05 APR 2019

POLITIETS
SIKKERHETSTJENESTE

Postboks 4773 Nydalen
0421 OSLO
post@pst.politiet.no
Tlf.nr. 23 30 50 00
Faksnr. 23 30 51 20
Besøksadresse:
Nydalen allé 35

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref.:
Vår ref.: 18/12060-7
Dato: 29. mars 2019

Innspill fra PST- Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer og NOU 2018:14 IKT-sikkerhet i alle ledd

Politiets sikkerhetstjeneste (PST) viser til brev fra Justis- og beredskapsdepartementet (JD) om felles høring av:

1. Utredning fra IKT-sikkerhetsutvalget (Holte-utvalget) NOU 2018:14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet
2. Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett.

PST beklager fristoversittelse, men viser til dialog med departementet vedrørende dette.

Generelt

PST er positive til at det stilles sikkerhetskrav i lovs form til IKT-systemer og at det utarbeides regler for håndtering av hendelser. PST mener at kombinasjonen av pålegg og sanksjonsmuligheter er viktig for å oppnå nødvendig IKT-sikkerhet. Erfaring viser at mangelfull kontroll over og sikring av digitale verdier er en utfordring for mange sektorer.

Statlig styrte nettverksoperasjoner en vedvarende trussel mot norske verdier, og angriperne finner stadig nye sårbarheter de kan utnytte. Videre er virksomheter innen norsk statsforvaltning, kritisk infrastruktur, deler av norsk næringsliv og norske teknologibedrifter utsatte etterretningsmål og må sørge for god IKT-sikkerhet og oversikt over egen nettverksstruktur[1].

Videre medfører tjenesteutsetting i mange tilfeller komplekse og uoversiktlige avhengigheter på tvers av sektorer. Utkontraktering av IKT-tjenester kan øke sikkerheten når de legges til profesjonelle leverandører, men det skaper samtidig utfordringer knyttet til kontroll over virksomhetens verdier, herunder sikring og tilgang. Dette gjelder særlig

[1] PST trusselvurdering 2019

når tjenestene utsettes til utenlandske selskaper, og deler av verdikjedene forlater norsk jurisdiksjon.

Utvalget beskriver i liten grad behovet for beslutningsunderlag og oppdaterte situasjonsbilder i det digitale rom. Etter PST oppfatning er det imidlertid klart at god trusselkunnskap hos sentrale beslutningstakere er en forutsetning for gode beslutninger, og kunne således vært beskrevet tydeligere.

Et tema som ikke er behandlet i utvalgets rapport er hvorvidt tjenesteleverandørers/vertstjenesters virksomhet i større grad burde vært regulert. Såkalt Bulletproof hosting (BPH) er tjenester designet for å motstå deteksjon, sporing og nedstengning, og er således tilrettelagt for kriminell anvendelse. BPH-leverandører kjøper legitime vertstjenester fra vestlige selskaper og benytter disse som byggeklosser. Utviklingen er en del av en strategi for å omgå svartelisting og trafikkblokkering fra myndighetshold. Ved å gjemme seg blant annen legitim trafikk og organisere BPH-tjenestene i flere ledd, etableres en frisone hvor uønsket aktivitet er krevende å avdekke og stanse. Foruten truslene dette kan representere direkte, kan dataressurser under norsk jurisdiksjon benyttes av utenlandske trusselaktører mot mål i utlandet. Uten strengere regulering av markedet for vertstjenester er det til grunn til å frykte økt involvering av norske tilbydere i kriminell og annet ondsinnet virksomhet.

NOU 2018:14

Utvalget har følgende 5 anbefalinger:

1) Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning. Hvordan tette digitale sårbarheter i lange og komplekse digitale verdikjeder?
2) Krav om IKT-sikkerhet ved anskaffelser
3) Etablere nasjonalt IKT-sikkerhetssenter
4) Tydelig regulering og ansvar for tilkoblede produkter og tjenester
5) Tydelig styring og bedre koordinering av nasjonal IKT-sikkerhet

Forslag om ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

Utvalget belyser viktige problemstillinger i vårt digitale samfunn, og PST støtter behovet for en klargjøring av regelverket på området. I høringen til utvalgets mandat rettet PST fokus mot at offentlige og private virksomheter må forholde seg til mange og ulike regelverk om informasjonssikkerhet. Videre er dagens regulering tett knyttet mot sektorprinspippet, med den risikoen det medfører for at avhengigheter på tvers av sektorer ikke synliggjøres og at ansvaret for å vurdere verdiene samlet sett ikke er klart.

