Næringslivets sikkerhets-råd

Kommunal- og distriktsdepartementet
Postboks 8112 dep.
003 Oslo

Åpenhet uten omtanke?
Innspill til ny nasjonal digitaliseringsstrategi

Næringslivets Sikkerhetsråd viser til Kommunal- og distriktsdepartementets invitasjon om å komme med innspill til ny nasjonal digitaliseringsstrategi, og samtale med fagdirektør Timothy Szlachetko tirsdag 12. desember 2023 om utsatt innmeldingsfrist. På vegne av sikkerhets- og beredskapsmiljøet i næringslivet ønsker vi å sette fokus på de sikkerhetsmessige utfordringene knyttet til digitalisering.

Digitalisering gir store gevinster og muligheter, og vi stiller oss i stor grad bak NHOs innspill. Samtidig kan digitalisering skape sårbarheter med store konsekvenser for privatpersoner og bedrifter – og i verste fall for samfunns- og statssikkerheten. NSR forventer derfor at den nye nasjonale digitaliseringsstrategien også tar høyde for sikkerhetsmessige aspekter ved digitalisering. Vi bidrar gjerne med våre erfaringer og synspunkter i dette arbeidet, og vil benytte anledningen til å trekke frem et par konkrete eksempler fra skjæringspunktet mellom digitalisering, offentlighet og sikkerhet.

Tidsriktig og automatisert svindel basert på offentlige kilder

De siste årene har det vært en voldsom økning i bedragerier mot norske privatpersoner og bedrifter. Ifølge Finanstilsynet hadde norske banker 614 millioner kroner i tap i 2022, som følge av svindel og bedrageri. Tall fra DNBs sikkerhetsavdeling viser at digitale bedragerier har økt med 832 prosent fra 2018 til 2022, og fortsatt er i sterk økning. Bedrageriene er så omfattende og sofistikerte, at Økokrim kaller det et samfunnsproblem og en trussel mot hele det tillitsbaserte samfunnet.

NSR deltar i et samarbeid med finansnæringen, teleoperatørene, politiet, Nasjonal kommunikasjonsmyndighet, og andre interesseorganisasjoner om å forebygge disse bedragerie ne. Akkurat nå pågår det for eksempel et prosjekt for å gjøre tekniske tiltak i telenettet, slik at svindelmeldinger ikke skal komme gjennom på telefon og SMS. Vi ser at slike tverrfaglige samarbeid mellom private og offentlige aktører er svært viktig for å kunne håndtere sårbarheter som oppstår i kjølvannet av en stadig mer digital hverdag.

a) **Forslag til tiltak:** Den nasjonale digitaliseringsstrategien bør fremheve viktigheten av tverrfaglige samarbeid mellom offentlige og private aktører, for å kunne håndtere sikkerhetsutfordringene som følger med økt digitalisering.

Gjennom arbeidet med å forebygge bedrageri og svindel ser vi også hvordan trusselaktørenes metoder stadig utvikler seg for å omgå sikkerhetstiltakene. En generell trend er at svindelforsøkene

har gått fra å være masseutsendte og lite treffsikre, til å bli individualisert. Trusselaktørens mål er ofte å gjennomføre såkalt sosial manipulering, der offeret ved hjelp av skreddersydde meldinger narres til å utføre en handling. Det kan for eksempel være å logge inn på en nettside med bankID, overføre penger, eller kjøre et vedlegg med skadevare. Kjernen i slike skreddersydde og troverdige meldinger er et sett med realistiske/reelle data om offeret. NSR er bekymret for at data fra offentlige registre allerede brukes som grunnlag i slike svindelforsøk, og at problemet trolig vil vokse dramatisk fremover.

En relativt ny svindelmetode vi vil gjøre departementet oppmerksom på, er hvordan data fra offentlige databaser benyttes som kilde i tidsriktige svindelforsøk. Vårt inntrykk er at enkelte trusselaktører overvåker offentlige registre for endringer i sann tid, for deretter å bruke disse sanntidsdataene i skreddersydde, målrettede og tidsriktige svindelforsøk. Personer som har sendt inn digital salgsmelding for kjøretøy til Statens Vegvesens har eksempelvis fått en svindelmeldinger med krav om å betale omregistreringsavgift kort tid etter innsending. SMS-ene har hatt «VEGVESEN» som avsender, og bestått av individualisert og tidsriktig informasjon fra innsendingen som akkurat ble gjennomført. Slike svindelforsøk er svært vanskelige å oppdage, siden de fleste ikke har kunnskap om at dataene de melder inn raskt blir offentlige – og dermed kan utnyttes av kriminelle.

