UTFORDRINGENE I 2021 – HVA VAR DE STØRSTE UTFORDRINGENE INNEN SIKKERHET OG BEREDSKAP OG HVORDAN HAR NORSKE VIRKSOMHETER LØST DISSE?

Standard Morgen - Samfunnssikkerhet – hvordan styrke sikkerheten og beredskapen i samfunnet – før og etter korona

CARSTEN RAPP
24.11.2021

BDO
tett på

Kilder

- Koronakommisjonen – NOU 2021: 6 Myndighetenes håndtering av koronapandemien
- JD – Samfunnssikkerhetsmeldingen (Meld.St.5(2020-2021)
- NSM – Nasjonalt digitalt risikobilde 2021 & Risiko 2021
- DSB – Årsrapport 2020 (Kap. 5 Vurdering av fremtidsutsikter)
- PST – Nasjonal trusselvurdering 2021
- Politiet – Trusselvurdering 2021
- NorSIS – Trusler og trender 2021
- NSR – KRISINO 2021 (Kriminalitets- og sikkerhetsundersøkelsen) & Beredskapsundersøkelsen 2021
- BDO – Våre egne erfaringer fra oppdrag for offentlige og private virksomheter

TRUSSELBILDET MOT NORSKE VIRKSOMHETER

Statlig etterretningsvirksomhet

- Flere lands etterretningstjenester bruker store ressurser på etterretningsaktivitet i Norge. Russiske og kinesiske tjenester utgjør den største trusselen.
  - Formålet er å innhente informasjon, bl.a. kartlegge norsk infrastruktur og utnytte akademia til ulovlig kunnskapsoverføring, samt påvirke beslutninger.
- Nettverksoperasjoner vil utgjøre den største delen av russisk og kinesisk etterretningsaktivitet mot Norge, men spesielt russiske etterretningsoffiserer bruker mye tid på å forsøke å rekruttere kilder og pleie kontakt med personer i Norge.
  - Illustrert ved cyberoperasjonene mot Stortinget
- Gjennom oppkjøp og investeringer i norsk næringsliv kan fremmede stater få tilgang til informasjon og innflytelse som det ikke er i Norges interesse at de får.
- Flere stater forsøker å skaffe teknologi i Norge som de ikke har lov til å kjøpe.

Politisk motivert vold og trusselen mot myndighetspersoner

- Ekstrem islamisme og høyreekstremisme forventes fortsatt å utgjøre de største terrortruslene mot Norge, og det er mulig disse vil forsøke å gjennomføre terrorhandlinger i Norge.

- Antistatlige strømninger, der staten anses som illegitim, vurderes å ha et potensial for å radikalisere enkelte personer.

- Trusler mot myndighetspersoner forventes å øke noe i 2021.
  - Dette forårsakes av enkeltes misnøye med Covid-19-tiltak, flere radikaliserte høyreekstreme samt økt eksponering av saker og politikere i forbindelse med stortingsvalget.

Nærmere om cybertrusselen

- Antall alvorlige hendelser registrert hos Nasjonalt cybersikkerhetssenter (NCSC) i NSM i 2020 var tre ganger så mange som i 2019

- Spesielt om datainnbrudd med løsepengevirus (krypteringsvirus)
  - Det har vært en jevn og vesentlig økning i antallet datainnbrudd med løsepengevirus de siste årene, og det er meget sannsynlig at norske virksomheter vil bli utsatt for dette videre.
  - Metoden gir mulighet for høy fortjeneste samtidig som at identifisering av gjerningspersoner og straffeforfølgelse er meget komplekst.
  - Det er mulig at også norske virksomheter med samfunnskritiske funksjoner vil bli utsatt for slike datainnbrudd.
  - Koronapandemien har belyst sårbarheten til offentlige virksomheter med kritiske beredskapsfunksjoner. Internasjonalt er det meldt om flere hendelser med løsepengevirus mot nasjonale beredskapsfunksjoner.

Bedrageri mot næringslivet

- Det har vært en økning i antallet faktura- og direktørbedrageri rettet mot norske virksomheter de siste årene, og det er meget sannsynlig at kriminelle aktører vil øke sin aktivitet på området.

- Metoden gir høy fortjeneste og det er lav oppdagelsesrisiko.

- Større virksomheter er mer utsatt for målrettede bedragerier, mens mindre virksomheter oftere er utsatt for massebedragerier. Også frivillige organisasjoner er målgruppe.
  - Økt bruk av hjemmekontor har gjort bedrifter særlig utsatt for faktura- og direktørbedrageri. Under koronapandemien har det også blitt avslørt mange fakturabedragerier knyttet til blant annet smitteforebygging.

