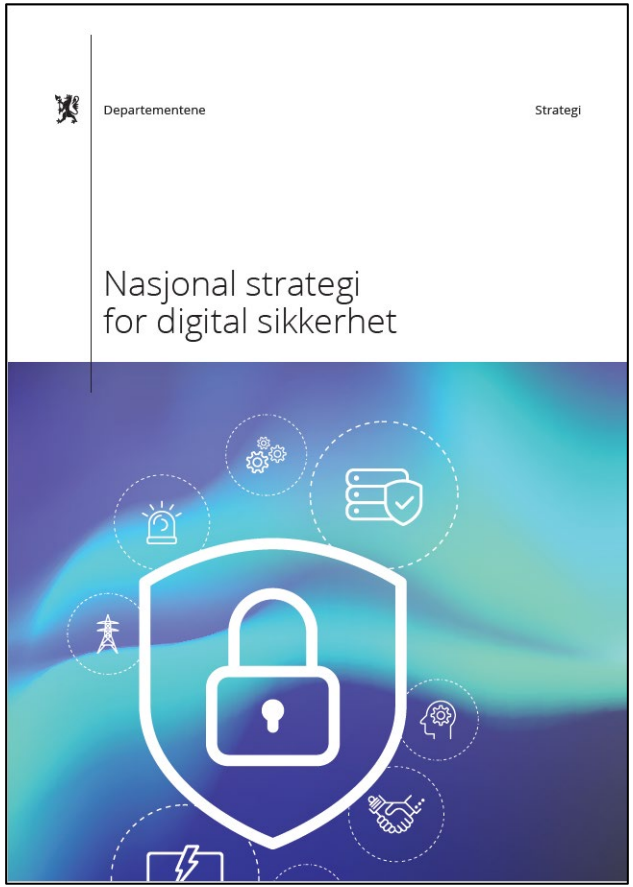
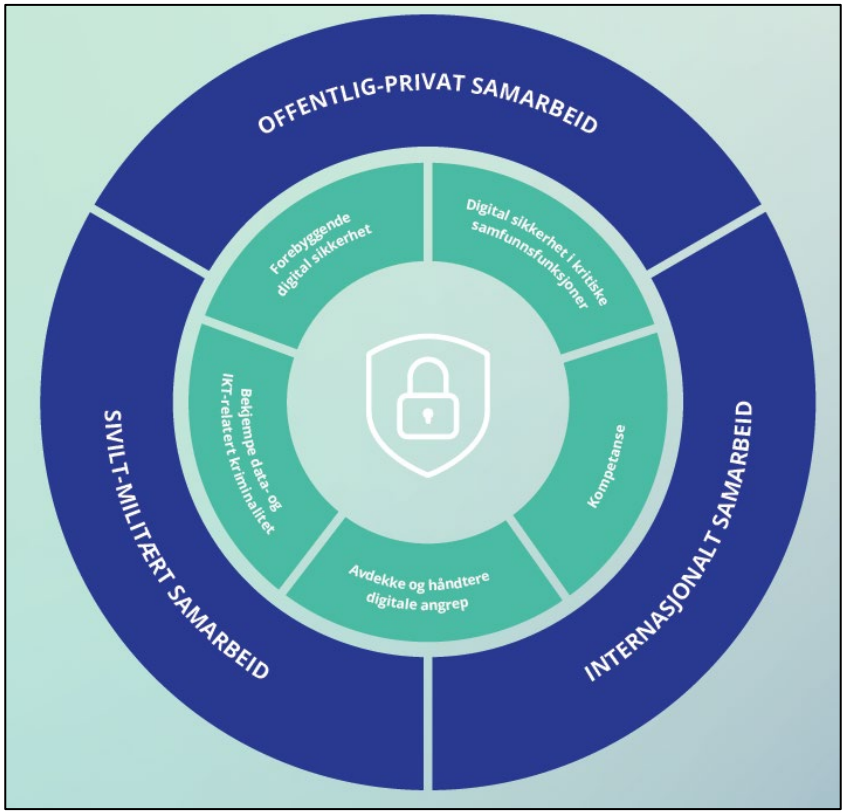
Trusler i det digital rom

Hvordan kan vi ivareta sikkerheten og bygge kultur for det?

Nils Kalstad, instituttleder
Institutt for informasjonssikkerhet og kommunikasjonsteknologi
18.05.2022


Departementene
Strategi
Nasjonal strategi
for digital sikkerhet


OFFENTLIG-PRIVAT SAMARBEID
INTERNASJONALT SAMARBEID
SIVILT-MILITÆRT SAMARBEID
Forebyggende digital sikkerhet
Digital sikkerhet i kritiske samfunnsfunksjoner
Kompetanse
Avdekke og håndtere digitale angrep
Bekjempe data- og IKT-relatert kriminalitet

Tiltak 27: Norwegian Cyber Range (NCR)

Norwegian Cyber Range (NCR) er den første nasjonale test- og øvingsarenaen for cyber- og informasjonssikkerhet på tvers av alle samfunnssektorer. NCR skal både være en akademisk og kommersiell øvingsarena, og på sikt også tilby kommersielle tjenester mot ulike markedssegmenter både privat og offentlig.

Testing, trening og øving er virkemidler for å eksponere virksomheter og mennesker for hendelser i realistiske, men trygge omgivelser. NCR sikrer effektiv og virkelighetsnær kompetansebygging, og kobler sammen samfunnsmodeller, digitale verdikjeder og digital infrastruktur i ett eller flere definerte miljøer. I tillegg vil man ut fra en slik øvingsarena kunne legge til rette for målrettet etter- og videreutdanningstilbud innenfor nasjonal IKT-sikkerhet.

NTNU har fått støtte fra fylkeskommunen i Oppland på 20 mill. kroner fordelt over tre år til å bygge opp NCR. Dette gjøres som en del av et samarbeid med Cyberforsvaret, Sivilforsvaret, Telenor Norge, EVRY, NorSIS, NSM og mnemonic gjennom NTNUs Center for Cyber and Information Security (NTNU CCIS).

Samarbeidet inkluderer også et felles prosjekt med Estland. Denne delen av prosjektet kalles «Open Cyber Range». Estland og Norge har fått 32 mill. kroner av EØS-midlene for å bli bedre til å bekjempe cyberkriminalitet. Prosjektet ledes av Estlands forsvarsdepartement, med deltagelse fra Teknologiuniversitet i Tallinn og NTNU sitt Institutt for informasjonssikkerhet og kommunikasjonsteknologi.

Ansvarlig virksomhet: NTNU
Gjennomføres: Lansert 2018

Styrke kjernemiljøene ved en kryptologisatsing fra 2018

Basisbevilgningen fra JD til NTNU CCIS (fra 2016) er på 5 mill. kroner årlig til områder som personvern, digital etterforskning og biometri. HOD bidrar til grunnbevilgningen med 2

En pilot om opplæring av barn og ungdom i regi av NSM, NVE, NorSIS, NTNU, UiO og Abelia i Oppegård, Ski og Rogaland.

Piloten er finansiert gjennom et spleiselag fra norske myndigheter, frivillig dugnad fra universiteter, private selskap og økonomisk støtte fra den amerikanske ambassaden. Piloten

CyberSec4Europe – et pilotprosjekt som del av den fremtidige etableringen av et felles europeisk kompetansenettverk for digital sikkerhet:

Pilotprosjektet startet ved årsskiftet 2018/2019. Formålet med pilotprosjektet er å bidra til at EU ivaretar og blir ledende i neste generasjon av digital sikkerhet og teknologi. I løpet av 3,5

European Cyber Security Challenge i regi av ENISA

Dette er en nasjonal og internasjonal konkurranse for å synliggjøre unge talenter. En juniorgruppe 16-20 år og en seniorgruppe 21-25 år. NTNU CCIS står for den norske konkurransen. Slike tiltak kan bidra til å skape blest og medieoppmerksomhet om kompetanse på digital sikkerhet blant ungdom og unge voksne.