Videre er sektorregelverkene ofte fragmenterte, benytter ulike begreper og har ulikt detaljeringsnivå. Eksempelvis er det forskjeller mellom beredskapsforskriften (forskrift om forebyggende sikkerhet og beredskap i energiforsyningen) og drikkevannsforskriften, selv om begge har mål om å opprettholde grunnleggende nasjonale funksjoner.

Som et utgangspunkt anser PST det som hensiktsmessig med en ny lov om IKT-sikkerhet. Ikke minst er tjenesten positive til rapporteringsplikt for virksomhetene. Som utvalget selv påpeker i innledningen til kapittel 10 er det mye regelverk som kan ha betydning for IKT-sikkerhet. Utvalgets kartlegging viser at regelverket er fragmentert og omfattende. PST ser at det omfattende regelverket som eksisterer i dag kan være krevende å se som en helhet og reiser derfor spørsmålet om hvorvidt enda en lov vil være det mest

hensiktsmessige virkemiddelet for å løse denne utfordringen. Uavhengig av om man velger å vedta en ny lov på området, bør det utarbeides veiledninger for hvordan eksisterende regelverk skal forstås og brukes, for eksempel på lik linje med NSMs veiledere til sikkerhetsloven.

Krav om IKT-sikkerhet ved anskaffelser

PST støtter utvalgets vurderinger knyttet til lange og komplekse digitale verdikjeder og risikoen ved at bidragsytere tidlig i verdikjeden vil kunne påvirke sikkerheten lenger ut i samme kjede. Ansvaret for å påse at sikkerheten er ivaretatt bør tillegg hver enkelt aktør i kjeden.

Det fremstår som hensiktsmessig å implementere et IKT-sikkerhetselement inn i Statens standardavtaler, samt sette fokus på informasjonssikkerhet generelt i offentlige anskaffelser. Det kan videre være nyttig å implementere krav/mulighet for gjennomføring av sikkerhetsrevisjon hos alle underliggende.

Når det gjelder skybaserte tjenester og leverandører bør disse etter PSTs oppfatning ses i en større sikkerhetsmessig kontekst enn kun personvern og konfidensialitet. Videre er skyleverandører etablert i ulike land og er ofte underlagt ulik lovgivning noe som bør hensyntas ved anskaffelser.

Etablere nasjonalt IKT-sikkerhetssenter

Flere av de funksjonene som utvalget beskriver er nå på plass i NSM sitt nye senter som etter planen skal åpne medio 2019. I tillegg har Kripos et eget cybersenter og EOS-tjenestene, sammen med Kripos, samhandler i Felles Cyberkoordineringssenter. Dersom det vurderes å etablere nok et senter er PST bekymret for at mange aktører ikke evner å koordinere og samordne seg. Det bør videre ses hen til de funksjonene som allerede eksisterer i dag, for eksempel NSMs ansvar for rådgivning og kontroll med beskyttelsesverdige nettverk og systemer, en vurdering av hvorvidt NorCert sin deteksjonskapasitet kan vurderes utvidet og andre Cert-funksjoner som kan utvides. Videre er det uklart for PST hvordan man ser for seg grenseoppgaven mot PSTs oppgaver etter politiloven § 17 b, samt til det allerede etablerte koordineringselementet i FCKS.

Dersom det vurderes å etablere et nytt IKT-sikkerhetssenter, må det også tas hensyn til behovet for spesialkompetanse. Tilgangen på slik kompetanse er begrenset i Norge i dag. Senterets kompetansebehov vil derfor kunne gå på bekostning av allerede etablerte funksjoner/strukturer som enten besitter eller vil ha behov for fremtidig kompetanse. Ved innføring av nye lover og nye sikkerhetskrav er det viktig å samtidig utvikle en kapasitet til gjennomføring og etterlevelse.

PST anbefaler også å se hen til andre land innen EU som på tvers av landegrenser har etablert gode samarbeid innenfor cybersecurity og deteksjon.

Tydelig regulering og ansvar for tilkoblede produkter og tjenester

PST har forståelse for intensjonen og behovet for å regulere markedet for tilkoblede produkter og tjenester, men ser at dette kan være utfordrende i praksis når det gjelder produkter som faller innenfor IOT-området. Her vil antall enheter som er koblet til internett mangedobles i løpet av få år med et stort antall sensorer som for eksempel værstasjoner, høyttalere, kjøleskap, vaskemaskiner osv. IOT-enheter vil bli benyttet både i private hjem, samt av kommersielle aktører og offentlige etater. Disse enhetene vil også kunne være en mulig angrepsvektor mot nettverk og representerer derfor en stor sikkerhetsutfordring. PST vil anbefale deteksjonskapasitet som påkrevde løsninger i kritisk

infrastruktur for å håndtere veksten i antall enheter. NorCert vil også kunne avdekke storskala misbruk av IOT-enheter ved å følge med på trafikkflyten på internett i Norge.

