CYBERSIKKERHET

VEIKART FOR NORGE

(Oktober 2023 - versjon 0.8)

IKT Norge

INNHOLDSFORTEGNELSE

INNLEDNING

EU og resten av verden bruker nå store ressurser for å skape fremtidens digitale konkurransekraft. For at Norge skal kunne følge med på dette, og får å kunne ta en ledende rolle innen cybersikkerhet, er det avgjørende både med en robust og sikker infrastruktur, og myndigheter og selskaper som tar ansvar for å skape nødvendige tillit.

Norge er også helt avhengig av digital infrastruktur og digitale løsninger for at dagens samfunnet skal fungere. Vi - både borgere og bedrifter - har krav og forventninger om at alt skal virke selv i en eventuell krise eller under angrep. Dette må få store konsekvenser for hvordan innsatsen og investeringene skal være fremover.

Med denne bakgrunnen har IKT-Norge identifisert ti områder vi mener bør inngå i et "Veikart for Cybersikkerhet" i Norge.

(Dette er en beta-versjon vi skal videreutvikle sammen med medlemmene. Første lansering blir som innspill til regjeringens digitaliseringsstrategi innen 30. november.)

1. STRATEGI

Norge trenger å utvikle en omfattende nasjonal cybersikkerhetsstrategi som klart definerer nasjonens mål, ansvar, og forventninger. Dette har vi ikke i dag. Denne strategien må oppdateres regelmessig for å reflektere det skiftende trussellandskapet.

Vi trenger å :

a. Sette felles mål på tvers av sektorer og privat, offentlig, akademia (se vedlegg 1).
b. Definere tydelige roller og ansvar mellom offentlige og private sektorer, og styrke samhandlingen mellom EOS-tjenestene.
c. Kartlegge nasjonale kritiske infrastrukturer, tjenester og avhengigheter.
d. Etablere en plan for måling, beredskap og respons ved cyberangrep.
e. Etablere strategien som en langtidsplan med årlige revisjoner med mål å realisere det digitale målbildet.

2. SITUASJONSFORSTÅELSE

Norge trenger en fortløpende og oppdatert situasjonsforståelse på tvers av samfunnet. Dette gjelder på tvers av sivilt og militært, departement og sektorer, privat og offentlig. Dette har vi ikke i dag.

Vi trenger å:

a. Etablere tydelig ansvar for hvem som har ansvaret for innhenting, analyse og kommunikasjon på tvers av alle sektorer i Norge (i utgangspunktet justis og forsvar)
b. Etablere løsninger for sikkerhetsgradert samhandling
c. Opprette et rammeverk for obligatorisk rapportering av cyberhendelser (nå rapporteres 1% - ref. side 25 NSM).
d. Etablere systematisk overvåkning av hybridoperasjoner inklusiv "virkelighetsmanipulering" som rapporteres inn sammen med det totale situasjonsbildet.
e. Etablere økt evne til å avdekke skjult cyberaktivitet i virksomhetens infrastruktur.
f. Gjennomføre en kvantitativ undersøkelse første halvår 2024 for å få status dekke dagens motstandskraft som utgangspunkt for prioritering
g. Gjennomføre systematisk kartlegging av leverandørkjeder og tredjepartsrisiko - ref NSM Risiko 2023 [1]

3. RESPONSEVNE

Sikre responsmekanismer på tvers av samfunnet på bakgrunn av et felles oppdatert situasjonsbildet, og som reagerer koordinert på tvers av sektorer etter innøvde planer gjennom hele krisespekteret.

Vi trenger å:

a. Etablere tydelig ansvar og ledelse på tvers av sektorer i hele krisespekteret
b. Oppdatere beredskapsplaner for sivil sektor basert på krise- og krigsscenario.
c. Videreutvikle dagens nasjonale cybersikkerhetssenter som kan koordinere responsen til store cyberhendelser, inklusiv vurdere etablere

[1] "*Viktige samfunnsfunksjoner er avhengige av leverandører og underleverandører. Disse kan ha potensielt ukjente og alvorlige sårbarheter. Vi er ikke sikrere enn det svakeste ledd. Dette krever at vi evner å oppdage og avverge sikkerhetstruende virksomhet også i leverandørkjedene vi er så avhengige av*"

en SMB CERT, og tilby assistanse til berørte organisasjoner utover dagens mandat.

d. Sikre tilgang på digitale komponenter

4. INFRASTRUKTURELL ROBUSTHET

Sikre at kritisk infrastruktur (telekom, datasenter, kraftnett, finans, transport, helsevesen) er spesielt beskyttet og kan gjenopprettes raskt etter et angrep for å understøtte totalforsvarsevnen gjennom krisespekteret.

Vi trenger å:

a. Etablere en langtidsplan (etter mal for nasjonal transportplan) for digital infrastruktur som også dimensjonerer for krise og krig med målsetting, planer og tilhørende finansiering for å sikre nødvendig operativitet i hele krisespekteret.
b. Stille krav om vurdering av sikkerhet ved definerte anskaffelser

5. LOVER OG REGLER

Utvikle, tilpasse og implementere robuste lover og regelverk for cybersikkerhet som dekker alle aspekter av den digitale infrastrukturen, og setter klare standarder for organisasjoner og enkeltpersoner.

Vi trenger å:

a. Oppdater eksisterende lovgivning for å dekke dagens trusselbilde og etablere rapportering på status på tvers av sektorer inklusiv implementering av ny “Lov om digital sikkerhet”.
b. Innføre NIS 1 asap
c. Forberede innføring av NIS 2. Flere av tiltakene iht NIS 2 vil omhandle flere av områdene omtalt under de andre områdene i dette veikartet. Kombinert med blant annet TIBER, DORA og etter hvert EUs Cyber Resilience Act vil samlet styrke situasjonen.

6. UTDANNING OG BEVISSTGJØRING

Styrke satsingen på utdanning innen cybersikkerhet på alle nivåer – fra grunnskole til universitet – og fremme bevissthet om cybersikkerhet blant befolkningen.

Vi trenger å:

a. Gjøre NSMs grunnkurs obligatorisk for alle ledere i stat og kommune (ordførere, rådmenn etc)
b. Utvikle og implementere andre opplæringsprogrammer på tvers (obligatoriske og frivillige)
c. Gjennomføre nasjonale informasjonskampanjer med oppdaterte "best practice" inklusiv f.eks. insiderisiko etc.
d. Utvikle spesielle programmer innen kryptografi, cyber og kvanteteknologi.

7. FORSKNING OG UTVIKLING

Investere i forskning og utvikling for å holde tritt med den raske utviklingen innen teknologi og trusler. Dette inkluderer også fremme av offentlig-private partnerskap for å støtte innovasjon.

Vi trenger å:

a. Etablere flere sentre for forskning innen cybersikkerhet.
b. Integrer cybersikkerhet i utdanningssystemet, fra grunnskole til universitetsnivå.
c. Tilby spesialiserte kurs og sertifiseringer for profesjonelle.

8. INTERNASJONALT SAMARBEIDE

Arbeide tettere med allierte land og internasjonale organisasjoner for å dele trusselinformasjon, beste praksis og koordinere respons på grenseoverskridende trusler.

Vi trenger å:

a. Inngå bilaterale og multilaterale avtaler om cybersikkerhet.
b. Være en aktiv pådriver for mer nordisk samarbeid og økt aktivitet i internasjonale fora som NATO, EU og FN.
c. Bidra til utviklingen av internasjonale standarder og normer
d. Etablere Norden som en felles sikkerhetssone med felles sikkerhetsklarering av personell, lagring av kritiske komponenter, duplisering av funksjoner og redundante løsninger.