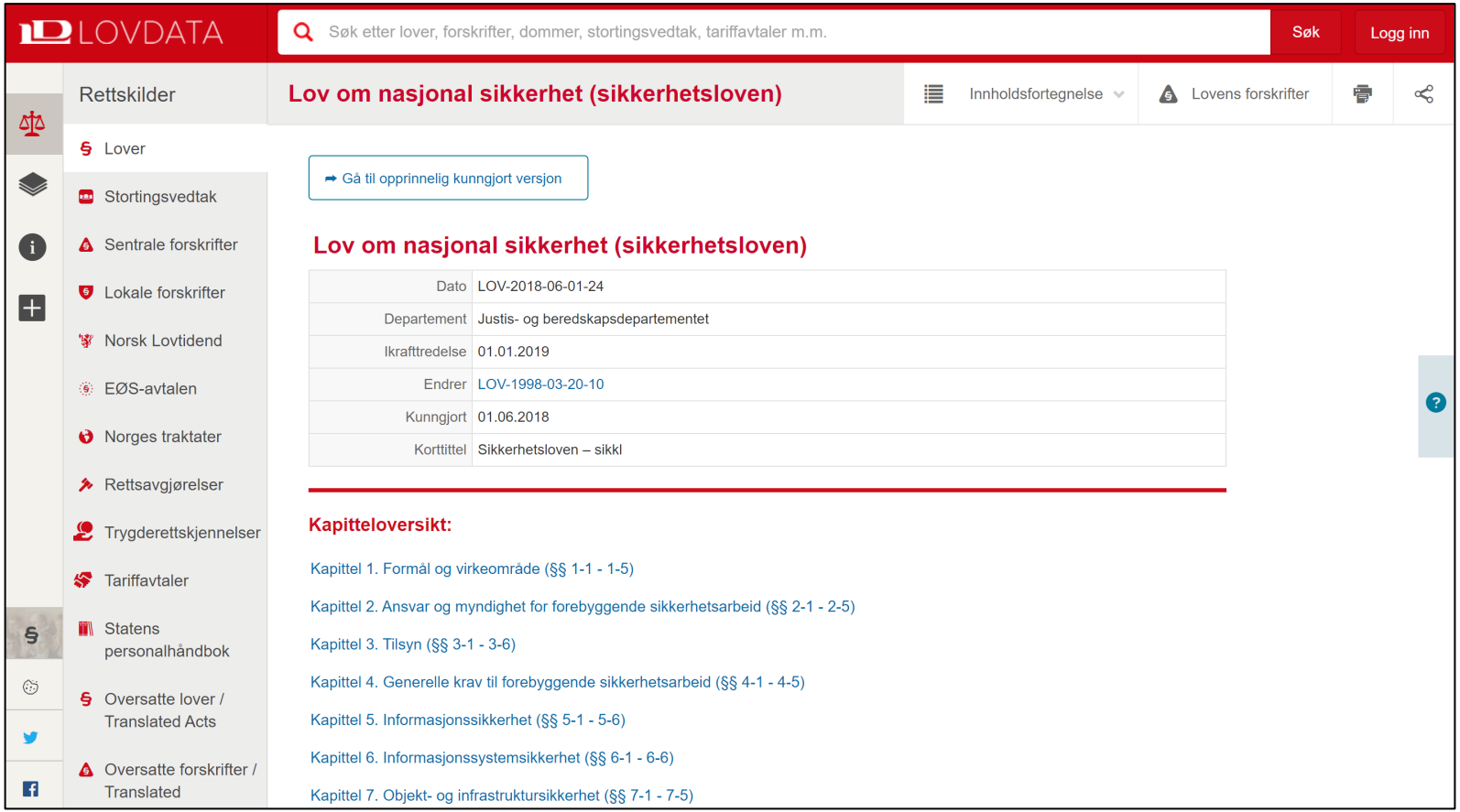
Our research groups:

- e-Health and Welfare Security
- Critical Infrastructure Security and Resilience
- Information Security and Privacy Management
- Norwegian Biometrics Laboratory
- Cyber Defence
- System security
- Applied Cryptography
- NTNU Digital Forenics Group

Our partners:

POLITIET, POLITIET, POLITIHØGSKOLEN, ØKOKRIM, ATEA, Hydro, KRIPOS, FST, Skatteetaten, COGNITE, bouvet, NORMA CYBER, WATCHCOM, Datatilsynet, tietoEvry, accenture, NKOM, Cyberingeniørskolen, Cyberforsvaret, Forsvarets høgskole, NORGES DOMSTOLER, KLUGE, TUSSA, buypass, BANEN, Hewlett Packard Enterprise, NASJONAL SIKKERHETSMYNDIGHET, NC-SPECTRUM, Innlandet, NorSIS, Nasjonalt ID-senter, DNV, IBM, HØGSKOLEN I INNLANDET, telenor, THALES, Eidsiva, Government of Iceland Ministry of Transport and Local Government, KINS, Statkraft, Sykehuset Innlandet HF, Capgemini, CIAM, FFI, DIPS, paloalto, VISMA, KPMG, EIDEL, cisco, BDO, IFE, KONGSBERG, Digdir, pwc, Orkla, Statnett, riskpoint, mnemonic, sopra steria

NTNU
CCIS – Center for Cyber and Information Security



https://lovdata.no/dokument/NL/lov/2018-06-01-24
https://lovdata.no/dokument/NL/lov/2018-06-01-24#KAPITTEL_6

Datatilsynet

Hva leter du etter?

MENY

1. Ansvarlighet, *internkontroll* og *informasjonssikkerhet*
2. Hvordan gjennomføre internkontroll i praksis
3. Iverksette styringssystem for informasjonssikkerhet
4. Oppfølging og opplæring
5. Internkontrollens struktur
6. Vedlegg – maler og støtteverktøy

Skriv ut alt innholdet

Søk i dette innholdet

Sist endret: 30.10.2018

Om informasjonssikkerhet

Personvernregelverket krever at personopplysninger skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, når de har behov for dem.

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.

Dersom risikovurderingen avdekker manglende tiltak må det vurderes om nye tiltak skal iverksettes for å oppnå tilfredsstillende sikkerhetsnivå for personopplysningene. Kontrollrutiner må utarbeides og jevnlig følges, for å kontrollere at tiltakene blir fulgt opp og virker etter hensikten.

En slik fremgangsmåte som skissert ovenfor vil sammen med tilhørende rutiner kunne utgjøre virksomhetens styringssystem for informasjonssikkerhet. Dette systemet for informasjonssikkerhet vil være en sentral del av virksomhetens internkontroll. Det er utviklet standarder som beskriver hvordan styringssystem for informasjonssikkerhet skal etableres.

Skriv ut denne siden

Neste side

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

NTNU

Nasjonale trusselvurderinger

Nasjonal sikkerhetsmyndighet

NSM er Norges direktorat for forebyggende nasjonal sikkerhet. Direktoratet gir råd om og gjennomfører tilsyn og andre kontrollaktiviteter på sivil og militær side knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har også et nasjonalt ansvar for å avdekke, varsle og koordinere håndtering av alvorlige IKT-angrep. «Risiko»-rapporten er NSMs årlige vurdering av risikobildet for nasjonal sikkerhet. I rapporten vurderer NSM hvordan sårbarheter i norske virksomheter og samfunnsfunksjoner påvirker risikobildet, i lys av trusselbildet som er trukket frem av Etterretningstjenesten og PST. Rapporten anbefaler også tiltak for å redusere risiko forbundet med sikkerhetstruende virksomhet.

Etterretningstjenesten

E-tjenesten er Norges nasjonale utenlandsetterretningstjeneste. Tjenesten er underlagt forsvarssjefen, men arbeidet omfatter både sivile og militære problemstillinger. E-tjenestens hovedoppgaver er å varsle om ytre trusler mot Norge og prioriterte norske interesser, støtte Forsvaret og forsvarsallianser Norge deltar i, og understøtte politiske beslutningsprosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitikk. I den årlige trusselvurderingen «FOKUS» gir E-tjenesten sin analyse av status og forventet utvikling innenfor tematiske og geografiske områder som tjenesten vurderer som særlig relevant for norsk sikkerhet og nasjonale interesser.

Politiets sikkerhetstjeneste

PST er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, underlagt justis- og beredskaps-ministeren. PST har som oppgave å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. Som ledd i dette skal tjenesten identifisere og vurdere trusler knyttet til etterretning, sabotasje, spredning av masseødeleggelsesvåpen, terror og ekstremisme. Vurderingene skal bidra i utformingen av politikk og støtte politiske beslutningsprosesser. PSTs årlige trusselvurdering er en del av tjenestens åpne samfunns-kommunikasjon der det redegjøres for forventet utvikling i trusselbildet.

Oppsummering

Den spente sikkerhetssituasjonen i Europa aktualiserer bruken av hybride trusler, såkalte sammensatte virkemidler. Russland og Kinas omfattende verktøykasser truer viktige nasjonale verdier og interesser. Risikoen for at vi ikke er i stand til å ivareta viktige sikkerhetsinteresser øker. En forverring av sikkerhetssituasjonen vil forsterke risikoen ytterligere. Den mest alvorlige utviklingen i det nasjonale risikobildet kan oppsummeres i tre hovedpunkter.

For det første øker gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner. Det skyldes blant annet at bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet, er for svak. Sikkerhetstiltakene er ikke dimensjonert for det reelle trusselbildet eller innføres ikke raskt nok når nye sårbarheter oppstår. Forståelsen for trussel- og risikobildet må økes og tiltak må iverksettes nå. Dette er et ledelsesansvar.

For det andre ser vi at sårbarheter i verdikjeder utnyttes mer målrettet. Gjennom stadig nye metoder og virkemidler, som cyberoperasjoner, investeringer og oppkjøp, utnytter trusselaktørene at virksomhetene er knyttet sammen i lange og komplekse verdikjeder. De leter etter sårbarheter hos leverandører og tilknyttede virksomheter. Ett av virkemidlene de bruker er å investere – direkte eller indirekte – i verdikjeder som er viktige for nasjonal sikkerhet. Dette gjør de gjennom kommersielle selskaper, og i de fleste tilfeller er aktiviteten helt lovlig.

Uoversiktlige verdikjeder gjør det vanskeligere å beskytte viktige nasjonale verdier. Verdikjedene må kartlegges, og sikkerhetsstyringen av leverandører og underleverandører må prioriteres høyere. For enkelte virksomheter kan det innebære at de må forenkle verdikjedene for å oppnå forsvarlig sikkerhet.

Datasentre og teleinfrastruktur, som igjen er avhengige av kraft, utgjør fundamentet i vår nasjonale digitale infrastruktur. Svikt i verdikjeder, også digitale, kan få konsekvenser både for samfunnssikkerheten og statssikkerheten, eksempelvis dersom sivile virksomheters tjenester eller leveranser til Forsvaret skulle falle bort. Viktige funksjoner må være tilgjengelige i fred, krise og krig.

For det tredje ser vi at taktskiftet i cyberaktivitet mot Norge skjerper den digitale risikoen. Fra 2019 til 2021 har NSM sett en tredobling i antall alvorlige hendelser og cyberoperasjoner. Fremmede etterretningstjenester står bak flere alvorlige hendelser i denne perioden. Risiko for alvorlige cyberoperasjoner er høy og øker for virksomheter som arbeider med utenriks-, forsvars- og sikkerhetspolitikk. Det samme gjelder virksomheter som driver forskning og utvikling innenfor forsvar, helse, maritim teknologi, petroleum og romvirksomhet.

I tillegg ser vi en kraftig økning i digital utpressing og sabotasje, såkalte løsepengevirus eller ransomware. Både her hjemme og i andre land har slike hendelser fått omfattende konsekvenser ved at systemer lammes og viktige tjenester stopper. Bare i desember 2021 ble matvareprodusenten Nortura, mediekonsernet Amedia og Nordland fylkeskommune rammet av slike cyberhendelser.

Selv om flere tar innover seg alvoret i det digitale trussel- og risikobildet, går den teknologiske utviklingen og endringene i sårbarhetsbildet så raskt at den digitale risikoen fortsetter å øke. Sikkerheten i IKT-systemene i norske virksomheter må derfor styrkes. NSMs grunnprinsipper for IKT-sikkerhet er et godt utgangspunkt for IKT-sikkerhetsarbeidet.

Nasjonal sikkerhet utfordres av teknologiutviklingen fordi vi gjør oss avhengige av nye tjenester, og fordi nye sårbarheter oppstår. Utviklingen innen satellitt- og romteknologi, droner, telekommunikasjon og kvanteteknologi er eksempler på fremskritt som også skaper sårbarheter trusselaktører kan utnytte. Vi må kontinuerlig utvikle sikkerheten i takt med den teknologiske utviklingen.

Det er et bredt spekter av både offentlige og private virksomheter som utgjør første skanse i beskyttelsen av Norge i dag. Det må settes av tilstrekkelige ressurser for å få på plass operasjonell risikostyring. Tiltak må iverksettes fortløpende basert på oppdaterte risikovurderinger.

For å styrke nasjonal sikkerhet trenger vi et betydelig løft i bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet, fra virksomhetens øverste ledelse til den enkelte ansatte. I denne rapporten gir vi en rekke anbefalinger for å bedre sikkerheten i norske virksomheter og øke den nasjonale motstandskraften mot hybride trusler.

Økt risiko krever økt årvåkenhet. Hjelp oss med å bygge et nasjonalt situasjonsbilde gjennom å rapportere sikkerhetstruende aktivitet og hendelser. Slik kan vi sammen iverksette de riktige og viktige tiltakene.

Internasjonal terrorisme

Terrortrusselen mot Europa kommer i hovedsak fra personer og løse nettverk av sympatisører uten sterke bånd til internasjonale terrororganisasjoner.

Et sammensatt trusselbilde

Russland og Kina benytter alle statens virkemidler for å fremme sin internasjonale posisjon.

Russlands åpne maktbruk

Det moderniserte russiske forsvaret er den dimensjonerende militære trusselen mot Norges suverenitet, befolkning, territorium, sentrale samfunnsfunksjoner og infrastruktur.

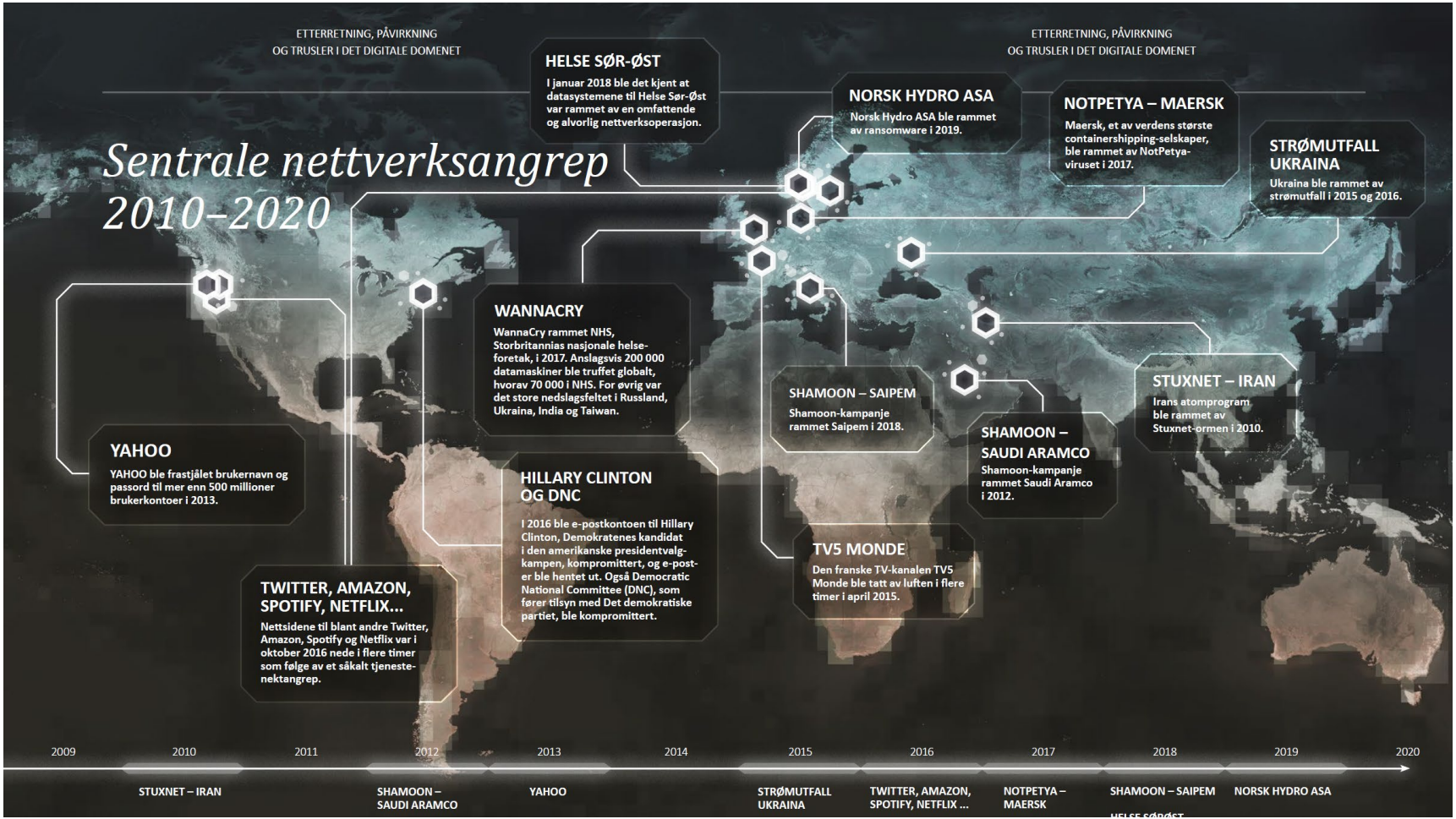
Xi Jinpings Kina

Kombinasjonen av selvsikkerhet og opplevelsen av å bli motarbeidet har gitt opphav til en mer offensiv utenriks-politikk og et mer konfliktfylt forhold til både USA og Vesten.

Regionale konflikter

Politisk uro og væpnet konflikt øker handlingsrommet til internasjonale terrororganisasjoner.

Fokus 2022
Innhold


ETTERRETNING, PÅVIRKNING
OG TRUSLER I DET DIGITALE DOMENET
ETTERRETNING, PÅVIRKNING
OG TRUSLER I DET DIGITALE DOMENET
Sentrale nettverksangrep
2010–2020
HELSE SØR-ØST
I januar 2018 ble det kjent at datasystemene til Helse Sør-Øst var rammet av en omfattende og alvorlig nettverksoperasjon.
NORSK HYDRO ASA
Norsk Hydro ASA ble rammet av ransomware i 2019.
NOTPETYA – MAERSK
Maersk, et av verdens største containershipping-selskaper, ble rammet av NotPetya-viruset i 2017.
STRØMUTFALL UKRAINA
Ukraina ble rammet av strømutfall i 2015 og 2016.
WANNACRY
WannaCry rammet NHS, Storbritannias nasjonale helse-foretak, i 2017. Anslagsvis 200 000 datamaskiner ble truffet globalt, hvorav 70 000 i NHS. For øvrig var det store nedslagsfeltet i Russland, Ukraina, India og Taiwan.
SHAMOON – SAIPEM
Shamoon-kampanje rammet Saipem i 2018.
STUXNET – IRAN
Irans atomprogram ble rammet av Stuxnet-ormen i 2010.
SHAMOON – SAUDI ARAMCO
Shamoon-kampanje rammet Saudi Aramco i 2012.
YAHOO
YAHOO ble frastjålet brukernavn og passord til mer enn 500 millioner brukerkontoer i 2013.
HILLARY CLINTON OG DNC
I 2016 ble e-postkontoen til Hillary Clinton, Demokratenes kandidat i den amerikanske presidentvalg-kampen, kompromittert, og e-post-er ble hentet ut. Også Democratic National Committee (DNC), som fører tilsyn med Det demokratiske partiet, ble kompromittert.
TV5 MONDE
Den franske TV-kanalen TV5 Monde ble tatt av luften i flere timer i april 2015.
TWITTER, AMAZON, SPOTIFY, NETFLIX...
Nettsidene til blant andre Twitter, Amazon, Spotify og Netflix var i oktober 2016 nede i flere timer som følge av et såkalt tjeneste-nektangrep.
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
STUXNET – IRAN
SHAMOON – SAUDI ARAMCO
YAHOO
STRØMUTFALL UKRAINA
TWITTER, AMAZON, SPOTIFY, NETFLIX ...
NOTPETYA – MAERSK
SHAMOON – SAIPEM
NORSK HYDRO ASA

Statlig etterretnings-virksomhet

Flere lands etterretningstjenester opererer på norsk jord. Blant disse vil russisk og kinesisk virksomhet utgjøre den største trusselen. De bruker en rekke metoder for å nå sine mål. Aktiviteten kan få alvorlige konsekvenser for Norge. Den kan påvirke Norges handlefrihet og svekke vår evne til å håndtere kriser. Den kan i tillegg svekke næringslivets konkurranseevne og bidra til at enkeltpersoner ikke føler seg trygge i landet vårt.

I året som har gått, har vi sett en markant økning i antall nettverksoperasjoner. Trusselen fra statlige nettverksoperasjoner er alvorlig og vil vedvare også i 2022.

Videre vil personer i Norge bli forsøkt rekruttert som kilder av andre lands etterretningstjenester. Andre stater vil ta i bruk stadig mer kompliserte selskapsstrukturer og utvise stor kreativitet for å anskaffe sensitiv teknologi fra norske virksomheter. Opposisjonelle og minoriteter vil bli overvåket av andre land.

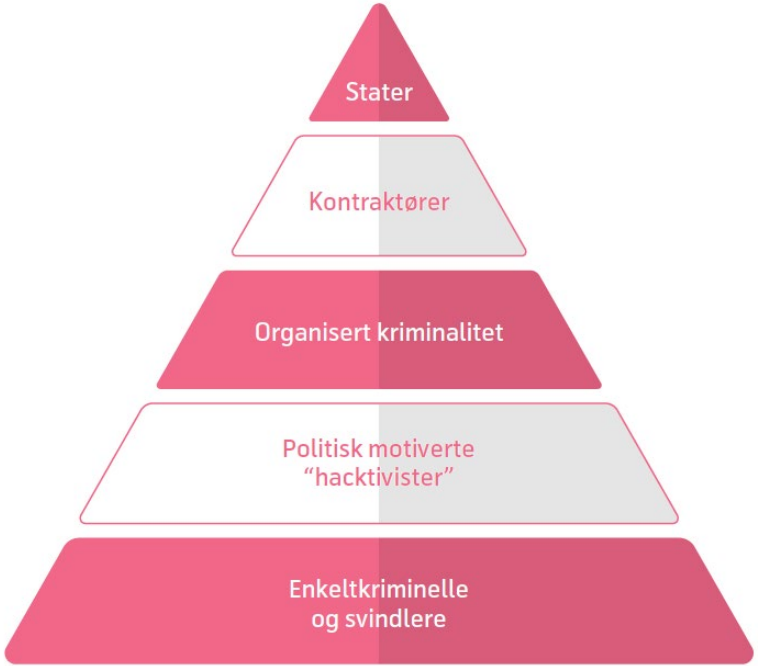
Nettverksoperasjoner vil fremdeles utgjøre en alvorlig trussel mot Norge

Nettverksoperasjoner har blitt en integrert del av aktiviteten til andre lands etterretningstjenester. Operasjonene mot Stortinget i 2020 og 2021 er eksempler på svært alvorlige hendelser. Fra foregående år har Nasjonal sikkerhetsmyndighet (NSM) observert en tredobling av alvorlige cyberhendelser mot offentlige og private virksomheter i Norge. En del av disse er utført av trusselaktører som opererer på vegne av fremmede stater. I 2021 har slike aktører lyktes med å bryte seg inn i nettverkene til norske myndigheter og private virksomheter. I all hovedsak er det Kina og Russland som står bak disse operasjonene. PST forventer at disse landene vil fortsette med sine nettverksoperasjoner mot Norge i 2022.

Flere land søker informasjon om norske beslutningsprosesser. Virksomheter som arbeider med norsk utenriks-, forsvars- og sikkerhetspolitikk, vil være særlig utsatte for nettverksoperasjoner. Det samme gjelder selskaper og forskningsmiljøer innenfor forsvar, helse og maritim teknologi. Petroleumssektoren og romsektoren bør også være forberedt på at uvedkommende vil forsøke å stjele informasjon fra deres datanettverk.

Som følge av Norges medlemskap i FNs sikkerhetsråd er etterretningstrusselen mot utenrikstjenesten forhøyet. Dette gjelder spesielt på det digitale området. Dette trusselbildet vil vedvare i 2022. Trusselen vil hovedsakelig komme fra Kina og Russland. Vi vet samtidig at aktører tilknyttet andre land også har utført nettverksoperasjoner mot Norge. Målet for disse operasjonene har ikke nødvendigvis vært å svekke Norge, men å styrke eget handlingsrom i eller opp mot Sikkerhetsrådet.

Etter normaliseringen av det bilaterale forholdet mellom Norge og Kina, har PST sett at kinesiske nettverksoperasjoner i økende grad fokuserer på norske politiske forhold. Dette er en endring fra tidligere, hvor en større andel av operasjonene var rettet mot teknologivirksomheter. Det er sannsynlig at kinesiske digitale trusselaktører har fått i oppdrag å kartlegge norske politikere og andre som kritiserer Kina. Det økte fokuset



Trusselaktørene
Det er flere typer trusselaktører som har interesser av våre tjenester og infrastruktur. Hvem og hva vi står opp mot er sammensatt og aktørene bak har forskjellig motivasjon.

De mest avanserte omtales ofte som *Advanced Persistent Threats* (APT), og er aktører med kapasitet, evne og vilje til å drive skjulte operasjoner over tid (i måneder og år) for å oppnå sin intensjon. Både stater, kontraktører og avansert organisert kriminalitet kan drive slike operasjoner. Aktører på et lavere nivå kan operere sammen med eller til støtte for aktører lenger opp.

Stater og kontraktører
Statlige aktører agerer for å understøtte egen stats politiske mål. Kontraktører er oppdragsstyrt og driver operasjoner som er betalt av stater, industri eller organiserte kriminelle. Disse kan ta oppdrag fra et videre spekter av oppdragsgivere, hvor motivene også kan sprike mer, fra industrispionasje på forskning og utvikling, til spionasje mot forhandlingsprosesser som kontraktsforhandlinger, fusjoner, budrunder og andre forretningskritiske prosesser.

Organisert kriminalitet
Organisert kriminalitet i cyberspace driver svindel for egen vinning, men er i ytterste konsekvens involvert i svært alvorlig kriminalitet som for eksempel hvitvasking av penger fra narkotikaomsetning, menneskehandel og terrorfinansiering. I dette segmentet har aktører tilgang til både verktøy og metoder som tidligere bare har vært forbeholdt statlige aktører og kontraktører.

Hacktivisme
Dette er cyberkriminelle med en politisk intensjon som de siste årene har blitt mindre synlige i aktørbildet.

Enkeltkriminelle og svindlere
Dette segmentet er kriminelle med en intensjon om å tjene penger til seg selv, og i noen tilfeller kriminelle som ønsker å vise hvor dyktige de er for å få innpass høyere opp i aktørhierarkiet.

Angrepet på Østre Toten kommune

Natt til 9. januar 2021 ble Østre Toten kommune rammet av et hackerangrep på våre datasystemer. Dette ble oppdaget på omsorgssenteret vårt umiddelbart og på morgenen ble det raskt klart at alle våre systemer var nede og kommuneledelsen satte krisestab. Hackerne hadde på forhånd forberedt angrepet inne på våre systemer slik at de denne natta kunne låse oss ned. De lastet over våre data til seg og slettet våre *backuper*. Vi våknet opp til en ny dag denne morgenen der internett og fagsystemer ikke var tilgjengelige. Det var svarte skjermer rundt i tjenestene våre.

Bror Helgestad
Ordfører
Østre Toten kommune

> Det har gått fem måneder siden angrepet nå. Vi nærmer oss en normalsituasjon der systemene kommer på plass, og data som produseres flyter til rett plass og kan hentes fram av de som trenger dem.

Østre Toten er en middels stor kommune sør i Innlandet. Vi har 15.000 innbyggere og vi lever av et aktivt og moderne landbruk, og mange av oss jobber i industribyen Raufoss eller i kunnskapsbyen Gjøvik. Østre Toten er et godt sted å bo og arbeide. Men for oss i kommuneledelsen og for de ansatte i kommunen må jeg fortelle at dette året har vært utfordrende. Covid-19 har gitt alle norske kommuner viktige oppgaver å løse i over et år, og nå rammet dette hackerangrepet oss i Østre Toten spesifikt.

Klokken 10:00 den 9. januar satte vi altså i krisestab uten internettforbindelse og med svarte skjermer rundt i tjenestene. Vi hadde 4G, egne telefoner og sosiale medier som verktøy i den akutte fasen der informasjonsbehovet var stort. Både ansatte, innbyggerne i kommunen og nasjonale så vel som lokale medier ville vite hva som hadde skjedd, og hvordan vi skulle løse det. Liv og helse var viktigst, deretter miljø og økonomi.

Østre Toten ligger i lavlandet Østafjells. Vi er ikke spesielt utsatt for flom, ras, storm og ikke når vi hatt terrortrusler heller. Vi bekymrer oss for om været passer avlinga og om markedet for bildeler fra Raufoss er godt, men nå var det altså alvor for oss i kommuneledelsen.

Kommunenes datasystemer på ulike fagområder er mange og de kommuniserer ofte sammen. Omkring 250 ulike fagsystemer, blant annet helse, skole, byggesak, personalstyring og lønn, var alle rammet. Som eksempler mistet helsesykepleierne timeavtalene sine og alle sine journaler, omsorgssenteret måtte få tak i en gammel telefaks for å formidle resepter og temperaturstyring av byggene vi bruker måtte passes manuelt. Vi gikk over til manuelle rutiner på svært mange oppgaver. Tjenestene klarte å levere og liv og helse ble ivaretatt, men det var krevende.

> Vi bekymrer oss for om været passer avlinga og om markedet for bildeler fra Raufoss er godt, men nå var det altså alvor for oss i kommuneledelsen.