På samme måte har bedrifter fått falske SMS-er med avsender «ALTINN», like etter at de har endret bedriftens data i Enhetsregisteret/Altinn. I SMS-en vises de endrede dataene, og en lenke for å «bekrefte» endringene. Også denne SMS-en er falsk. Bekreftelseslenken går til pålogging i nettbank, der trusselaktøren gjør forsøk på å overføre offerets penger til sin egen konto.

b) Forslag til tiltak: Det bør utarbeides tiltak, for eksempel forsinkelsesregler for publisering av sanntidsdata, for å unngå denne type utnyttelse av data fra offentlige databaser.

c) Forslag til tiltak: Flere databaser bør underlegges et autentiseringsregime, der man for eksempel må logge på via ID-porten for å få tilgang til data. Dette vil hindre at utenlandske trusselaktører misbruker norske offentlige databaser for å svindle norske borgere. Dersom norske borgere misbruker dataene vil en innloggingsløsning bidra til at politiet har digitale spor som kan etterforskes ved behov. En slik påloggingsmekanisme er allerede i drift for skattelistene, men bør utvides til flere offentlige databaser.

NSR er også bekymret for at den nevnte svindelmetoden vil kunne automatiseres og effektiviseres, for eksempel ved hjelp av generativ kunstig intelligens (GKI). Det er derfor behov for en prinsipiell åpenhetsdebatt i en ny digital tid – åpenhet for maskiner og mennesker, eller bare åpenhet for mennesker?

d) Forslag til tiltak: Norske offentlige databaser bør prinsipielt være åpne for mennesker, ikke maskiner. Det bør utvikles vilkår for unntak, der legalt bruk for eksempel underlegges et søknadsregime med krav om sikkerhet.

Behov for legitimeringsplikt i innsynssaker

Offentleglova er viktig for det norske demokratiet, og et utgangspunkt for arbeidet med digitalisering i offentlig sektor. I dag kan hvem som helst søke om innsyn i hva som helst i offentlig forvaltning, uten å oppgi navn, og uten å oppgi formål. Næringslivets Sikkerhetsråd er bekymret for at innsynsregimet misbrukes av trusselaktører for å hente ut informasjon fra myndighetene som hver for seg er ugradert og offentlig, men som i sum er av en slik art at det utgjør en sikkerhetsrisiko.

De siste årene har vi for eksempel sett at en rekke helseforetak har utlevert sammenstilte lister med data om sine ansatte, til anonyme tredjeparter. Slike sammenstilte databaser vil vesentlig kunne lette gjennomføring av flere typer straffbare handlinger, og er etter vår vurdering derfor

unntaksberettiget etter offentleglova § 24. Denne type sammenstillinger vil særlig kunne lette gjennomføring av tre typer straffbare handlinger:

- **Digital kriminalitet og bedrageri:**
  Opplysningene vil gi trusselaktører mulighet til å lage svært målrettede og troverdige phishing/spear phishing-kampanjer i et digitalt angrep. Informasjonen kan også misbrukes til sosial manipulering, der offeret lures til å begå digitale, sikkerhetstruende hendelser. Dette kan ramme både virksomheten, og den enkelte ansatte. Den digitale kriminaliteten mot norske virksomheter øker, og konsekvensen av digitale angrep er svært alvorlig: Sensitiv informasjon kommer på avveie, og data blir kryptert/ødelagt.

- **Utenlandsk etterretningsaktivitet og hybrid krigføring:**
  Ifølge Politiets sikkerhetstjeneste er den utenlandske etterretningsaktiviteten i Norge høy. Norske offentlige virksomheter, som omfattes av offentleglova, er svært mulige mål for denne aktiviteten. Databaser med informasjon om ansatte vil vesentlig lette de utenlandske etterretningsoperatørenes jobb. For det første vil selve databasen i seg selv ha høy etterretningsverdi. For det andre vil databasen gi verdifull informasjon om potensielle mål. For det tredje kan informasjonen i databasen benyttes i manipulasjonsforsøk, påvirkningsoperasjoner og målrettede etterretningsoperasjoner. Denne utfordringen har blitt mer åpenbar etter den russiske invasjonen av Ukraina, og norske virksomheter må i større grad enn tidligere regne med at utenlandske etterretningsoperasjoner vil ta i bruk hybride virkemidler – også mot norske virksomheter.

- **Fysiske trusler:**
  Mange ansatte i offentlig sektor kan ha et skjermingsbehov som følge av sin jobb. Det kan være risiko for fysiske trusler fra kilder, klienter, pasienter, eller andre personer man håndterer som en del av jobben. En annen, og viktigere utfordring, er imidlertid å ta hensyn til ansatte som har mer overhengende fysiske trusler mot seg, og som har fortrolig eller strengt fortrolig (hemmelig) adresse. Et overslag viser at rundt 250 personer med hemmelig adresse arbeider i offentlig sektor. Disse personene har et åpenbart behov for å holde både sitt arbeidssted og bopel skjult. Ved utlevering av store datasett med informasjon om ansatte, vil man ikke kunne skjerme disse personene – og en trusselaktør vil kunne oppsøke dem på arbeidsstedet med onde hensikter.

Selv om mye av informasjonen er offentlig, for eksempel i sosiale medier, på virksomhetenes nettsider, og i telefonkatalogen, er det sammenstillingen av informasjonen som utgjør den største trusselen. Det er sammenstillingen som vesentlig bidrar til å kunne lette gjennomføring av straffbare handlinger.

I disse konkrete sakene har innsynsbegjæringene blitt sendt fra anonyme e-postadresser fra uidentifiserbare personer. Helseforetakene avslo først innsynsbegjæringene etter offentleglova § 24, men ble overprøvd av klageinstans. I dag er derfor dataene utlevert. Helseforetakene har etter personvernforordningen kapittel 15 plikt til å opplyse de ansatte *til hvem* deres personopplysninger er utlevert til. Dette er ikke mulig, når innsynsbegjæringen er sendt av en anonym aktør som ifølge offentleglova har krav på anonymitet. NSRs dialog med blant annet Datatilsynet og Justis- og beredskapsdepartementet har vist at forholdet mellom disse to lovene ikke er avklart.

Siden mye av digitaliseringsarbeidet skjer i relasjon til offentlighetsprinsippet, tror NSR det er viktig at den nye strategien går inn i noen av de sikkerhetsmessige utfordringene knyttet til utvidet digitalisering og tilgang til offentlige dokumenter og databaser. Det bør vurderes en legitimasjonsplikt ved innsyn, som sikrer at norske borgere sikres innsyn og tilgang til digitale løsninger, samtidig som trusselaktører holdes ute. En løsning kan være å kreve pålogging gjennom

ID-porten til eInnsyn. En mulig løsning kan være en datasegregering som gjør at søkerens anonymitet ivaretas overfor forvaltningsorganene, men likevel registreres hos eInnsyn.

e) **Forslag til tiltak:** Det bør innføres en legitimeringsplikt for innsynsbegjæringer, som hindrer at (utenlandske) trusselaktører fritt kan hente offentlige data ved bruk av offentleglova.

Behov for et cybersikkerhetssenter for næringslivet

Det er behov for et miljø dom kan ivareta digital sikkerhet for de deler av næringslivet som i dag ikke er underlagt et sektorvis responsmiljø for digital sikkerhet (SRM). NSR konstaterer at kun en liten andel av det norske næringslivet er knyttet til et slikt miljø i dag, og følgelig at de fleste bedrifter *ikke* er i et system for varsling og informasjonsdeling om digital sikkerhet.

