DSA
Direktoratet for strålevern og atomsikkerhet
Norwegian Radiation and Nuclear Safety Authority

Direktoratet for e-helse
Postboks 221 Skøyen
0213 OSLO
Land

Kontaktperson

Unntatt offentlighet

Ref.:
22/01599-1 /

Dato:
09.09.2022

Saksbehandler:
Eva Kvammen

Innspill til kommende stortingsmelding om helseberedskap – tema: Digital sikkerhet, saksnummer 22/448

Innledning/bakgrunn
Nasjonal strategi for digital sikkerhet (2019) definerer digital sikkerhet som beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte er avhengig av informasjons- og kommunikasjonsteknologi (IKT). De senere år har vist at trusselaktører i stadig større grad utnytter muligheter som måtte oppstå i det digitale rom og fremmedstatlig etterretningsaktivitet mot både offentlige og private virksomheter øker.
Det er videre et styrende prinsipp i den nasjonale strategien at myndigheter og næringsliv skal samarbeide for å identifisere, utveksle erfaringer om og drøfte digitale sikkerhetsutfordringer. Det er et delmål innen forebyggende sikkerhet at myndigheter og virksomheter deler informasjon om trusler, sårbarheter, hendelser og effektive tiltak med relevante aktører for å øke samfunnets robusthet mot uønskede digitale hendelser.
DSA er fag- og forvaltningsmyndighet på strålevern, atomsikkerhet, radioaktiv forurensning og radioaktivt avfall. Vi har et bredt spekter av samarbeidspartnere hvorav flere er sivile næringslivsaktører. Sikring av de nukleære anleggene og nukleært materiale er en av våre mange oppgaver. Ivaretagelse av godt strålevern, atomsikkerhet, atomberedskap og ikke-spredning av atomvåpen er vesentlig i vårt samfunnsoppdrag og en god oppdragsløsning er avhengig av at vi til enhver tid sikrer god og felles situasjonsforståelse hos våre samarbeidspartnere.

Hoveddel
Noen av våre samarbeidspartnere er *underlagt* sikkerhetsloven gjennom enkeltvedtak (IFE), mens andre er *omfattet* av sikkerhetsloven. Det å være underlagt sikkerhetsloven innebærer at «virksomhetene kan settes i stand til å få tilgang til sikkerhetsgradert informasjon – som for eksempel trusselvurderinger og andre opplysninger som er av betydning for sikkerhetsarbeidet». Det er ikke etablert faste styringssystemer som sikrer informasjonsspredning på en tilfredsstillende måte i dag.
DSA opplever at det er en gjentagende problemstilling at virksomheter og næringsliv som leverer kritiske samfunnstjenester ikke har tilgang til sikkerhetsgradert informasjon. Vi oppfatter at det ikke er etablert gode rutiner med avklart og erkjent ansvarsforhold for deling av informasjon. Dette kan omfatte både generelle trusselvurderinger, men også spesifikk informasjon som ønskes delt. Dette vanskeliggjør informasjonsflyt og spesielt gjelder dette i de tilfeller der informasjonen er gradert, men er også utfordrende i forbindelse med søknadsbehandling og tilsyn. Sistnevnte innebærer gjerne et ønske fra tilsynsmyndigheten om å få oversendt omfattende materiale fra virksomheten det skal føres tilsyn med. Dette kan omfatte alt fra kilderegister til risikovurderinger. Det er en gjensidig forventning at sensitiv informasjon kan formidles ved hjelp av noe annet enn vanlig epost.
DSA ivaretar oppfølging av våre atomanlegg i Halden og Kjeller, samt i Himdalen, i tillegg til reaktordrevne fartøyer i norsk havn og farvann, foruten strålekilder i en rekke norske

Postadresse *Postal address:*
Postboks 329 Skøyen NO-0213
Oslo, Norway
T +47 67 16 25 00
F +47 67 14 74 07

Besøksadresse *Office:*
Grini næringspark 13, 1361
Østerås, Norway
dsa.no
dsa@dsa.no

Swift address: UNBANOKK
Bankkonto *Bank account:*
8276 01 00494
IBAN: NO76 8276 01 00494
Org.nr.: 867 668 292

virksomheter. Vi har både en generell veiledningsplikt og tilsynsansvar. God digital sikkerhet i vår sektor krever at vi legger til rette for gode partnerskap med relevante aktører ved informasjonsdeling og et vedvarende fokus på bygging av felles situasjonsforståelse. Effektiv digital sikkerhet forutsetter medvirkning fra næringslivet. DSA opplever at det er en utfordring at vi identifiserer kritisk infrastruktur eller grunnleggende nasjonale funksjoner (GNF) uten at det etableres gode systemer og rutiner for informasjonsdeling. Relevant informasjonsdeling i en tilrettelagt struktur vil sikre at objekteiere sitter på et oppdatert trusselbilde, noe som i sin tur bidrar til felles situasjonsforståelse. I siste instans vil dette kunne bidra til å identifisere svakheter innen digital sikkerhet og utbedre disse med adekvate tiltak.

Konklusjon
DSA registrerer at problemstillingen om samvirke med aktører som ikke har tilgang til alle informasjonsplattformer, og da særlig i forbindelse med utveksling av sensitiv eller gradert informasjon, ikke er nevnt i høringsutkastet. Vi opplever at dette er en identifisert svakhet i bygging av tilfredsstillende digital sikkerhet og anbefaler at stortingsmeldingen gir tydeligere signaler og retning innen dette domenet. Behovet for etablering av gode styringssystemer og/eller rutiner for deling av sensitiv og gradert informasjon mellom offentlige myndigheter og næringsliv bør etter vår vurdering fremkomme av stortingsmeldingen.

Vennlig hilsen

Per Strand
Direktør

Eva Kvammen
seniorrådgiver

Dokumentet er elektronisk godkjent.

Vedlegg:

Liste over kopimottakere: