17 MAR 2016

Politiets sikkerhetstjeneste
Den sentrale enhet

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

Kontaktperson:

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref.: 15/8216
Vår ref.: 201500719-3
Dato: 15. mars 2016

Høring - NOU 2015:13 - Digital sårbarhet - Sikkert samfunn

PST viser til brev av 9. desember 2015 der utredningen fra Det digitale sårbarhetsutvalget (Lysneutvalget) – *Digital sårbarhet – sikkert samfunn*, sendes på høring. Departementet ber om høringsuttalelser innen 15. mars 2015.

Innledende betraktninger

Utvalget innleder utredningen med å peke på at digitaliseringen har ført til gjennomgripende samfunnsmessige endringer. Samfunnet har på mange måter blitt enklere og mer effektivisert, men de store teknologiske endringene fører også med seg utfordringer. Samfunnet opplever store endringer i risiko- og sårbarhetsbildet. Vi opplever for eksempel nye trusler som cyber-angrep i regi av anonyme aktører i andre land rettet mot norske maskiner og infrastruktur. Dette påvirker behovet for nye politimetoder. Utredningen har således et bredt nedslagsfelt og PST er på flere måter berørt av de problemstillinger som utvalgets utredning omfatter.

Utredningen er preget av det brede nedslagsfeltet på den måten at den reiser flere store problemstillinger som utvalget ikke har kunnet gå nærmere inn i, grunnet omfang, tid eller utvalgets sammensetning. Det betyr at utvalget i hovedsak har belyst store utfordringer uten å komme med andre konkrete løsningsforslag enn at man må gå disse i dybden. Utvalget har imidlertid kommet med sju hovedanbefalinger, og PST har derfor valgt å konsentrere sin høringsuttalelse om disse.

Et viktig utgangspunkt for PST i denne sammenheng, er at tjenestens ansvar er identisk i det digitale rom som i den fysiske verden. PST må derfor være i stand til å utføre sin del av myndighetsnærværet også i det digitale rom. Tjenesten må kunne bevege seg, samle og lagre informasjon for å forebygge og etterforske på en hensiktsmessig måte tilsvarende det tjenesten kan i den fysiske verden. Dette er også lovgivers ansvar.

Det er i den sammenheng viktig å være klar over at den teknologiske utviklingen ikke bare skaper muligheter, men også vanskeliggjør bruk av eksisterende lovfestede metoder. Et eksempel på dette er at fordi kryptering av personlig kommunikasjon nå er regelen, har politiet i dag mindre nytte av lovfestet kommunikasjonskontroll enn da denne metoden ble innført. For det andre ligger det en håndteringsutfordring i det faktum at mengden åpen informasjon som deles og tilgjengeliggjøres for allmennheten på internett i dag er svært stor. Dette er et paradigmeskifte som dagens metoder ikke er beregnet på.

Dagens utfordringer hva gjelder etterretningstrusselen gjenspeiler den rivende tekniske utviklingen i samfunnet som helhet. Nettverksbaserte etterretningsoperasjoner har blitt en integrert del i fremmede sikkerhets- og etterretningstjenesters arbeid, og utføres i stort omfang mot Norge og norske interesser. Flere land har i løpet av de siste ti årene utviklet en omfattende etterretningskapasitet i det digitale rom, med vide juridiske og politiske fullmakter til å utnytte denne. Mange stater bruker dessuten store ressurser på sine etterretningstjenester, og tillegger informasjonen som disse produserer, en vesentlig rolle i egen beslutningskjede.

PST mener på denne bakgrunn at datanettverksbaserte operasjoner er den etterretningsmetoden som i dagens samfunn, og i nær fremtid, kan ha de mest alvorlige og omfattende skadevirkningene på hele spekteret av norske interesser. Dagens teknologiske muligheter til ulovlig å hente ut enorme mengder informasjon, samt utføre sabotasjeoperasjoner, underbygger dette.

Et helhetlig rammeverk for digital hendelseshåndtering

PST støtter utvalget i at det er viktig med et helhetlig rammeverk for digital hendelseshåndtering, herunder utvalgets forslag om at det skal opprettes et nasjonalt cyber-senter med det formål å forebygge og etterforske kompleks og grenseoverskridende IKT-kriminalitet. Tjenesten vil imidlertid understreke at det er viktig at dette helhetlige rammeverket åpner for at aktørene kan ivareta eget ansvar på området. Dette er særlig aktuelt for EOS-tjenestene.

Det skjer allerede et betydelig arbeid og samarbeid på dette feltet, aktørene og deres håndtering blir bedre og EOS-tjenestene har erfart ressursøkning. Utredningens beskrivelse yter således ikke dagens virkelighet fullstendig rettferdighet. PST bestrider imidlertid ikke at det er viktig å finne den beste og mest effektive måten for å få etablert et enhetlig situasjonsbilde og samarbeid.

Samtidig er det en kjensgjerning at det krever, og alltid vil kreve, et helt spesielt samarbeid, EOS-tjenestene i mellom, for å håndtere de mest alvorlige truslene på dette området, både nasjonalt og internasjonalt. Med alvorlige trusler og cyber-hendelser menes her statlige eller statsstøttede aktørers spionasje og sabotasje i det digitale rom rettet mot norsk samfunnskritisk infrastruktur og informasjon, samt mot norske samfunnskritiske funksjoner. Det er nødvendig med mulighet for hurtig informasjonsutveksling og effektive mekanismer for å etablere en felles nasjonal situasjonsforståelse i denne sammenheng. Det vil kunne sikre at nødvendige forebyggende tiltak og/eller operative mottiltak blir gjennomført, slik at digitale trusler, på dette området, tas ned, uskadeliggjøres eller fjernes.

Dette samarbeidet skjer i Cyberkoordineringsgruppen (CKG) og er i dag beskrevet i Retningslinjer for samarbeid mellom EOS-tjenestene om forebygging og håndtering av alvorlige cyber-hendelser. CKG møtes regelmessig. Kripos deltar også i en utvidet del av dette samarbeidet, og det er p.t. til vurdering hvordan man best mulig kan involvere Kripos på en mer hensiktsmessig måte. Samarbeidet er for øvrig beskrevet i utredningens punkt 21.2.1.

Samarbeidet er innrettet mot nettverkstrusler og - operasjoner som går mot mål av grunnleggende nasjonal interesse hvor det er grunn til å anta statlige eller statsstøttede aktører står bak. EOS-tjenestene har blant annet med bakgrunn i dette, i felleskap sendt et forslag til Justis- og beredskapsdepartementet og Forsvarsdepartementet om å styrke samarbeidet tjenestene i mellom i det digitale rom.

Det er for PSTs del nødvendig med et tett og fortrolig samarbeid med flere andre nasjonale myndighetsaktører, særlig Kripos og det ordinære politiet, som også i den fysiske verden er nære og viktige samarbeidspartnere for PST. Tilsvarende er det viktig å samarbeide med disse i det digitale rom. Imidlertid kan ikke all informasjon deles med alle, blant annet på grunn av tredjepartsregelen. Tredjepartsregelen hviler på et prinsipp om at utsteder av

informasjonen forbeholder seg retten og eierskapet til opplysningene, og at disse kun skal brukes til etterretningsformål og ikke videreformidles uten samtykke. Dersom opplysningene skal brukes til noe annet, for eksempel etterforskning eller videreformidles til andre myndigheter, må det innhentes tillatelse fra utsteder. Regelen er nedfelt i politiregisterforskriften § 21-7 andre ledd. PST mener imidlertid at EOS-samarbeidet med fordel kan *samlokaliseres* med flere aktører i rammen av et større senter med et utvidet mandat som går ut over de mest alvorlige trusler i det digitale rom. Slik er tjenesten samstemte med utvalgsflertallets syn på fordelene med samlokalisering. Forutsetningen er selvsagt at infrastrukturen i tilstrekkelig grad tilrettelegger for hensiktsmessige autorisasjonsskiller.

Datanettverksoperasjoner er grenseoverskridende kriminalitet som også krever et utstrakt internasjonalt samarbeid. Det er derfor også viktig at PSTs evne til samarbeid med andre tjenester med tilsvarende ansvar styrkes og utvikles i tråd med vurderingen om digitale truslers økende alvorlighet. Dette vil på sikt kunne gjøre det betydelig enklere å få et enhetlig situasjonsbilde.

