Næringslivets sikkerhets-råd

Næringslivets Sikkerhetsråds høringsinnspill til NOU 2024: 14 «Med lov skal data deles»

Vi viser til Digitaliserings- og forvaltningsdepartementets invitasjon til å inngi høringsinnspill til NOU 2024: 14 «Med lov skal data deles».

Næringslivets Sikkerhetsråd (NSR) er en stiftelse eid av NHO, Virke, Spekter, Rederiforbundet og Finans Norge, og har rundt 300 større bedrifter i Norge som medlemmer. Stiftelsens formål er å ivareta næringslivets fellesinteresser innen sikkerhet og beredskap, særlig knyttet til tilsiktede trusler. På vegne av sikkerhets- og beredskapsmiljøet i næringslivet ønsker vi å kommentere Viderebruksutvalgets vurderinger om sikkerhet, slik de fremgår i kapittel 10.

NSR mener vurderingene om sikkerhet i for stor grad er knyttet til statssikkerhetsdimensjonen, altså hvilken trussel deling av data kan ha for rikets sikkerhet. Dette er etter vårt syn bare en liten del av sikkerhetsutfordringene med deling av data. Næringslivet opplever allerede i dag at data fra offentlige kilder misbrukes av kriminelle og antatt statlige trusselaktører, og at det er behov for tiltak for å begrense misbruk av offentlige data.

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 607 millioner i tap første halvår av 2024, kun som følge av svindel og bedrageri. Bedrageriene er så omfattende og sofistikerte, at Økokrim kaller det et samfunnsproblem og en trussel mot hele det tillitsbaserte samfunnet.

Gjennom arbeidet med å forebygge bedrageri og svindel ser vi 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 vet at data fra offentlige registre allerede brukes som grunnlag i slike svindelforsøk, og er bekymret for at problemet 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.

a) **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.

b) **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?

c) **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.

NSR mener det må 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.

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

Risiko for mange tilsynsfunksjoner

EU har, eller er i ferd med, å innføre ulike direktiver om digitalisering og digital sikkerhet, som vil kreve nye tilsynsfunksjoner i Norge. I NSRs høringsinnspill til Justis- og beredskapsdepartementet om digitalsikkerhetsforskriften, er vi bekymret for at norske virksomheter i fremtiden vil få for mange kontaktpunkter for varsling, rapportering og tilsyn innen digitalisering, teknologi og digital sikkerhet.

Næringslivets Sikkerhetsråd vil derfor oppfordre Regjeringen til å gjøre en overordnet vurdering av tilsynsstrukturen for personvern, teknologi, datadeling og digital sikkerhet, og se dette i sammenheng med andre EU-krav som er under innføring i norsk rett. Vi tror det kan være fornuftig å vurdere et felles tilsyn for personopplysninger, kunstig intelligens, og digital sikkerhet, i stedet for at Datatilsynet, Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, og en rekke sektortilsyn skal løse disse oppgavene hver for seg.

Oslo, 16. desember 2024

Odin Johannessen
Direktør, NSR