NSR har igjennom sitt arbeid generelt og med Mørketallsundersøkelsen spesielt, etablert et godt bilde av bilde av den digitale sikkerheten i næringslivet. NSR er særlig bekymret for de små og mellomstore bedriftene. Dette er viktige aktører i større verdikjeder, og vi har sett eksempler på at sårbarheter hos en liten bedrift kan gi adkomst til langt større, og ofte mer samfunnskritiske, virksomheter. Vi vet også at det er i denne kategorien vi finner flest virksomheter som ikke har et rammeverk og/eller styringssystem for informasjonssikkerhet, noe som ytterligere øker virksomhetens sårbarhet overfor cyberhendelser. I dette bildet er det spesielt viktig med et sikkerhetssenter som kan motta og videresende varsler og råd knyttet til digital sikkerhet på en forutsigbar, kontrollert og sikker måte. Videre er det behov for et SRM som kan motta rapporter fra næringslivet, vurdere og videreformidle et aggregert situasjonsbilde til myndighetene.

Mange bransjer har oppdaget denne sårbarheten, og ønsker å opprette egne sektorvise responsmiljø. NSR har eksempelvis arbeidet med matbransjen det siste året, som ønsker å bli en del av et slikt sikkerhetssamarbeid. NSR kjenner også til at flere andre bransjer ønsker å få egne sektorvise responsmiljøer. Dette er etter vårt syn en uheldig utvikling. Ved å etablere et stort antall små, bransjeorienterte sentre for digital sikkerhet vil man trolig ikke oppnå tilstrekkelig kvalitet og dybde i hvert enkelt senter. Samtidig vil kampen om kvalifisert arbeidskraft bli stor. En ukontrollert utvikling av stadig nye SRM-er er derfor ikke ønskelig i et overordnet sikkerhetsperspektiv. NSR anbefaler at man i stedet konsoliderer ressursene innen digital sikkerhet, og oppretter ett sektorvis responsmiljø for hele næringslivet.

f) **Forslag til tiltak:** Den nasjonale digitaliseringsstrategien bør understreke viktigheten av god digital sikkerhet, og utrede tiltak for å styrke arbeidet med digital sikkerhet – for eksempel gjennom et cybersikkerhetssenter for næringslivet.

Uavklarte tilsynsroller som følge av EU-direktiv

EU har, eller er i ferd med, å innføre ulike direktiver om digitalisering og digital sikkerhet. Eksempler på dette er AI Act, NIS1/NIS2 og Dora. Etter det NSR forstår vil disse direktivene innføres i Norge som forordninger eller gjennom nasjonal lovgivning. Det er foreløpig uklart hvordan disse direktivene skal operasjonaliseres i Norge. For eksempel beskriver flere direktiver en tilsynsfunksjon, blant annet et algoritmetilsyn i AI Act, og et tilsyn om digital sikkerhet i NIS2. Innad i EU løser ulike land tilsynsmyndigheten på svært ulike måter. NSR mener at disse kommende tilsynsmyndighetene må sees i en sammenheng. Av hensyn til kostnader, rekruttering, likebehandling og kvalitet tror NSR på fellesløsninger (få tilsynsmyndigheter) fremfor desentraliserte/sektorvise løsninger (mange tilsynsmyndigheter).

g) **Forslag til tiltak:** Det må gjøres en overordnet utredning om hvordan norske myndigheter skal løse tilsynsrollene som følger av flere varslede EU-direktiv.

Stort kompetansebehov innenfor digital sikkerhet

Økt digitalisering fører til at internasjonale trusselaktører får en større angrepsflate mot norske interesser. Fysiske avstander og landegrenser er ikke lenger en beskyttelse i seg selv, digitale sårbarheter kan angripes uavhengig av hvor de er, fra trusselaktører lokalisert over hele verden. Dette innebærer i praksis en enorm volumøkning i antall trusselaktører som har kapasitet og intensjon om å angripe norske interesser. Konsekvensen er at norske virksomheter må ha større fokus på sikkerhet, enn tidligere. Fremover vil derfor kompetanse innen digital sikkerhet bli en kritisk og knapp ressurs. I en rapport fra 2022 anslår PWC at man innen 2030 vil mangle 4000 personer med denne kompetansen, bare i Norge. Den nye nasjonale digitaliseringsstrategien bør derfor utrede hvordan den digitale sikkerhetskompetansen kan styrkes fremover. Styrkingen bør omfatte både grunnleggende- og spisskompetanse, og bør gjennomføres i samarbeid mellom myndigheter, utdanningsinstitusjoner og næringslivet.

Oslo, 14. desember 2023

Odin Johannessen
Direktør, NSR