Vurdering av nye politimetoder - balansen mellom personvern og et sikrere samfunn må sikres gjennom utredninger og offentlig debatt
PST vil understreke at tjenesten på generelt grunnlag er enig i at det ved innføring av nye, inngripende politimetoder og virkemidler, er viktig at beslutningen tas på grunnlag av en godt opplyst og åpen debatt. PST mener derfor at det i regelen er nyttig at det settes ned bredt sammensatte offentlige utvalg for å vurdere slike spørsmål. Det er imidlertid av avgjørende viktighet at arbeidet blir fulgt opp i ettertid. Som tidligere nevnt, og lagt til grunn av utvalget, er den teknologiske utviklingen rivende og PSTs ansvar og oppgaver er verken et annet eller mindre i den digitale verden sammenlignet med den fysiske. Forventningene til tjenestens oppgaveløsning er tilsvarende, men mulighetene for tilfredsstillende oppgaveløsning er begrenset. Metodene som tidligere ga politiet tilgang til verdifull informasjon er i dag av mindre betydning fordi samfunnet generelt har endret sine måte å kommunisere, samhandle og agere på.

Gjeldende metoder er ikke innrettet for den type kriminalitet som knytter seg til digitale angrep. Det er derfor ikke bare nødvendig å kartlegge behovet for nye metoder, men også å tilpasse eksisterende regelverk til den digitale verden, for å sikre ivaretakelse av lovgivers intensjon i allerede vedtatte metoder.
Utvalget peker selv på at det er vesentlig at både E-tjenesten, PST og politiet har anledning til å innhente tilstrekkelig mengder ulik informasjon for å kunne utføre sine oppgaver. Dette er ikke tilfellet i dag. Det er derfor viktig at Lysne-utvalget blir fulgt opp ved at det gjennom utredninger legges til rette for at alle sider av denne situasjonen vurderes grundig.

Opprettelse av et utvalg for å utrede bruk av stordata
PST støtter utvalgets anbefaling om en egen utredning/NOU vedrørende bruk av stordata. En grundig utredning, som kan vurdere alle samfunnsinteresser og konsekvenser, vil gi et godt utgangspunkt for offentlig diskurs, og et mer opplyst og balansert bilde av behov og omfang enn debatten frem til i dag har båret preg av.

Et slikt arbeid vil klargjøre og utdype politiets behov generelt og PSTs behov spesielt. Samtidig vil det, etter tjenestens oppfatning, kunne vise at personvern og rettssikkerhet kan ivaretas ved valg av metodisk og teknisk tilnærming. Metodevalg knyttet til åpne kilder, som bruk av stordata, bør være transparent og tilgjengelig for demokratisk kontroll.

Utvalget mener at bruk av kryptografi ikke bør ikke reguleres
Utvalget peker på at kryptografi er nødvendig for å beskytte kommunikasjon, samtidig er det en utfordring at kryptografi gjør det umulig å oppfylle politiets og etterretningens legitime behov for avlytting. Utvalget er likevel tydelig på at bruk av kryptografi ikke bør reguleres, verken nasjonalt eller internasjonalt, fordi det er svært vanskelig å lage systemer som både ivaretar legitime behov for beskyttelse og legitime behov for avlytting. Utvalget

sier derfor at nye etterforskningsmetoder må utvikles for å sikre effektivt politiarbeid i en verden der mer og mer krypteres. PST mener at det er særlig viktig at dette følges opp.

Kryptering kan blant annet gjøre informasjonen (innholdsdata) uleselig for utenforstående. Informasjonen som blir utvekslet er beskyttet ved at den er pakket inn på en slik måte at det i utgangspunktet kun er de med rett «nøkkel» som kan lese innholdet. Det går således i visse tilfeller fortsatt an å fange innholdet og en kan forsøke å "gjette seg til" riktige nøkler for å få tilgang. Dette er tid- og ressurskrevende og vil i de fleste tilfeller ikke gi resultater. Krypteringen er implementert på ulike måter, men det er vanlig at innholdsleverandører benytter en ende-til ende-kryptering. I praksis betyr det at innholdet krypteres på enheten som kommunikasjonen sendes fra, og det dekrypteres ikke før det når enheten kommunikasjonen sendes til.

