjer.

Nettsidene våre skal videreutvikles i løpet av 2022, og vi vil i enda større grad være bevisste på innhold og kanalvalg.

Norsis.no
Norsis.no er primært en informasjonskanal for nyhetssaker og annen relevant informasjon om digital sikkerhet. Disse sakene distribueres også gjennom jevnlige nyhetsbrev til våre følgere.

I 2021 hadde nettstedet 83 636 brukere, noe som er en økning på 6 prosent fra 2020. Det har imidlertid vært en nedgang på antall sidehenvisninger fra 183 074 i 2020 til 169 996 i 2021. Dette er en nedgang på litt over 7 prosent.

Det ble publisert i alt 79 nyhetssaker på norsis.no i 2021. Dette er en nedgang på 19 saker fra 2020.

Pressemeldinger
I 2021 sendte NorSIS ut 23 pressemeldinger mot 20 året før. Pressemeldingene ble sendt ut via NTB-nettverket og har hatt ulike budskap knyttet til informasjonssikkerhet, blant annet advarsel om nye svindelmetoder og resultater fra relevante rapporter. I tillegg ble flere enkeltsaker spilt direkte inn til ulike redaksjoner.

Medieomtale
I alt ble NorSIS nevnt i 1220 mediesaker i 2021, en svak økning fra 1187 saker i 2020, ifølge en analyse fra Retriever. Totalt ble NorSIS og merkevarene (Slettmeg.no, nettvett.no, Nasjonal sikkerhetsmåned og Fidusprisen) omtalt i 2161 mediesaker.

Nettvett.no
Nettvett.no er et samarbeid mellom NorSIS, Nasjonal kommunikasjonsmyndighet (Nkom) og Nasjonal sikkerhetsmyndighet (NSM). Samarbeidet skal bidra til en mer koordinert og bedret informasjonsflyt om sikkerhet og sikkerhetskultur knyttet til IKT.

NorSIS har redaktøransvaret for nettvett.no og drifter nettstedet. Her ligger veiledninger og kurs om digital sikkerhet. Disse inneholder informasjon, råd og veiledning om sikrere bruk av internett. Informasjonen er rettet både mot enkeltpersoner fra barn til voksne, forbrukere samt små og mellomstore bedrifter.

En metode nettvett bruker for å nå ut, er å benytte positive ord og vendinger og et språk målgruppen forstår. Nettvett skal gi brukerne selvtillit gjennom gode veiledninger som gir verdi for dem selv, og som de klarer å følge på egenhånd. Vi benytter den faglige kompetansen i de miljøene vi samarbeider med for å kunne gi riktige og troverdige råd. Nye veiledninger blir gjennomgått av et redaksjonsråd med eksperter.

I 2021 ble det opprettet en ny kursportal på nettvett.no i samarbeid med den norske læringsplattformen Motimate. Målet er å tilby både virksomheter og privatpersoner engasjerende og motiverende opplæring i digital sikkerhet.

Resultater

ANTALL BRUKERE AV NETTVETT.NO I 2021:

361 000

jevnt fordelt over hele året

5 veiledninger ble publisert på nettvett.no i løpet av 2021. I alt er det nå 198 veiledninger tilgjengelig på nettvett.no

NETTVETT.NO BLE NEVNT I

120 artikler

i norske medier i løpet av 2021

Kilde: Retriever

Det ble ikke utviklet nye kurs på nettvett i løpet av 2021, men tre kurs ble refreshet og flyttet fra Xtramile til Motimate. Totalt tilbyr vi nå seks gratis nettkurs på nettvett.no

«Nettsidene våre skal videreutvikles i løpet av 2022, og vi vil i enda større grad jobbe bevisst med innhold og kanalvalg.»

Hanne Stine Kind, kommunikasjonsleder i NorSIS

«Norwegian Cyber Range er en arena for testing, trening og øving innen cybersikkerhet der brukere og systemer eksponeres for realistiske hendelser i trygge omgivelser.»

ANDRE AKTIVITETER I 2021

I løpet av 2021 har NorSIS gjennomført en rekke ulike aktiviteter og prosjekter, og samarbeidet bredt med ulike aktører. Det er stor bredde i aktivitetene, og hensikten er å oppnå tverrfaglig kompetanse på sikkerhetsutfordringene for målgruppen.

Safer Internet Day
Hvert år i februar markeres Safer Internet Day over store deler av verden. Hensikten er å øke oppmerksomheten rundt hvordan vi kan bidra til et godt og trygt internett for barn og unge. NorSIS markerte dagen med et digitalt arrangement, med tittelen «Den digitale foreldrefloka – nye problemstillinger eller kjente utfordringer i nye kanaler?».

Arendalsuka 2021
Sammen med SMB Norge inviterte NorSIS til to arrangementer under årets Arendalsuke. Temaet for det første arrangementet var læringspunkter etter cyberangrep, mens det i arrangement nummer to ble diskutert om norske politikere gjør nok for å sørge for god datasikkerhet i Norge. Begge arrangementene ble godt besøkt, i tillegg til at de ble strømmet.

Lanseringsseminar knyttet til rapporten «Trusler og trender2021»
Lanseringen av «Trusler og trender 2021» ble markert med et digitalt seminar sammen med SMB Norge.

NorSIS-konferansen
I november arrangerte NorSIS en todagers konferanse i Oslo, der vi diskuterte temaer som sikkerhetskultur, hets i arbeidslivet og digitale trusler. Konferansen rettet seg mot ledere og ansatte i både offentlig og privat sektor.

Samarbeid med NTNU (CyberRange, NORCICS, CyberSmart, CCIS)
Norwegian Cyber Range: NorSIS deltar i prosjektet som gjennomføres av NTNU. Dette er en arena for testing, trening og øving innen cybersikkerhet der brukere og systemer eksponeres for realistiske hendelser i trygge omgivelser.

NORCICS: SFI NORCICS ved NTNU mottar støtte fra Norges forskningsråd over en periode på åtte år. De skal bidra til at norske selskaper digitaliserer på en sikker og pålitelig måte. NorSIS deltar som prosjektpartner og bidrar med prosjektressurser knyttet til formidling, kunnskapsoverføring og kommunikasjon

CyberSmart: Dette er et prosjekt som skal utdanne lærere og elever i IKT-sikkerhet. NorSIS er representert i styringsgruppen/rådet i det løpende prosjektet, og samarbeider her med NTNU, NSM, RENATEsenteret, UiO, Cyberingeniørhøgskolen og NVE.

Samarbeid med Skatteetaten om ID og ID-tyveri
Konferansen IDentitet, som NorSIS og Skatteetaten i en årrekke har arrangert, måtte dessverre avlyses i år på grunn av koronapandemien. Vi fikk imidlertid gjennomført den årlige Identitetsundersøkelsen som omhandler ID-tyveri og sikker identitet.

Samarbeid med UiO om SODI-prosjektet
I prosjektet Samfunnssikkerhet og digitale identiteter, SODI, undersøkes det hvordan juss og teknologi kan virke sammen for å avdekke og redusere sårbarheter ved bruk og misbruk av eID-systemer.

Sønstebyprisen 2020 ble utdelt i januar 2021
NorSIS var en av elleve cyberforsvarere som fikk Sønstebyprisen 2021. Hovedformålet med prisen er å hedre «den person eller organisasjon som i handling har fremstått som en modig forsvarer av de grunnleggende verdier i vårt demokrati, herunder holdt forsvarsviljen levende og bidratt til at vårt forsvar trygger landets frihet og uavhengighet».

ÅRSREGNSKAP 2021

RESULTATREGNSKAP FOR 2021

DRIFTSINNTEKTER OG KOSTNADER	NOTE	2021	2020
Salgsinntekt	3	15 291 156	16 501 691
Annen driftsinntekt		4 500	10 875
Sum driftsinntekter		**15 295 656**	**16 512 566**
Varekostnad		403 504	905 983
Lønnskostnad	2	9 702 086	9 579 081
Avskrivning varige driftsmidler	4	117 403	13 144
Annen driftskostnad	2	6 312 011	6 042 549
Sum driftskostnader		**16 535 004**	**16 540 756**
DRIFTSRESULTAT		**-1 239 348**	**-28 190**
Finansinntekt og finanskostnad			
Annen renteinntekt		24 413	35 231
Annen finansinntekt		5 964	9 652
Annen rentekostnad		-7 399	-1 349
Annen finanskostnad		0	-1 241
Resultat av finansposter		**22 979**	**42 293**
ÅRSRESULTAT		**-1 216 370**	**14 104**
OVERFØRINGER			
Avsatt til annen egenkapital	6	0	14 104
Overført fra annen egenkapital		-1 216 370	0
SUM OVERFØRINGER		**-1 216 370**	**14 104**

BALANSE
PR. 31. DESEMBER 2021

	NOTE	2021	2020
EIENDELER			
Varige driftsmidler			
Inventar og utstyr	4	750 806	36 146
Sum varige driftsmidler		**750 806**	**36 146**
SUM ANLEGGSMIDLER		**750 806**	**36 146**
OMLØPSMIDLER			
Fordringer			
Kundefordringer		2 000 761	1 190 309
Andre fordringer		287 981	139 924
Sum fordringer		**2 288 741**	**1 330 233**
Betalingsmidler			
Bankinnskudd og kontanter	5	5 191 363	8 833 758
Sum betalingsmidler		**5 191 363**	**8 833 758**
SUM OMLØPSMIDLER		**7 480 105**	**10 163 991**
SUM EIENDELER		**8 230 911**	**10 200 137**

FORTS. BALANSE
PR. 31. DESEMBER 2021

	NOTE	2021	2020
EGENKAPITAL OG GJELD			
EGENKAPITAL			
Opptjent egenkapital			
Annen egenkapital	6	5 248 056	6 464 426
Sum opptjent egenkapital		**5 248 056**	**6 464 426**
SUM EGENKAPITAL		**5 248 056**	**6 464 426**
GJELD			
Kortsiktig gjeld			
Leverandørgjeld		742 892	174 509
Skyldige offentlige avgifter		1 003 268	756 884
Annen kortsiktig gjeld		1 236 695	2 804 318
Sum kortsiktig gjeld		**2 982 855**	**3 735 711**
SUM GJELD		**2 982 855**	**3 735 711**
SUM EGENKAPITAL OG GJELD		**8 230 911**	**10 200 137**

Gjøvik, 02.03.2022

Bjørn Erik Thon
styremedlem

Kristine Beitland
styremedlem

Nils Kalstad
styremedlem

Hans-Henrik Merckoll
styreleder

Lars Rognås
styremedlem

Karoline Hultman Tømte
styremedlem

Lars-Henrik Bakke Gundersen
daglig leder

Lill Sissel Sverresdatter Larsen
styremedlem

NOTER TIL ÅRSREGNSKAPET

NOTE 1 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. Nedskrivingen reverseres når grunnlaget for nedskrivingen 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

Lønnskosstnader	2021	2020
Lønninger	7 468 984	7 558 338
Arbeidsgiveravgift	1 229 888	1 102 243
Pensjonskostnader	468 052	421 065
Andre ytelser	535 161	497 435
Sum	**9 702 086**	**9 579 081**

Selskapet har i 2021 sysselsatt 8,5 årsverk.

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

NOTE 3 OFFENTLIG TILSKUDD

Selskapet har mottatt kr 9 975 000 i grunnfinansiering. For øvrig er det mottatt prosjektstøtte på kr 1 364 249.

NOTE 4 ANLEGGSMIDLER

	DRIFTSLØSØRE, INVENTAR O.L.	SUM
Anskaffelseskost pr. 01.01.21	284 974	284 974
+ Tilgang kjøpte driftsmidler	832 063	832 063
= Anskaffelseskost 31.12.21	**1 117 038**	**1 117 038**
Akkumulerte avskrivninger 31.12.21	366 232	366 232
= Bokført verdi 31.12.21	**750 806**	**750 806**
Årets ordinære avskrivninger	117 403	117 403
Økonomisk levetid	3-5 år	

Selskapet leier kontorlokaler. Årets kostnad inkl felleskostnader utgjør kr 849 292.

NOTE 5 BANKINNSKUDD

Innestående midler på skattetrekkskonto (bundne midler) er på kr. 370 144.

NOTE 6 EGENKAPITAL

	ANNEN EGENKAPITAL	SUM EGENKAPITAL
Pr. 31.12.2020	6 464 426	6 464 426
Endringer ført mot EK	0	0
Pr 01.01.2021	**6 464 426**	**6 464 426**
Årets resultat	-1 216 370	-1 216 370
Pr 31.12.2021	**5 248 056**	**5 248 056**

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."