9. MÅLING OG REGELMESSIGE VURDERINGER

Innføre KPIer som måler trusselbildet og beredskapen, og gjennomføre regelmessige risikovurderinger og "red team"-øvelser for å identifisere sårbarheter i systemene, samt teste beredskap og responskapasitet.

Vi trenger å:

a. Gjennomføre regelmessige kriseøvelser.
b. Utvikle spesifikke planer for beskyttelse av kritiske infrastrukturer.
c. Etablere hurtige responskapasiteter ved cyberhendelser.

10. UTVIKLE EN VERDENSLEDENDE SIKKERHETSINDUSTRI

Norge har et godt utgangspunkt for å utvikle en verdensledende sikkerhetsindustri som vil bidra til at Norge kan ligge i front på cybersikkerhet. Norge er blant verdens mest digitale land, har høy kompetanse og modenhet, og vi er et land kjent for sikkerhet, forutsigbarhet og etterrettelighet.

Vi trenger å:

a. Utvikle målrettede programmer for næringsutvikling av norsk sikkerhetsindustri
b. Målrette satsingen på utvikling av økosystemet rundt cybersikkerhet inkludert datasenterindustrien, industrielle programvare etc.

VEDLEGG 1: Strategiske Sikkerhetsmål

Vi støtter “Strategiske Sikkerhetsråd” gitt av NSM i sin rapport “Et motstandsdyktig Norge - Sikkerhetsfaglige råd, 9 mai 2023

1. Norske virksomheter skaper bærekraftige verdier og ivaretar forsvarlig sikkerhet.
2. Norske myndigheter har en omforent situasjonsforståelse av trussel- og risikobildet.
3. Regjeringen får rettidig beslutningsstøtte som sikrer målrettet respons ved hendelser som kan skade nasjonal sikkerhet.
4. Sikkerhetsarbeidet i det norske samfunnet bidrar til å opprettholde tillit og til å styrke motstandskraft og forsvarsvilje i hele befolkningen.
5. Myndigheter, virksomheter og enkeltindivider gjenkjenner og varsler om sikkerhetstruende aktivitet og påvirkningsoperasjoner.
6. Norge har tilstrekkelig nasjonal kontroll over funksjoner og infrastruktur med betydning for nasjonal sikkerhet.
7. Norge har høy kompetanse innen cybersikkerhet og teknologier av betydning for nasjonal sikkerhet.
8. Norge har robust infrastruktur og satellittbaserte tjenester som understøtter totalforsvarsevnen gjennom krisespekteret.
9. Norge evner å motstå cyberoperasjoner som truer nasjonal sikkerhet i fred, krise og krig.
10. Alle deler av det norske samfunnet har digital motstandskraft på et langt høyere nivå.
11. Norske myndigheter hindrer at trusselaktører får tilgang til data om enkeltindivider som kan brukes til å skade nasjonal sikkerhet.
12. Norge har en god nasjonal evne til å avdekke, forhindre og håndtere innsidevirksomhet.

VEDLEGG 2: Relevante ressurser og referanser

Accenture
State of Cybersecurity Resilience 2023
How cybersecurity boosts enterprise reinvention to drive business resilience

Deloitte
Deloitte Global Future of Cyber Survey 2023

KPMG
Cybersecurity considerations 2023

Microsoft
Developing a National Strategy for Cybersecurity: FOUNDATIONS FOR SECURITY, GROWTH, AND INNOVATION

NSM
Et motstandsdyktig Norge - sikkerhetsfaglige råd

Radar Group
State of the Nation Norge
Digital- och säkerhetsmognad små och mellanstora svenska företag
Lägesbild cyberhot Maj 2023
Cybersäkerhet 2023
Säker digitalisering med hjälp av NIS2

Telenor
Det blir alvor - Digital sikkerhet 2023

VEDLEGG 3: Langtidsplan for den digitale infrastrukturen

Les mer om IKT-Norges forslag og rapport om en langtidsplan for den digitale infrastrukturen.

VEDLEGG 4: Forslag til bevilgninger i Statsbudsjettet 2024

(Spilt inn til finansdepartementet i juni 2023)

IKT-Norge er fortsatt bekymret for Norges evne til å stå mot cybersikkerhet, bl.a. begrunnet med at cybersikkerhet ikke er prioritert høyt nok de siste årene og at det både utdannes og rekrutteres for få med spisskompetanse knyttet til cybersikkerhet. Dette gjenspeiles også i Riksrevisjonens seneste undersøkelse av myndighetens samordning av arbeidet med digital sikkerhet i sivil sektor. Undersøkelsen konkluderer bl.a. med at Justis- og beredskapsdepartementet ikke ivaretar ansvaret for digital sikkerhet i sivil sektor godt nok, noe som igjen kan få alvorlige konsekvenser for kritiske samfunnsfunksjoner og nasjonale sikkerhetsinteresser.

IKT-Norge er særlig bekymret for den digitale sikkerheten i kommunene. Bare ca. 60 prosent av norske kommuner mener at de har sikret sine egne data godt nok. Rapporten «IT i praksis» (Rambøll 2022) viser at kun 38 prosent av kommunene mener at de selv har tilstrekkelig kompetanse på informasjonssikkerhet.
En undersøkelse fra YouGov viser at et stort flertall av innbyggerne ikke har tillit til at kommunene har nok kunnskap til å ivareta personlige data på en trygg måte eller har tillit til at kommunen prioriterer IT-sikkerhet i tilstrekkelig grad. Bare 26 prosent har tillit til at kommunene har ressurs nok til å stå imot mulige hackerangrep.

Dessuten er datainnbrudd i kommunesektoren svært dyrt. Datainnbruddet i Østre Toten kommune i januar 2021 kostet kommunen minst 32 millioner kroner, i tillegg til bot fra Datatilsynet på 4 millioner kroner. Av dette har igjen staten kompensert Østre Toten med 16 millioner kroner.

Vi etterlyser derfor resultater av de 50 millioner kroner som ble bevilget til økt sikkerhet i kommunesektoren i forbindelse med Stortingets behandling av Prop. 78 S (2021-2022) “Ukraina-pakken” i fjor vår og viser bl.a. til Dokument nr. 15:1726 (2022-2023) hvor det fremgår at regjeringen fortsatt ikke har en plan for hvordan disse midlene skal brukes.

Vi er videre kjent med at Simula i innspill til KDD har tatt initiativ til å starte et arbeid for å utarbeide og vedlikeholde en oversikt over Norges digitale avhengigheter mot fremmede makter. Dette er etter vårt syn både et viktig og helt nødvendig arbeid. Vi ber derfor regjeringen sette av nødvendige midler til et slikt forskningsarbeid i forbindelse med statsbudsjettet for 2024

Vi viser også til vårt innspill til næringsministeren om et økt samarbeid mellom næringslivet og myndighetene knyttet til cybersikkerhet, spesielt i de minste bedriftene og våre forslag til konkrete tiltak.

Konkret ber IKT-Norge regjeringen om:

1. **Målrettede tiltak for å styrke den digitale sikkerheten i kommunesektoren i størrelsesorden 50-100 mill. kroner**
2. **Styrke nasjonalt cyberkrimsenter (NC3) med 50 mill. kroner**
3. **Opprette et nasjonalt beredskapslager for sentrale IKT-komponenter**
4. **Sørge for fortgang i arbeidet med å etablere en felles informasjonsportal etter dansk modell.**
5. **Vurdere å opprette et eget bransjeprogram knyttet til datasikkerhet i små bedrifter.**
6. **Sette i gang et forsknings- og kartleggingsarbeid med formål å utarbeide og vedlikeholde en oversikt over Norges digitale avhengigheter mot fremmede makter.**