Det har gått fem måneder siden angrepet nå. Vi nærmer oss en normalsituasjon der systemene kommer på plass, og data som produseres flyter til rett plass og kan hentes fram av de som trenger dem. Vi har brukt tiden godt. Selv om backuper var fjerna fra oss kunne vi hente fram et øyeblikksbilde som har gitt oss våre grunndata tilbake. Men de måtte inn i ny og frisk infrastruktur. Denne infrastrukturen har vi tilpassa slik at sikkerheten ivaretas på den beste tilgjengelige måten i dag. Det var viktig for oss å kunne overvåke aktiviteten i våre systemer for å avdekke unormal aktivitet, og dette har krevd mye av våre nye leverandører. Gjenoppbyggingа har krevd bruk av tid og kompetanse. Vi har brukt ca. 30 millioner NOK i egne tjenester, innkjøp av eksterne tjenester i tillegg til kjøp av varer. For framtida blir vi en krevende kunde i IKOMM AS som har overtatt vår IKT-avdeling.

Angrepet på Østre-Toten kommune

Å være ordfører i denne perioden har vært lærerikt. Kriseledelse og kommunikasjon uten tilgang til de normale hjelpemidlene stiller særskilte krav. Vi er jo en åpen organisasjon som er til for innbyggerne og publikum. Da går det ikke an å si «ingen kommentar». Vi valgte å fortelle åpent og ærlig om alt vi visste så tidlig som mulig. Vi ga konkret informasjon om hvordan hver enkelt tjeneste ble påvirket til innbyggerne våre. Både lokale og nasjonale medier har formidlet fra oss og vi tror det har bidratt til forståelse for hvor viktig datasikkerhet er. Vi er den eneste kommunen i landet som har blitt rammet av hacking på dette nivået til nå i Norge. Derfor er det viktig å fortelle historien slik at trusselen forstås og håndteres godt i kommunene.

Jeg tror også at små og mellomstore bedrifter er tjent med å lytte til oss. Datasikkerhet er en kostnad som må veies opp mot andre viktige innsatser i budsjettene. Vi vil gjerne bidra til at datasikkerhet får en større vekt.

Å være innbygger i vår kommune i denne perioden tror jeg har vært ganske fint. De er informert, som nevnt, og problemene som vi har hatt har først og fremst vært krevende for kommunen som organisasjon, og i mye mindre grad rammet innbyggerne. Med ett viktig unntak: når datakaprerne lastet data over fra oss til seg tok de med seg noen personsensitive data. Når de ikke fikk løsepenger fra oss truet de med å sende disse dataene ut i offentligheten på det mørke nettet. Og det gjorde de i noen grad i april. Vi fulgte opp dette med varslingsrutiner til innbyggerne generelt og til de innbyggerne som ble rammet spesielt. Datatilsynet ble varslet umiddelbart etter hendelsen om at slike data kunne være på avveie. Det er viktig å håndtere denne delen godt for å beholde innbyggernes tillit. Når vi passer på data som gjelder innbyggerne våre trenger vi den tilliten.

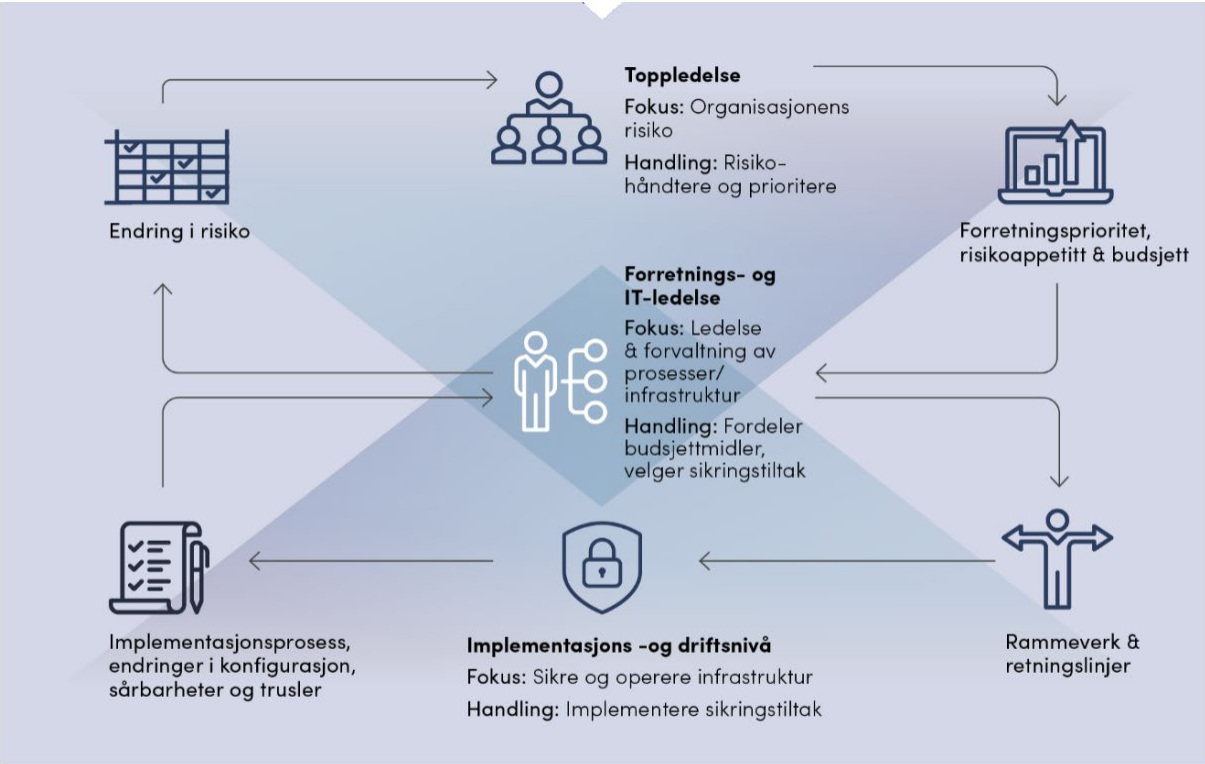
Norge har høye ambisjoner for digitalisering av offentlige tjenester. Den største andelen av disse tjenestene leveres av kommunene. Vi digitaliserer raskt og mye, men vi har nok ikke prioritert datasikkerhet høyt nok. Østre Toten sitt nivå på datasikkerhet skilte seg ikke vesentlig ut fra gjennomsnittet i norske kommuner i januar 2021.