PST ser viktigheten av kryptografi. I en tid der elektronisk kommunikasjon i økende grad går over IP-baserte plattformer, kombinert med generelt høyere sikkerhetsbevissthet hos den enkelte bruker og implementering av kryptering som standard, har imidlertid politiet i dag allerede mistet tilgang til store mengder innholdsdata. Dette vil trolig eskalere i takt med den teknologiske utviklingen av nye kommunikasjonsplattformer. Uten tilpassede metoder vil politiets arbeid svekkes sammenlignet med i dag.

Det er ingen nye politimetoder på trappene som vil løse denne utfordringen fullstendig. Regjeringen la imidlertid 11. mars 2016 frem forslag til endringer i straffeprosessloven om bruk av skjulte tvangsmidler[1]. Forslaget omfatter blant annet dataavlesning som metode for politi og PST. En slik metode vil gi økt informasjonstilgang sammenlignet med den begrensningen kryptering medfører i dag.

Redusere kritikaliteten av Telenors kjerneinfrastruktur

PST støtter utvalgets anbefaling om å arbeide mot et målbilde der minst én tilleggsaktør har et landsdekkende kjernenett som er på samme nivå som Telenors med hensyn til dekning, kapasitet, fremføringsdiversitet, redundans og uavhengighet. PST ser gjennom sitt forebyggende arbeid at samfunnets avhengighet av Telenor i mange tilfeller er kritisk.

I den sammenheng er det viktig å være klar over at det ikke bare er det faktum alene at vi er avhengig av Telenors kjerneinfrastruktur som gjør samfunnet sårbare på dette området. Som en del av utviklingen gjenbrukes ofte eldre teknologi for å sikre brukervennlighet. Dette skaper betydelige sikkerhetsutfordringer. Brukervennlighet og sikkerhet er ofte motpoler. Høy sikkerhet fører gjerne til lite brukervennlige løsninger, mens god brukervennlighet kan bety at bakoverkompatibel (eldre) teknologi benyttes. Bakoverkompatibel betyr i utgangspunktet at nyere teknologi har innebygd funksjonalitet som ivaretar og kan benytte eldre teknologi/funksjonalitet. Ved å benytte slik teknologi, unngår man å ekskludere brukere og deres tidligere teknologivalg. Dersom økt sikkerhet tillegges større vekt, vil det gjerne føre til at forbruker uten oppdatert utstyr ekskluderes og at prisen på tjenestene øker. Utvalget peker imidlertid selv på at kompleksiteten i teknologien i dag allerede gjør det vanskelig for borgere å ta de rette IKT-sikkerhetsmessige valgene. Dette viser at det er viktig å tillegge sikkerhet mer vekt enn lavest mulig pris på tjenester.

De resterende hovedanbefalingene

PST mener det er viktig å styrke Justis- og beredskapsdepartementets tverrsektorielle virkemidler på IKT-sikkerhetsområdet. IKT er sektorovergripende av natur og dette vil i økende grad påvirke departementets arbeid ettersom samfunnet stadig søker økt effektivitet gjennom bruk av teknologi. Det er derfor viktig å kunne se de digitale sårbarhetene i sammenheng på tvers av sektorer. En helhetlig oversikt over digitale sårbarheter vil være et nyttig verktøy for å kunne redusere risiko på den mest hensiktsmessige måten.

---

[1] Prop. 68 L (2015-2016)

Behovet for å styrke politiets evne til å bekjempe IKT-kriminalitet understøttes av Politiets omverdensanalyse 2015. Her pekes det blant annet på at Norge er spesielt utsatt for kriminalitet på nett.[2]

Et utydelig myndighetsansvar for romvirksomheten, vil også kunne gjøre sikkerhetsansvaret ved romvirksomheten utydelig. PST mener derfor utvalgets anbefaling om å tydeliggjøre dette myndighetsansvaret er riktig og viktig.