Investeringsbedrageri

- Et investeringsbedrageri går ut på å forlede privatpersoner eller foretak til å investere i prosjekter eller produkter som er verdiløse eller ikke-eksisterende. Sosial manipulering er en sentral del av bedrageriprosessen.

- Under koronapandemien har det vært en økning i antallet tilfeller av investeringsbedrageri
  - Spesielt aksjebedragerier via falske handelsplattformer.
  - Det er meget sannsynlig at investeringsbedragerier vil fortsette å øke både knyttet til kryptovaluta og falske handelsplattformer.

- Eiendomsbedrageri har vist seg å være lukrativt i Norge.
  - Bedragerne etablerer egne aksjeselskap som angivelig driver med eiendomsutvikling, og lurer småsparere til å investere. Aktørene selger så overprisede eiendommer til aksjeselskapene og sitter igjen med overskuddet. Et eksempel er Indigo Finans-saken.

RISIKOSTYRING OG ETTERLEVELSE INNEN SIKKERHET OG BEREDSKAP I NORSKE VIRKSOMHETER

Sårbarhet og sikkerhet

- Tre nasjonale hovedtrekk ifølge NSM
  1. Det digitale risikobildet er skjerpet
  2. Tydeligere risiko knyttet til sammensatte trusler

     Såkalte hybride trusler med bruk av et bredt spekter av virkemidler, der også påvirkning og villedning i sosiale medier, digitale angrep og strategiske kjøp og investeringer inngår
  3. Covid-19-pandemien har forsterket det eksisterende risikobildet

Nærmere om digital sårbarhet og sikkerhet (NSM)

- Digitaliseringen medfører økt effektivisering og innovasjon, men samtidig introduseres nye sårbarheter, avhengigheter og konsentrasjonsrisikoer som kan utnyttes og derfor må håndteres.
- Stadig flere prioriterer det digitale sikkerhetsarbeidet, men for mange norske virksomheter ikke har et forsvarlig sikkerhetsnivå for å beskytte viktige verdier.
  - F.eks. har mange virksomheter som rammes av løsepengevirus i liten grad vært forberedt. Økt bevissthet om digital risiko har ofte ikke blitt omsatt til handling. Dette bør være et tema i alle styrerom og ledergrupper.
- Noen digitale tjenester og leveranser er kritiske for samfunnet og vil kreve nasjonal digital autonomi. Datasenter står sentralt i vår felles digitale grunnmur og må følges opp grundig.
  - Store skytjenesteleverandørers datasentre er hovedsakelig lokalisert i utlandet og er underlagt et annet lands jurisdiksjon.
  - Tjenestene baseres til dels på digital infrastruktur som krysser mange landegrenser og som er sårbar for sabotasje, ødeleggelse og sikkerhetspolitiske endringer.
  - Disse leverandørene er også kommersielle aktører som vil kunne ha andre prioriteringer enn å opprettholde viktige norske samfunnsfunksjoner – f.eks. omprioritere ressurser i henhold til vertslandets egne beslutninger, herunder nedprioritering av support og lagrings-/prosesserings-/ nettverkskapasitet.

Andre sårbarheter og sikkerhetsforhold - funn i KRISINO 2021 (NSR)

- Risikostyring
  - Mens halvparten av de offentlige virksomhetene har skriftlig sikkerhetsvurdering er det bare en fjerdedel av de private som har det.
  - Store private virksomheter har det i like stor grad som store offentlige, men mellomstore og små private virksomheter skiller seg ut ved å ha det i mindre grad enn mellomstore og små offentlige virksomheter.
  - Offentlig virksomheter leser PSTs, NSMs og andre trusselvurderinger i større grad enn private virksomheter, mens Økokrims trusselvurdering leses i like stor grad av private som offentlige. Det er samtidig et klart mønster at store virksomheter bruker disse trusselvurderingene i større grad enn mindre virksomheter.
- Utro tjenere – ja, de finnes også i Norge…
  - 8 prosent har avdekket utro tjenere blant egne ansatte. Blant disse er det 25 prosent som anmeldte forholdet.
- Vold mot ansatte - skjer nok oftere enn man tror…
  - 10 prosent av virksomhetene har opplevd at ansatte har blitt utsatt for vold eller trusler om vold. Det er en nedgang fra 2019 da det var 13 prosent.
  - Hele 33 prosent av offentlige virksomheter har opplevd at ansatte utsettes for vold eller trusler om vold, mens det tilsvarende i private virksomheter er 4 prosent.