Bror Helgestad
Ordfører
Østre Toten kommune

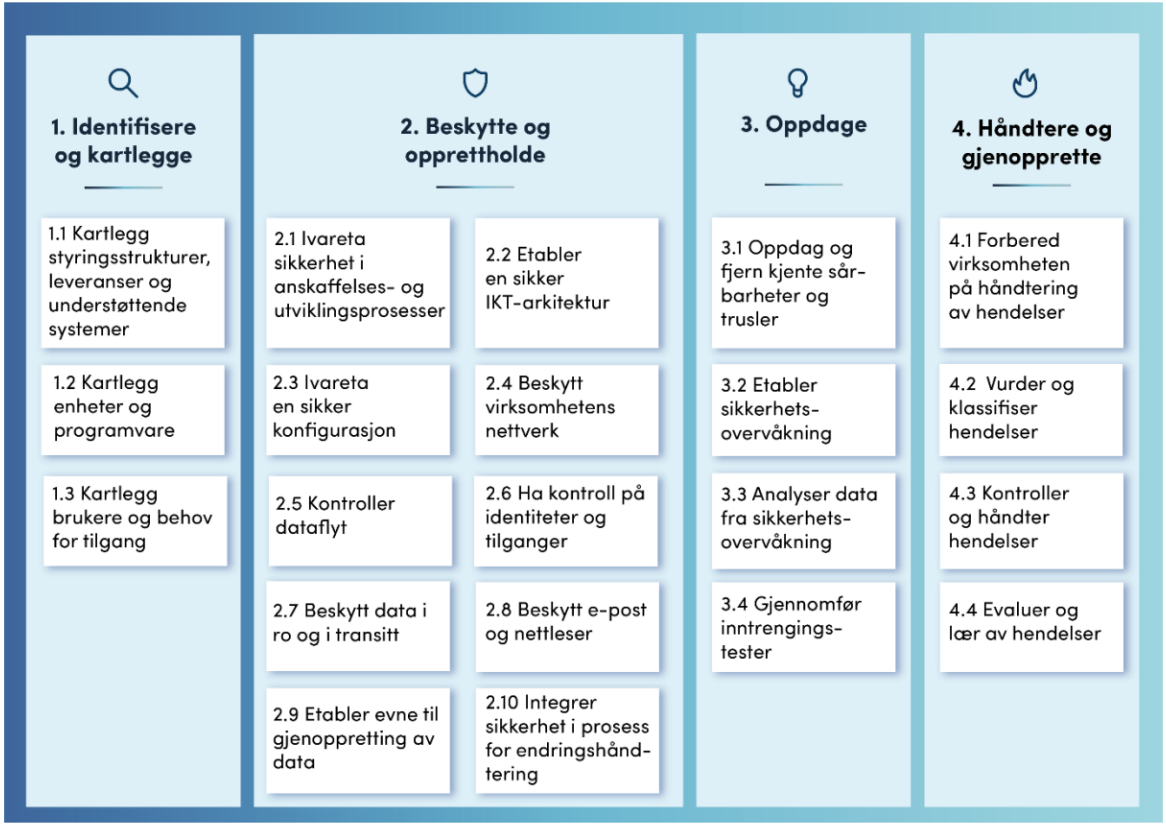
Virksomhetens behov i førersetet

Informasjonssikkerhet har fire funksjoner i en virksomhet

- Understøtte virksomhetens operative evne
- Beskytte virksomhetens data og informasjon
- Sikker drift av virksomhetens IKT-systemer
- Beskytte virksomhetens teknologiske aktiva

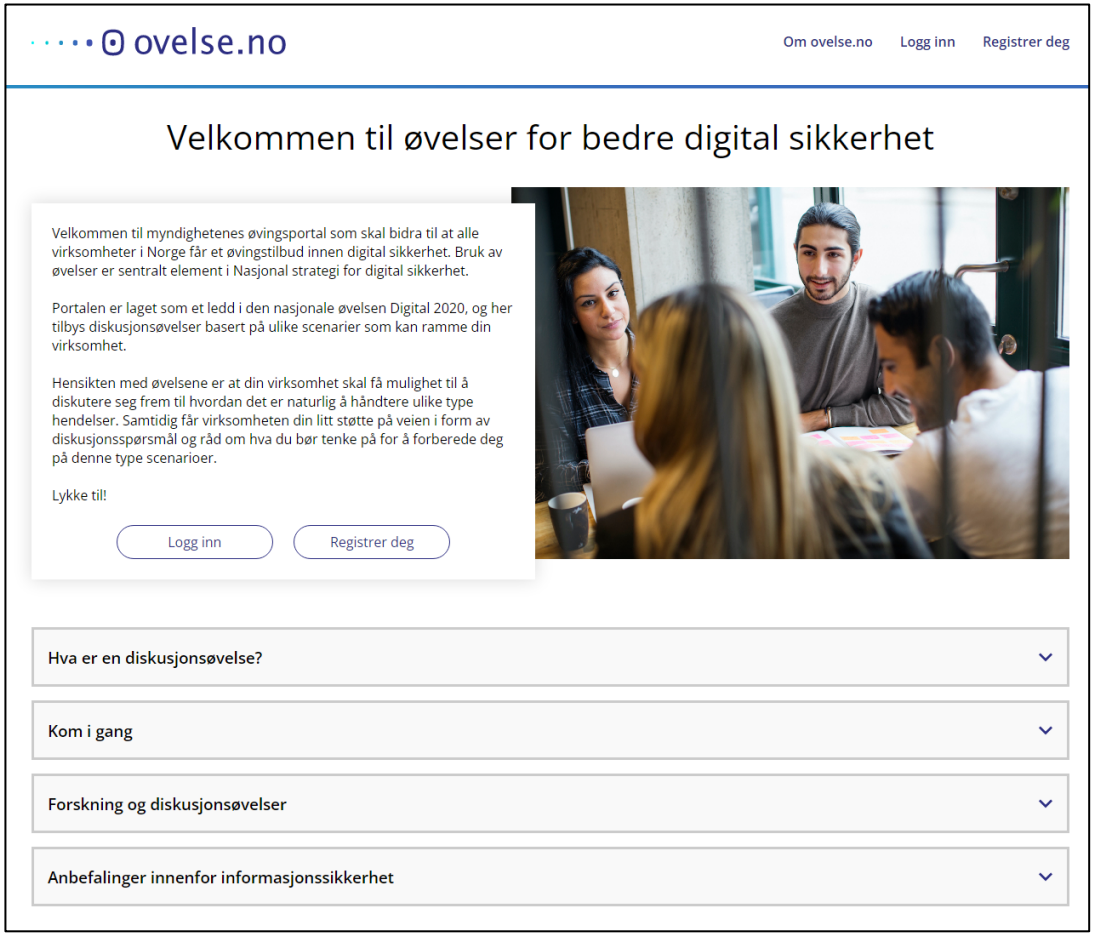


Figur 1 - Informasjonsflyt i en virksomhet



Figur 2 - Oversikt over NSMs grunnprinsipper for IKT-sikkerhet.

https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt



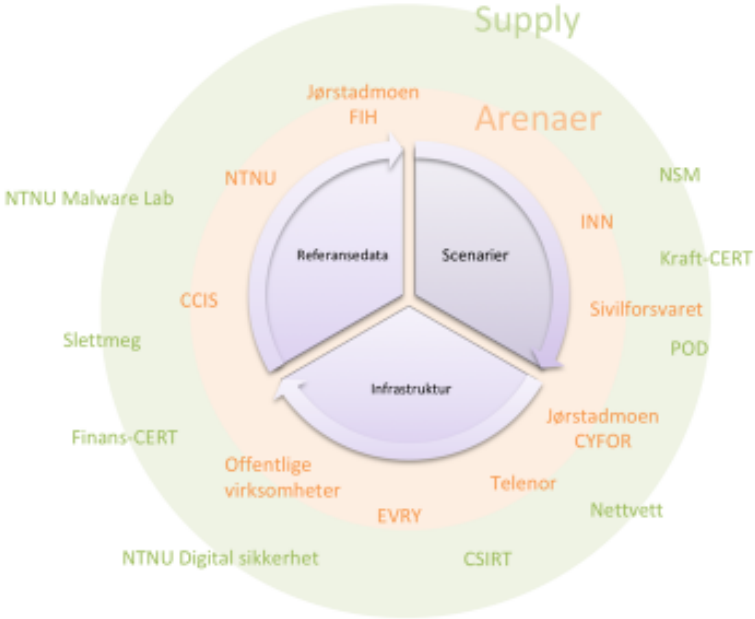
Øvelser i portalen:

1. Samfunnskritiske funksjoner ute av spill
2. Innsider vitende
3. Samfunnsviktige systemer ute av spill
4. Sårbarhetsvarsling
5. Personopplysninger på avveie – phishing
6. Kompromitterte servere
7. Personopplysninger på avveie – forsendelse med e-post
8. Personopplysninger på avveie – outsourcing og Office365
9. Innsider utvidende
10. Direktørsvindel
11. Bevissthet rundt egen teknologi
12. Hjemmekontor

Samarbeidspartnere

dsb Direktoratet for samfunnssikkerhet og beredskap
Digitaliseringsdirektoratet Norwegian Digitalisation Agency
NTNU Kunnskap for en bedre verden
NorSIS
NASJONAL SIKKERHETSMYNDIGHET