Styrke IKT-sikkerhetskompetansen i sektortilsynene
Digitale sårbarheter reduseres ikke bare gjennom tiltak i det digitale rom. Sårbarheter opptrer grenseoverskridende mellom digitale og fysiske domener. Derfor oppstår det situasjoner hvor det ikke alltid er tydelig hvor det beste sårbarhetsreduserende tiltaket bør rettes. PST støtter derfor at sektortilsynene bør styrkes med sikkerhetskompetanse, og IKT-sikkerhetskompetansen som en del av dette..

Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet
PST støtter utvalgets forslag om å etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet for å sikre tilstrekkelig kompetanse og forståelse for denne problematikken.

Som utvalget selv sier, er egenberedskap essensielt for å kunne avverge digitale angrep. IKT- sikkerhet er først og fremst et virksomhetsansvar, og det er derfor viktig at virksomhetsledere tar stilling til både IKT-sikkerhet og all annen sikkerhet i egen virksomhet. Viktigheten av virksomhetsledelsens engasjement i sikkerhetsarbeidet er tidligere også påpekt fra Nasjonal sikkerhetsmyndighet[3]. Dette er imidlertid vanskelig uten tilstrekkelig og tilfredsstillende kompetanse.

Andre merknader
PST vil avslutningsvis peke på noen mindre forhold ved utredningen tjenesten har merket seg.

Prosjektprosess og sikkerhet
Utredningen berører i liten grad prosjektmetode og sikkerhet, men i en IKT-sammenheng er dette viktig. Prosjekt er ofte en arbeidsmetodikk som benyttes i utvikling og innføring av komplekse informasjonssystemer. Således er det viktig at sikkerhet integreres som en naturlig del av prosjekteringen. Sikkerhet bør bli et krav i prosjektprosessene til sektorer, på lik linje med for eksempel rapporteringskrav og kvalitetskrav. Tilstrekkelig rapportering på sikkerhet til prosjekteier i prosjekteringsfasen er viktig.
Manglende integrasjon i prosjektprosessen kan være en av årsakene til at sikkerhet har en tendens til å bli lagt til "i etterkant" og ikke bygd inn i produktet som prosjektet leverer fra starten av.

For å bøte på dette foreslår PST at sikkerhet integreres i Direktoratet for forvaltning og IKT (DIFI) sin anbefalte prosjektmodell for gjennomføring av digitaliseringsprosjekter i offentlig sektor[4].

Anskaffelsesprosess og sikkerhet
Utredningen berører også i liten grad sikkerhet i anskaffelsesprosesser. Utredningen beskriver at problematikken tidligere er nevnt av Organisation for Economic Co-operation and Development (OECD)[5] . Manglende sikkerhetstenkning er en utfordring i alle

[2] Politidirektoratet, Politiets omverdensanalyse 2015, side 29).
[3] Nasjonal sikkerhetsmyndighet, Rapport om sikkerhetstilstanden 2014
[4] www.difi.no/veiledning/prosjektveieviseren
[5] NOU 2015: 13, side 91

anskaffelser, men det er, etter PSTs oppfatning, særskilt relevant for IKT-tjenester. Dette fordi IKT-tjenester gjerne i sin natur er komplekse og håndterer potensielt store informasjonsverdier. Videre gjør utkontraktering (outsourcing) av IKT-tjenester seg stadig mer gjeldende.

Et konkret tiltak for å adressere denne problemstillingen ville være å integrere sikkerhet inn i DIFIs standardiserte prosessmodell for gjennomføring av offentlige anskaffelser.

Etablere tiltak for å regulere utlevering av trafikkdata til politiet
Utvalget skriver i punkt 11. 7. 5 at det er behov for å avklare hjemmelsgrunnlaget for regulering av tilgang til signaleringsdata. PST stiller seg positiv til dette.

Forebygge og forberede
PST gjør oppmerksom på at nest siste avsnitt i punkt 21.3.1 ser ut til å legge til grunn at politiets etterretningsdoktrine fra 2014 regulerer PSTs utlevering av sikkerhetsgradert etterretning til andre EOS-tjenester internasjonalt. Dette medfører ikke riktighet. Dette reguleres av politiregisterloven med tilhørende forskrift.

Marie Benedicte Bjørnland