Hans-Henrik Merckoll
Styrets leder
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5998-4-1736132
IP: 194.182.xxx.xxx
2022-03-04 09:48:29 UTC
bankID

Bjørn Erik Thon
Styremedlem
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5999-4-1061865
IP: 217.144.xxx.xxx
2022-03-04 14:44:23 UTC
bankID

Kristine Beitland
Styremedlem
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5999-4-1795242
IP: 84.212.xxx.xxx
2022-03-05 10:42:23 UTC
bankID

Karoline Hultman Tømte
Styremedlem
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5995-4-87354
IP: 84.209.xxx.xxx
2022-03-06 15:14:50 UTC
bankID

Nils Kalstad
Styremedlem
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5993-4-2125356
IP: 80.212.xxx.xxx
2022-03-06 19:36:12 UTC
bankID

Lars-Henrik B Gundersen
Adm. direktør
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5995-4-960101
IP: 85.166.xxx.xxx
2022-03-09 16:37:52 UTC
bankID

Lars Rognås
Styremedlem
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5995-4-87782
IP: 77.106.xxx.xxx
2022-03-15 08:57:17 UTC
bankID

Lill Sissel Sverresdatter Larsen
Styremedlem
På vegne av: Norsk Senter For Informasjonssikring
Serienummer: 9578-5997-4-420722
IP: 193.23.xxx.xxx
2022-03-15 09:50:01 UTC
bankID

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 orginalen?
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**

Deloitte.

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

Konklusjon
Vi har revidert Norsk Senter for Informasjonssikrings årsregnskap som består av balanse per 31. desember 2021, resultatregnskap for regnskapsåret avsluttet per denne datoen og noter til årsregnskapet, herunder et sammendrag av viktige regnskapsprinsipper.

Etter vår mening

- oppfyller årsregnskapet gjeldende lovkrav, og
- gir årsregnskapet et rettvisende bilde av organisasjonens finansielle stilling per 31. desember 2021, og av dens resultater for regnskapsåret avsluttet per denne datoen i samsvar med regnskapslovens regler og god regnskapsskikk i Norge.

Grunnlag for konklusjonen
Vi har gjennomført revisjonen i samsvar med de internasjonale revisjonsstandardene International Standards on Auditing (ISA-ene). Våre oppgaver og plikter i henhold til disse standardene er beskrevet nedenfor under *Revisors oppgaver og plikter ved revisjonen av årsregnskapet*. Vi er uavhengige av organisasjonen slik det kreves i lov, forskrift og International Code of Ethics for Professional Accountants (inkludert internasjonale uavhengighetsstandarder) utstedt av the International Ethics Standards Board for Accountants (IESBA-reglene), og vi har overholdt våre øvrige etiske forpliktelser i samsvar med disse kravene. Innhentet revisjonsbevis er etter vår vurdering tilstrekkelig og hensiktsmessig som grunnlag for vår konklusjon.

Øvrig informasjon
Styret og daglig leder (ledelsen) er ansvarlige for øvrig informasjon som er publisert sammen med årsregnskapet. Øvrig informasjon omfatter informasjon i årsrapporten bortsett fra årsregnskapet og den tilhørende revisjonsberetningen. Vår konklusjon om årsregnskapet ovenfor dekker ikke øvrig informasjon.

I forbindelse med revisjonen av årsregnskapet er det vår oppgave å lese øvrig informasjon. Formålet er å vurdere hvorvidt det foreligger vesentlig inkonsistens mellom den øvrige informasjonen og årsregnskapet og den kunnskap vi har opparbeidet oss under revisjonen av årsregnskapet, eller hvorvidt øvrig informasjon ellers fremstår som vesentlig feil. Vi har plikt til å rapportere dersom øvrig informasjon fremstår som vesentlig feil. Vi har ingenting å rapportere i så henseende.

Ledelsens ansvar for årsregnskapet
Ledelsen er ansvarlig for å utarbeide årsregnskapet og for at det gir et rettvisende 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.

Deloitte.

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 avviklet.

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 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 ISA-ene, utøver vi profesjonelt skjønn og utviser profesjonell skepsis gjennom hele revisjonen. I tillegg:

- identifiserer og vurderer 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 regnskapsestimatene 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. 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 rettvisende bilde.

Vi kommuniserer med styret 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.

Gjøvik, 2. mars 2022
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
2022-03-15 13:21:39 UTC
bankID

Penneo Dokumentnøkkel: 66KEZ-PX0WL-LN5YT-HXZKD-IFZYI-BW3CU

NorSIS

Design: Nucleus AS
Foto: iStock og Nucleus AS

NORSK SENTER FOR INFORMASJONSSIKRING
Studievegen 2
2815 Gjøvik
Tlf. 40 00 58 99
post@norsis.no
www.norsis.no