NTNU



SOCIETY

- Strategic, policy and regulation level

DIGITAL VALUE CHAINS

- Operational and tactical decision level

CYBER INFRASTRUCTURE

- Technical and design decision level


ENTREPRENEUR
ACADEMICS
CAPITAL
YOUR CLUSTER THEME
CLUSTER LEADERS
CLUSTER MEMBERS
GOVERNMENT
CORPORATE

IDÉMOTTAK

3

1. VerifyMed
2. Pulse measurement for helmet
3. Readiness toolkit

IDÉVURDERING

7

1. Modeling and Measuring Maturity of Organization
2. System and Method to Introduce Vulnerabilites in Computer Systems
3. Secure-AIS
4. Morphing Attack Detection (250')
5. Threat actor simulation
6. LOCARD
7. AI Driven Smartband

PROSJEKT DESIGN

5

1. Face morphing detection on smartphone (3)
2. 3D face morphing
3. Soundprint
4. Post-quantum protocol (250')
5. ADDING (450')

PROSJEKT

3

1. AiBA (6 650'), spin-off April 2022
2. Fruit analysis/Raygrade (1 200') – April/May 2022
3. SeCORE (450') – 2022?

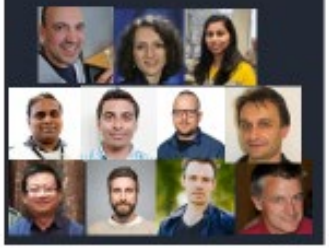
PORTEFØLJE

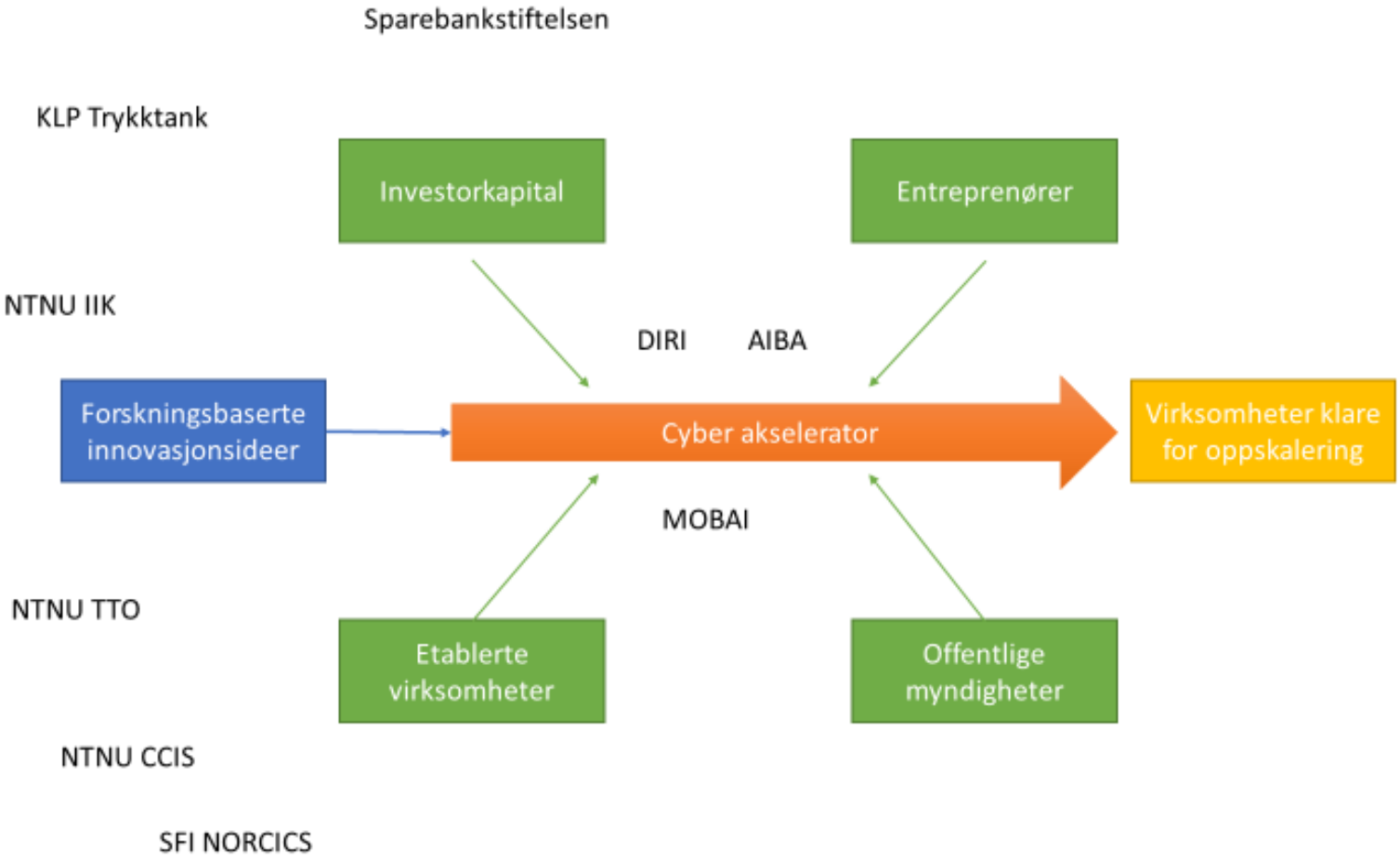
Memoscale AS (2016)
ABC Security AS / Biofy (2019)
Mobai AS (2019)
Graphchain AS (2019)
Diri AS (2020)
AiBA (2022)

6 + 6

SPIN-OFF

LISENSAVTALE




Sparebankstiftelsen
KLP Trykktank
Investorkapital
Entreprenører
NTNU IIK
DIRI
AIBA
Forskningsbaserte innovasjonsideer
Cyber akselerator
Virksomheter klare for oppskalering
MOBAI
NTNU TTO
Etablerte virksomheter
Offentlige myndigheter
NTNU CCIS
SFI NORCICS

NORCICS

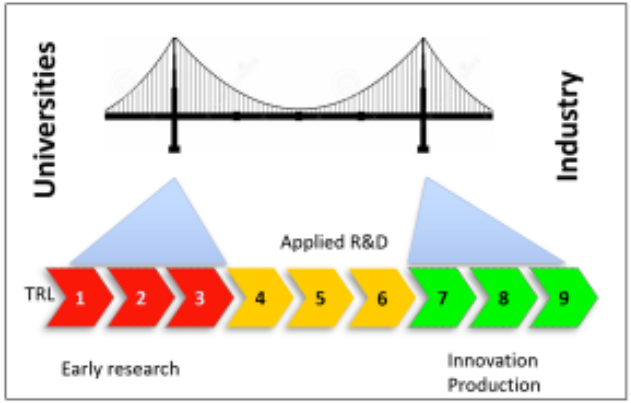
SFI Norwegian Centre for Cybersecurity in Critical Sectors

SFI: Norwegian Centre for Cybersecurity in Critical Sectors

(Norsk senter for cybersikkerhet i kritiske samfunnsfunksjoner)

Senterleder: Sokratis Katsikas

- **NORCICS** skal bidra til at Norge blir verdensledende ikke bare på digitalisering, men også på digital sikkerhet.
- **NORCICS** skal forberede sikkerheten og robustheten i våre kritiske samfunnsfunksjoner og i samfunnskritisk infrastruktur.
- **NORCICS** skal utvikle innovative cybersikkerhetsløsninger for at vi som nasjon, våre virksomheter og innbygger skal kunne stå imot et digitalt trusselbilde i rivende utvikling.



SIEMENS, HELGELAND KRAFT, YARA, Lyse, POLITIET, UiA Universitetet i Agder, Hydro, KONGSBERG, equinor, NC-SPECTRUM, NTNU CCIS Center for Cyber and Information Security, Elvia, mnemonic, NorSIS, SINTEF, NR Norsk Regnesentral