I et eventuelt lovverk bør det videre stilles krav til underleverandører om sikkerhet når de leverer tjenester til, eller leverer inn i prosjekter til, samfunnskritiske etater og bedrifter. PST ser et mønster i at underleverandører blir mål for operasjoner for å få tilgang til større bedrifters informasjon og systemer. Et lovverk alene vil imidlertid ikke kunne løse utfordringen, uten at det samtidig tas høyde for at enkelte trenger bistand eller tilgang på spesielle offentlige tjenester for å komme opp på et godt nok sikkerhetsmessig operativt nivå og for å imøtekomme kravene som stilles. Virksomheter som har behov for underleverandører i sin daglige drift må også ha bestillerkompetanse og god nok kunnskap til å kunne vurdere om leverandørene de benytter har et godt nok sikkerhetsnivå.

Tydelig styring og bedre koordinering av nasjonal IKT-sikkerhet

PST støtter utvalgets tilnærming om at IKT-sikkerhet må løftes inn i styringsprosesser på nasjonalt nivå.

Utkast til lov som gjennomfører NIS-direktivet i norsk rett

Lovens formål og virkeområde, jf. lovutkastet §§ 1 og 2

PST ser at den foreslåtte loven på flere områder kan være sammenfallende med sikkerhetsloven med forskrift og veiledere som også stiller en rekke krav til informasjonssystemer. Det fremgår ikke klart av forarbeidene hvordan disse to lovene skal anvendes i forhold til hverandre og det er uklart hvem som skal vurdere hvilket regelverk som skal gjøres gjeldende for virksomheter som tilsynelatende omfattes av begge regelverkene. Etter PSTs oppfatning bør dette tydeliggjøres slik at virksomhetene settes i stand til å implementere regelverket.

Krav om varsling, jf. lovutkastet §§ 8 og 10

Vi støtter en rapporteringsplikt på hendelser for de bedrifter/virksomheter som dekkes av loven. I dag er det store mørketall og mye forsøkes løst internt i virksomhetene uten at norske myndigheter har et klart bilde av det egentlige omfanget og konsekvensene av hendelsene. En rapporteringsplikt vil i større grad tilrettelegge for å rette innsatsen mot riktige områder samt muligheter til å bidra med forebyggende virksomhet. Det vil være hensiktsmessig at sektor-CERT'ene (Helse, Finans, Justis osv.) kan ta imot varsler som igjen koordineres nasjonalt etter eskaleringsprinsipper en blir enige om tverrsektorielt.

Generelle merknader

Det er for øvrig stor forskjell på å stille krav om IKT-sikkerhet og å inneha evnen til å avdekke avanserte angrep. Bedrifter er utsatt så lenge de er koblet til internett og det vil være tilfeller der bedrifter kommer i kontakt med sårbart utstyr som følge av innkjøp og feil eller mangelfull implementering av utstyr. Det krever spesiell kompetanse og mye ressurser for å avsløre/avdekke misligheter/svakheter i hardware og software som selges på det åpne markedet. PST ser stadig utstyr som ikke har et tilstrekkelig sikkerhetsmessig nivå. En lov bør klargjøre hvem som skal ha oversikt over godkjent utstyr/programvare og hva som bør unngås. Dersom utstyr/programvare tas i bruk og det senere avdekkes svakheter, bør en lov videre regulere hvem som er ansvarlig for å iverksette tiltak og hvilke økonomiske tap en bedrift må tåle å bære som følge av disse

kravene. Mange små bedrifter vil ha en lav tålegrense for dette og kan derfor måtte ha behov for mer offentlig hjelp for å bli gode på IKT-sikkerhet.

Når det gjelder bedrifter og virksomheter som er samfunnskritiske bør det vurderes om det kan være hensiktsmessig å oppstilles en plikt til å delta i NSMs VDI-nettverk. En slik plikt bør lovreguleres, men det bør også sies noe om hvilke krav som stilles mht. kompenserende tiltak i en forskrift eller lignende.

Departementet ber til slutt om innspill på fem konkrete spørsmål til utkast til lov som gjennomfører NIS-direktivet i norsk rett. PST anser det ikke som relevant eller hensiktsmessig at tjenesten besvarer disse.

Dersom departementet finner det formålstjenlig stiller PST gjerne på et møte for å gi utdypende innspill på enkelte av punktene.

Roger Berg
fung. sjef PST