Beredskap i virksomhetene – Funn fra Beredskapsundersøkelsen (NSR)

- Jo større en virksomhet er, desto større sannsynlighet er det for at den har et rammeverk for sikkerhets- og beredskapsarbeidet sitt, herunder også beredskapsplaner.
  - Før vi ble rammet av covid-19 var det mest vanlig og å ha beredskapsplaner for bortfall av strøm og/ eller elektronisk kommunikasjon. Beredskap mot pandemi var minst vanlig av de fire undersøkte områdene.
- Det er en større andel blant de største virksomhetene som hadde alle typer beredskapsplaner før covid-19, enn tilfellet er for de mindre virksomhetene.
  - Blant de som hadde beredskapsplan for pandemi opplever tre-fjerdedeler at den var nyttig for å håndtere Covid-19.
  - Man kan ikke legge detaljerte planer for alle eventualiteter, men har man en plan, kan den hurtig tilpasses den aktuelle situasjonen. Er planen kjent for de ansatte og øvet ved jevne mellomrom, blir det enda lettere å selv kunne styre hvordan utfordringen vil påvirke virksomheten.
- Halvparten av virksomhetene som rapporterer at de har beredskapsplaner, har også rutiner for opplæring og øvelser.
- Undersøkelsen viser at det er få som benytter trusselvurderingene fra myndigheten i beredskapsplanleggingen.

Etterlevelse av sikkerhetsloven

- Ny sikkerhetslov fra 2019
- Det er gjort et betydelig arbeid med departementenes identifisering av grunnleggende nasjonale funksjoner (sentralt tema i loven).
- I løpet av 2021 skal de fleste virksomheter underlagt sikkerhetsloven ha gjort vurderinger knyttet til avhengigheter og rapportert disse inn til NSM.
- Lovens krav om et forsvarlig sikkerhetsnivå skal oppfylles ved å vurdere og håndtere risiko for å identifisere og gjennomføre sikkerhetstiltak.
- Gjeldende sikkerhetslov er således mer kompetansekrevende enn forrige sikkerhetslov. Dersom virksomhetene mangler relevant kompetanse om forebyggende sikkerhet – og det gjør mange - utgjør det en sårbarhet.
  - Både NSM, BDO og Juristenes utdanningssenter har e-læringskurs om sikkerhetsloven, som ble laget og publisert under pandemien

Etterlevelse av sikkerhetsloven - Funn fra Beredskapsundersøkelsen 2021 (NSR)

- 17% av respondentene svarer at de er underlagt sikkerhetsloven, 51 % at de ikke er det, mens 32% at de ikke vet.
- I et verdikjedeperspektiv svarer 24% at de leverer varer eller tjenester til virksomheter underlagt sikkerhetsloven, 45% at de ikke gjør det, mens 31% ikke vet.
- Det signifikante for begge disse spørsmålene og et urovekkende funn, er det betydelige antallet som *ikke vet*.

Konklusjoner vi kan trekke

- Trusselbildet mot norske virksomheter er meget sammensatt og utfordrende
- Det er behov og potensial for betydelig forbedring på flere områder innen sikkerhet og beredskap i norske virksomheter
- Mange virksomheter var – og er fortsatt – lite forberedte og sårbare ved pandemi og mot digital trusler
- Spesielt små og mellomstore private virksomheter har et forbedringspotensial
  - Antakelig utfordringer med egen kompetanse innen sikkerhet og beredskap samt å skalere ned og tilpasse de metodene og tiltakene som faktisk er tilgjengelig

VEIEN MOT LØSNINGENE FOR GOD NOK SIKKERHET OG BEREDSKAP

Gjør dette – tilpasset virksomheten egenart og behov

- Etabler tydelig «eierskap», roller og ansvar innen sikkerhet og beredskap
  - Involver også øverste ledelse i virksomheten
- Utvikle kompetansen innen sikkerhet og beredskap
  - Det er nå mange e-læringskurs på området
  - Gjelder kompetansen til både sentrale roller, innen IKT og anskaffelser og den enkelte medarbeider generelt
- Vurder risikoer
  - Bruk en anerkjent standard til hjelp, som NS 5814, NS 5832 eller ISO/IEC 27005
  - Bruk veiledere og prosess og metode fra NSM, DSB og NSR
  - Bruk anerkjente kilder for å identifisere verdier, trusler og sårbarheter relevante for dere

Gjør dette – tilpasset virksomheten egenart og behov

- Håndter risikoer og etterlev krav til sikkerhet
  - Basert på risikovurderingene
  - Basert på regulative krav som virksomheten er omfattet av (f.eks. personopplysningsloven og evt. sikkerhetsloven)
  - Basert på avtaler med kunder
  - Basert på anerkjente standarder og rammeverk (det er flere relevante standarder på området, samt NSMs grunnprinsipper for sikkerhet)
- Etabler et system for kontinuitet
  - Basert på ISO 22301
- Etabler beredskapsplaner og beredskapsøvelser
  - Basert på ISO- og NS-standarder (det er flere relevante på området)
  - Basert på veiledere fra DSB

BDO

tett på